Компьютерные преступления.

{ Их виды.

- **Компьютерная преступность** (преступление с использованием компьютера) — представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом, компьютерная информация является предметом или средством совершения преступления.

Глава 21 Статья 159.6 УК РФ

Мошенничество в сфере компьютерной информации

Это преступления, **имеющие** своим **предметом** только лишь **аппаратно-технические средства вычислительных машин** (хищение, уничтожение). Т.е. **“Преступление против собственности”.**

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.

Глава 28.
Преступления в сфере компьютерной информации

УК РФ содержит три статьи, предусматривающие ответственность за совершение преступлений в сфере компьютерной информации:

ст. 272 (неправомерный доступ к компьютерной информации, повлекший за собой уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети);
ст. 273 (создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами);
ст. 274 (нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред).

Объективную сторону преступлений в сфере компьютерной информации составляют

- ❖ неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло уничтожение, блокирование, модификацию, копирование информации, нарушение работы ЭВМ или ее сети (ст. 272 УК РФ),
- ❖ создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ),
- ❖ нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред (ст. 274 УК РФ).

Субъектом преступлений в сфере компьютерной информации является **вменяемое физическое лицо, достигшее 16-летнего возраста.** Преступления в сфере компьютерной информации могут совершаться как с умыслом, так и по неосторожности (ст. 272, 274 УК РФ) или только с прямым умыслом (ст. 273 УК РФ).

Лица, совершающие преступления в компьютерной сфере

Что касается лиц, совершающих преступления в сфере компьютерной информации, то они делятся на три группы:

1. **Хакеры** — профессиональные взломщики защиты компьютерных программ и создатели компьютерных вирусов, которых отличает высокий профессионализм в сочетании с компьютерным фанатизмом.

В зависимости от вида деятельности хакеры имеют следующие специализации: **а) крекеры** (взломщики защиты программ от неоплаченного использования); **б) фрикеры** (используют альтернативные варианты оплаты телефонных услуг для обмана АТС); **в) кардеры** (оплачивают свои расходы с чужих кредитных карточек); г) сетевые хакеры (взломщики защиты провайдера) и др.

К признакам совершения преступлений в сфере компьютерной информации хакерами относятся оригинальность способа и отсутствие тщательной подготовки к преступлению и его сокрытию.

2. **Психически больные лица, страдающие компьютерными фобиями** (т.е. профессиональными информационными заболеваниями), которые уничтожают или повреждают компьютерную технику без наличия преступного умысла с частичной или полной потерей контроля над своими действиями.

3. **Криминальные профессионалы** — т.е. преступные группировки, преследующие политические цели; лица, занимающиеся промышленным шпионажем; группировки отдельных лиц, стремящихся к наживе. Преступления, совершаемые ими в сфере компьютерной информации носят серийный, многоэпизодный характер, совершают многократно, обязательно с применением мер по сокрытию преступления.

Большинство из преступников в сфере компьютерной информации составляют мужчины — 83%, но доля женщин быстро увеличивается в связи с появлением чисто «женских» специальностей, связанных с необходимостью овладения компьютерной техникой.

При этом размер ущерба от преступлений, совершенных мужчинами, в четыре раза больше, чем от преступлений, совершенных женщинами. Возраст правонарушителей на момент совершения преступления составлял: до 20 лет (33%); от 20 до 40 лет (54%) и старше 40 лет (13%). Из каждой тысячи преступлений в сфере компьютерной информации только семь совершаются профессиональными программистами. При этом 40% преступников имели среднее специальное образование, 40% — высшее и 20% — среднее.

Перечислим некоторые основные виды преступлений, связанных с вмешательством в работу компьютеров.

1) **Несанкционированный доступ к информации, хранящейся в компьютере.**

Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.
Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.п.), оказываются беззащитны против этого приема. Самый простой путь его осуществления - получить коды и другие идентифицирующие шифры законных пользователей.
Несанкционированный доступ может осуществляться и в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить все, что в них хранится.

2) Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

3) Разработка и распространение компьютерных вирусов.
«Троянские кони» типа сотри все данные этой программы, перейди в следующую и сделай то же самое» обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

4) Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.
Проблема неосторожности в области компьютерной техники сродни неосторожной вине при использовании любого другого вида техники, транспорта и т.п.
Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима.

