**Содержание:**


# Введение

Компьютерная сеть Интернет вобрала в себя не только достоинства глобальности, но и глобальные пороки. Возможности Сети все чаще становятся средствами совершения противоправных деяний. Усугубляется это возможностью наносить максимальный ущерб при минимуме затрат. Так по данным ФБР США, среднестатистический ущерб от одного такого преступления составляет 650 тыс.$ США.

Впервые компьютер был использован как инструмент для кражи из Банка Миннесоты в 1956 г. А первый закон был принят в США лишь в 1978 г. и предусматривал ответственность за модификацию, уничтожение, несанкционированный доступ к компьютерным данным. Отечественный преступный первенец относится к концу 70-х годов, а надлежащая правовая база появилась лишь в середине 90-х.

Популярность этой преступности растет из-за безнаказанности. СМИ также подогревают интерес к этому виду деятельности, создавая атмосферу романтики и славы.

Усиленные вторжения хакеров в те или иные компьютерные объекты показывают уязвимость компьютерных сетей, которые, стремясь к упрощению обмена информации и ускорению ее обработки, теряют на безопасности.

Хакеры привлекаются не только частными, но и государственными структурами. В 1986-1989 гг. немецкие хакеры по заданию КГБ СССР копировали секретные материалы из компьютерных сетей Пентагона и NASA.

За последние годы были взломаны: 1999г. сайт Совета Безопасности России, 2000- сайт Совета Федерации, МГТС, 2001- сайты Совета Федерации, Госкомстата, 2002- сайты МВД, Правительства Москвы. С октября 2002 г. существует «дыра» в системе защиты, через которую есть доступ к базе данных переписи населения.

# Компьютерные преступления

## Понятие компьютерных преступлений и их классификация

Научно-техническая революция повлекла за собой серьезные социальные изменения, наиболее важным из которых является появление нового вида общественных отношений и общественных ресурсов — информационных. Информация стала первоосновой жизни современного общества, предметом и продуктом его деятельности, а процесс ее создания, накопления, хранения, передачи и обработки в свою очередь стимулировал прогресс в области орудий ее производства: электронно-вычислительной техники (ЭВТ), средств телекоммуникаций и систем связи.

Появление на рынке в 1974 году компактных и сравнительно недорогих персональных компьютеров, по мере совершенствования которых стали размываться границы между мини- и большими ЭВМ, дали возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контролируемости доступа к информации, ее сохранности и доброкачественности. Организационные меры, а также программные и технические средства защиты оказались недостаточно эффективными.

Особенно остро проблема несанкционированного вмешательства дала о себе знать в странах с высокоразвитыми технологиями и информационными сетями.

Компьютерная информация – в соответствии со ст.2 закона “Об информации, информатизации и защите информации” под информацией понимаются – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, но применительно к комментируемым статьям под компьютерной информацией понимаются не сами сведения, а форма их представления в машиночитаемом виде, т.е. совокупность символов зафиксированная в памяти компьютера, либо на машинном носителе. При рассмотрении дел следует учитывать, что при определенных условиях и физические поля могут являться носителями информации.

Быстрый количественный рост преступности и ее качественные изменения, обусловленные обострением противоречий в различных областях общественной жизни, частой реорганизацией системы правоохранительных органов, несовершенство законодательства и частое его изменение, серьезные упущения в правоприменительной практике, способствуют ускорению процессов развития компьютерной преступности как социального явления.

Отсутствие четкого определения компьютерной преступности, единого понимания сущности этого явления значительно затрудняют определение задач правоприменительных органов в выработке единой стратегии борьбы с ней.

Компьютерные преступления условно можно подразделить на две большие категории – преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства. Не будем касаться “околокомпьютерных” преступлений, связанных с нарушением авторских прав программистов, незаконным бизнесом на вычислительной технике и т.п., а также физического уничтожения компьютеров.

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

## 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.

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

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.

5. Подделка компьютерной информации

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.

## 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.

Итак, под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть[2].