5) Подделка компьютерной информации.

По-видимому этот вид компьютерной преступности является одним из наиболее свежих. Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик причем имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

Естественно, что подделка информации может преследовать и другие цели.

6) Хищение компьютерной информации.

Если *«обычные»* хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путем краж и обмена краденым. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны.

Одной из наиболее распространенных из существующих классификаций преступлений в сфере компьютерной информации является кодификатор рабочей группы Интерпола, который был положен в основу автоматизированной информационно-поисковой системы, созданной в начале 90-х годов. В соответствии с названным кодификатором все компьютерные преступления классифицированы следующим образом :

QA Несанкционированный доступ и перехват:
QAH - компьютерный абордаж (несанкционированный доступ);
QAI – перехват с помощью специальных технических средств;
QAT - кража времени (уклонение от платы за пользование АИС);
QAZ - прочие виды несанкционированного доступа и перехвата.
QD - Изменение компьютерных данных:
QDL - логическая бомба;
QDT - троянский конь;
QDV - компьютерный вирус;
QDW- компьютерный червь;
QDZ - прочие виды изменения данных

QF - Компьютерное мошенничество:
QFC - мошенничество с банкоматами;
QFF - компьютерная подделка;
QFG - мошенничество с игровыми автоматами;
QFM - манипуляции с программами ввода-вывода;
QFP - мошенничества с платежными средствами;
QFT - телефонное мошенничество;
QFZ - прочие компьютерные мошенничества.
QR - Незаконное копирование:
QRG - компьютерные игры;
QRS - прочее программное обеспечение;
QRT - топология полупроводниковых устройств;
QRZ - прочее незаконное копирование.
QS - Компьютерный саботаж:
QSH - с аппаратным обеспечением (нарушение работы ЭВМ);
QSS - с программным обеспечением (уничтожение, блокирование информации);
QSZ - прочие виды саботажа.
QZ - Прочие компьютерные преступления:
QZB - с использованием компьютерных досок объявлений;
QZE - хищение информации, составляющей коммерческую тайну;
QZS - передача информации, подлежащая судебному рассмотрению;
QZZ - прочие компьютерные преступления.

Определенный интерес представляет классификация, предложенная В.А. Мещеряковым

1. Неправомерное завладение информацией или нарушение исключительного права ее использования.

1.1. Неправомерное завладение информацией как совокупностью сведений, документов (нарушение исключительного права владения).

1.2. Неправомерное завладение информацией как товаром.

1.3. Неправомерное завладение информацией как идеей (алгоритмом, методом решения задачи).

2. Неправомерная модификация информации.

2.1. Неправомерная модификация информации как товара с целью воспользоваться ее полезными свойствами (снятие защиты).

2.2. Неправомерная модификация информации как идеи, алгоритма и выдача за свою (подправка алгоритма).

2.3. Неправомерная модификация информации как совокупности фактов, сведений.

3. Разрушение информации.

3.1. Разрушение информации как товара.

3.2. Уничтожение информации.

4. Действие или бездействие по созданию (генерации) информации с заданными свойствами.

4.1. Распространение по телекоммуникационным каналам информационно-вычислительных сетей информации, наносящей ущерб государству, обществу и личности.

4.2. Разработка и распространение компьютерных вирусов и прочих вредоносных программ для ЭВМ.

4.3. Преступная халатность при разработке (эксплуатации) программного обеспечения, алгоритма в нарушение установленных технических норм и правил.

5. Действия, направленные на создание препятствий пользования информацией законным пользователям.

5.1. Неправомерное использование ресурсов автоматизированных систем (памяти, машинного времени и т. п.).

5.2. Информационное "подавление" узлов телекоммуникационных систем (создание потока ложных вызовов).

Необходимо заметить, что не все названные деяния признаются преступными по действующему российскому законодательству: часть из них лишь создает необходимые условия для последующего совершения наказуемых нашим Уголовным кодексом правонарушений и в определенных случаях может рассматриваться как приготовление или покушение на совершение преступлений, посягающих на различные объекты.

Приведенная классификация, скорее, отражает не преступления как таковые, а набор возможных противоправных посягательств на компьютерную информацию. Тем не менее, все они могут учитываться при совершенствовании действующего законодательства и дальнейшем решении вопроса о криминализации или декриминализации.