# Способы совершения компьютерных преступлений

Подходить к классификации компьютерных преступлений наиболее оправданно с позиций составов преступлений, которые могут быть отнесены к разряду компьютерных. Хотя состав компьютерных преступлений в настоящее время четко не определен, можно выделить ряд видов противоправных деяний, которые могут быть в него включены. Перечислим некоторые основные виды преступлений, связанных с вмешательством в работу компьютеров:

- «за дураком» – физическое проникновение в производственные помещения.
- «за хвост» – злоумышленник подключается к линии связи законного пользователя и дожидается сигнала, обозначающего конец работы.
- «компьютерный абордаж» – злоумышленник вручную или с использованием автоматической программы подбирает код (пароль) доступа к КС системе с использованием обычного телефонного аппарата:
- «неспешный выбор» – преступник изучает и исследует систему защиты от НСД, ее слабые места, выявляет участки, имеющие ошибки или неудачную логику программного строения, разрывы программ (брешь, люк) и вводит дополнительные команды, разрешающие доступ;
- «маскарад» – злоумышленник проникает в компьютерную систему, выдавая себя за законного пользователя с применением его кодов (паролей) и других идентифицирующих шифров;
- «мистификация» – злоумышленник создает условия, когда законный пользователь осуществляет связь с нелегальным терминалом, будучи абсолютно уверенным в том, что он работаете нужным ему законным абонентом.
- «аварийный» – злоумышленник создает условия для возникновения сбоев или других отклонений в работе СВТ. При этом включается особая программа, позволяющая в аварийном режиме получать доступ к наиболее ценным данным. В этом режиме возможно «отключение» всех имеющихся в компьютерной системе средств защиты информации.
- манипуляция данными и управляющими командами.

# Юридическая ответственность

Уголовный кодекс РФ предусматривает различные наказания за компьютерные преступления, а также разделяет преступления на группы:

| | |
|---|---|
| Ст. 272 | Неправомерный доступ к компьютерной информации. |
| Ст. 273 | Создание, использование и распространение вредоносных программ для ЭВМ. |
| Ст. 274 | Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети |

Но с помощью компьютера можно совершить любые преступления кроме изнасилования, поэтому количество статей, к которым они могут быть отнесены, велико.

1. ст. 129 Клевета
2. ст. 130 Оскорбление
3. ст. 137 Нарушение неприкосновенности частной жизни
4. ст. 138 Нарушение тайны переписи, телефонных переговоров, почтовых, телеграфных и иных сообщений.
5. ст. 146 Нарушение авторских и смежных прав
6. ст. 147 Нарушение изобретательных и патентных прав
7. ст. 158 Кража
8. ст. 159 Мошенничество
9. ст. 163 Вымогательство
10. ст. 165 Причинение имущественного ущерба путем обмана или злоупотребления доверием
11. ст. 167 Умышленное уничтожение или повреждение имущества
12. ст. 168 Умышленное уничтожение или повреждение имущества по неосторожности
13. ст. 171 Незаконное предпринимательство
14. ст. 182 Заведомо ложная реклама
15. ст. 183 Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну
16. ст. 200 Обман потребителя

17. ст. 242 Незаконное распространение порнографических материалов или предметов
18. ст. 276 Шпионаж
19. ст. 280 Публичные призывы к осуществлению экстремистской деятельности
20. ст. 282 Возбуждение национальной, расовой или религиозной вражды
21. ст. 283 Разглашение государственной тайны
22. ст. 354 публичные призывы к развитию агрессивной войны.

## Тенденции развития экономической преступности в России

Уровень компьютерной преступности определяется во многом объективными причинами и напрямую зависит от общего уровня информатизации общества. Большинством зарубежных и отечественных исследователей отмечается отставание России в вопросах компьютеризации от развитых стран в среднем на 20 лет. Если в США первое компьютерное преступление было зафиксировано в 1966 г., то в бывшем СССР — в 1979 г. Поэтому тенденции развития компьютерной преступности в России могут заметно отличаться от таковых в развитых странах. По мнению экспертов в данной области, следует, прежде всего, ожидать значительного количественного роста компьютерных преступлений. Этому способствует ряд причин, среди которых основными можно считать:

во-первых, резкий рост безработицы и падение уровня жизни среди так называемой «беловоротничковой» прослойки населения на фоне общего экономического кризиса и кризиса неплатежей;

во-вторых, массовая неконтролируемая компьютеризация и использование новейших электронных средств во всех сферах деятельности, прежде всего финансовых, банковских и кредитных учреждениях всех форм собственности;

в-третьих, отсутствие соответствующей правовой базы, препятствующей в сколько-нибудь заметной мере распространению и пресечению компьютерных преступлений.

Среди положительных тенденций можно прогнозировать сокращение числа краж собственно компьютерной техники и периферии, ввиду существенного падения цен на них и относительной доступности, а также сокращение незаконного использования машинных ресурсов и машинного времени.

На современном этапе развития ИТ в России назрела необходимость детального изучения проблемы основ криминалистического исследования компьютерной преступности. Следует отметить, что при совершении компьютерных преступлений, так же как и при совершении любых других общеизвестных видов преступлений, остаются «следы», обнаружение, фиксация и исследование которых является непременным условием при расследовании и раскрытии, как данного вида преступлений, так и в борьбе с «техногенной» преступностью в целом.

## Международная борьба

Стремительное развитие трансграничной компьютерной преступности поставило мировое сообщество перед необходимостью налаживания международного сотрудничества и совместного противодействия компьютерным преступникам.

Первый документ Совета Европы – Рекомендации № R89 (9) Комитета Министров Совета Европы о преступлениях с компьютерами (13 сентября 1989 года). К перечисленным правонарушениям, рекомендованных для включения в национальное законодательство, отнесены:

-компьютерное мошенничество

– компьютерный подлог

– причинение ущерба компьютерным данным и программам

– компьютерный саботаж

– несанкционированный доступ

– несанкционированный перехват

– несанкционированное воспроизведение микросхем.

Вскоре появилась международная «Конвенция о киберпреступности». Она содержит множество процессуальных положений. Россия является участником «Соглашения о сотрудничестве государств-участников СНГ в борьбе с преступностью в сфере компьютерной информации».
Формы сотрудничества: обмен информации, скоординированные мероприятия, подготовка квалифицированных кадров, создание информационных систем, обмен нормативно-правовыми актами.

# Заключение

Впервые мир узнал о компьютерных преступлениях в начале 70-х годов, когда в Америке было выявлено довольно большое количество таких деяний. Как известно – наиболее опасные преступления – это те, которые носят экономический характер. Изначально, как показывает история, органы уголовной юстиции боролись с ней при помощи традиционных правовых норм о преступлениях против собственности: краже, присвоении, мошенничестве, злоупотреблении доверием и тому подобное. Однако вскоре практика показала, что такой подход не отвечает всем требованиям сложившейся ситуации, поскольку многие преступления в сфере компьютерной деятельности не охватываются традиционными составами преступлений.

Преступления в сфере компьютерной информации имеют, на мой взгляд, как бы двоякий смысл, и поэтому требуют специальных статей в Уголовном кодексе. Принятый в недавнем прошлом кодекс содержит целую главу, включающую в себя три статьи, что, на мой взгляд, несколько мало. Даже исходя из дословного толкования, позволю себе сказать, что они уже несколько устарели по смысловому значению, и требуют обновлений. В своем реферате я попытался расширить само понятие преступлений в области компьютерной информации, придать ему новый смысл.

# Список использованных источников

1. Рааб М. “Защита сетей: наконец-то в центре внимания” / М. Рааб – М.: Просвящение, 1994. – 18с.
2. Векслер Д. “Наконец-то надежно обеспечена защита данных в радиосетях” / Д. Векслер – М.:Знания, 1996. – 13-14с.
3. Сухова С.В. “Система безопасности NetWare” / С.В.Сухова –М.: Сети, 1995.- 60-70с.
4. Беляев В. “Безопасность в распределительных системах” / В. Беляев – М.: Мысль, 1997. – 36-40с.
5. Ведеев Д. “Защита данных в компьютерных сетях” / Д.Ведеев – М.:Просвящение, 1995. – 12-18с.