Министерство образования Российской Федерации

**Новгородский Государственный Университет**

**им. Ярослава Мудрого**

**Кафедра уголовно-правовых дисциплин**

# Характеристика компьютерных

# преступлений в Великом Новгороде и Новгородской области

Контрольная работа по криминологии

### Выполнил

### Студента группы 6285з

**Избачкова Ю.С.**

**Проверил**

**Молокоедов В.В.**

**Новгород**

**1 Понятие преступлений в сфере компьютерной информации**

Компьютерные преступления впервые попали в сферу социального контроля в начале 70-х годов, когда в США было выявлено значительное количество подобных деяний. Этот факт привлёк к сфере компьютерной информации пристальное внимание органов юстиции и учёных-криминологов. Начались интенсивные исследования этого феномена в национальном и глобальном масштабах.

Различаются криминологические группы компьютерных преступлений: экономические, компьютерные преступления против личных прав и неприкосновенности частной сферы, компьютерные преступления простив общественных и государственных интересов.

Наиболее опасные и распространённые – экономические компьютерные преступления – включают компьютерное мошенничество, компьютерный экономический шпионаж и кражу программ, компьютерный саботаж, кражу и “компьютерного времени”, самовольное проникновение в автоматизированную систему, традиционные экономические преступления, совершаемые с помощью компьютера.

Компьютерные преступления против личных прав и свобод и неприкосновенности частной сферы чаще всего заключаются во введении в компьютерную систему неправильных и некорректных данных о лице, незаконном собирании правильных данных (незаконными способами либо с целью, например, неправомерного контроля профсоюзных активистов), иных незаконных злоупотреблениях информации на компьютерных носителях и неправомерном разглашении информации (разглашение, например, банковской или врачебной тайны, торговля банками информации и базами данных).

Компьютерные преступления против интересов государства и общества включают преступления против государственной и общественной безопасности, нарушение правил передачи информации за границу, дезорганизацию работы оборонных систем, злоупотребления с автоматизированными системами подсчёта голосов на выборах и так далее.

Первоначально, столкнувшись с компьютерной преступностью, органы уголовной юстиции начали борьбу с ней при помощи традиционных правовых норм о краже, присвоении, мошенничестве, злоупотреблении доверием. Однако такой подход оказался не вполне удачным, поскольку многие компьютерные преступления не охватываются составами традиционных преступлений. Так, например, простейший вид компьютерного мошенничества – перемещение денег с одного счёта на другой путём “обмана компьютера” – не охватывается ни составом кражи (ввиду отсутствия предмета кражи – материального имущества – так как деньги существуют здесь не в виде вещей, но в виде информации на компьютерном носителе), ни составом мошенничества, поскольку обмануть компьютер в действительности можно лишь в том смысле, в каком можно обмануть замок у сейфа.

Не будет и признаков уничтожения или повреждения имущества в случае, например, уничтожения информационного элемента компьютерной системы без повреждения его материального элемента, хотя подобные действия могут повлечь значительный имущественный ущерб.

Несоответствие криминологической реальности и уголовно-правовых норм потребовали корректировки последних. Это происходит в двух направлениях:

1) более широкого толкования традиционных норм (Голландия, Франция);

2) разработка специальных норм о компьютерных преступлениях (США, Швеция, Англия, Дания и абсолютное большинство других стран).

**2 Компьютерная преступность – латентная преступность**

В разделе 4 приведены статистические данные по Новгородской области. Данные почерпнуты из официальных источников, в первую очередь отчётов МВД.

Однако большинство преступлений в указанной сфере остаётся незафиксированными. Из этой группы я бы выделил две подгруппы.

Первая – создание и распространение вредоносных программ для ЭВМ (вирусов). Большинство таких программ создаётся за пределами Российской Федерации, поэтому борьба с мини невозможна. Хотя они наносят значительный ущерб, в том числе «железу». При этом даже если вирус создан в России, доказать его авторство не возможно.

Кроме того, потенциально возможная причина появления таких вирусов, как печально знаменитый «Чернобыль», заключается в том, что сами производители ЭВМ заинтересованы в обновлении парка офисного оборудования, которое замедлилось в связи со всё более большими проблемами технологического плана. Указанный вирус сделал непригодными в основном старые компьютеры. Не вдаваясь в технические моменты следует отметить, что его мог «сотворить» только человек очень, очень, очень, очень хорошо знающий оборудование на низком уровне.

Вторая – кражи электронной корреспонденции, доступа к информационным ресурсам.

Такие преступления очень трудно технически зафиксировать. Кроме того, сами организации, занимающиеся оказанием подобных услуг не заинтересованы в разглашении подобных фактов. Один такой случай имел место в Новгородской области в 1999-2000 годах.

**3 Уголовно-правовая характеристика компьютерных преступлений**

С принятием нового Уголовного кодекса в Российской Федерации стали преследоваться неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание программ для ЭВМ, могущих повлечь уничтожение, блокирование или копирование информации (так называемых компьютерных вирусов и программ-"взломов"), а также использование и распространение таких программ и машинных носителей с ними (ст. 273 УК РФ), нарушение правил эксплуатации ЭВМ или компьютерных сетей с причинением существенного вреда (ст. 274 УК РФ).

Форма вины для основного состава компьютерных преступлений - прямой либо косвенный умысел. Нужно отметить, что форма вины, предусмотренная для квалифицированного состава данной категории преступлений (т.е. для состава преступления, совершенного при обстоятельствах, отягчающих ответственность, и влекущего применение более суровых мер воздействия по сравнению с основным составом), является крайне любопытной. Дело заключается в том, что квалифицированные составы практически всех преступных деяний характерны усилением степени вины правонарушителя по сравнению с формой вины, необходимой для квалификации действий правонарушителя по основному составу (например, основной состав преступления - убийство, квалифицированный - убийство из корыстных побуждений). В данном случае при форме вины, установленной для основного состава преступления в виде умысла, для его квалифицированного состава Кодексом предусмотрена форма вины исключительно (!) в виде неосторожности: неосторожное причинение тяжких последствий при создании или использовании вирусных программ и неосторожное причинение тяжких последствий в результате нарушения правил эксплуатации влекут за собой лишение свободы соответственно на срок до 7 и до 4 лет. Умышленное причинение тяжких последствий при этом наказывается в рамках основного состава, за который санкции предусмотрены гораздо более легкие по сравнению с квалифицированным.[[1]](#footnote-1)

Объектами данных преступлений (тем, на что направлено преступное посягательство и что признано нуждающимся в защите) является не любая компьютерная информация, а только охраняемая законом (статьи 272, 274 УК РФ) и не любые уничтожение, блокирование, модификация, копирование информации при использовании вирусных программ, а только несанкционированные (ст. 273 УК РФ).[[2]](#footnote-2)

В размахе компьютерного пиратства может убедиться каждый, остановившись у киосков рядом с едва ли не любой станцией московского метро. Во многих из них торгуют "самопальными" компакт-дисками с нелицензионными копиями программ для ЭВМ, изготовленными без ведома владельцев авторских прав на эти программы. С аналогичным явлением можно столкнуться и при покупке компьютера. Ведь фирмы, занимающиеся сборкой и реализацией компьютеров, как правило, продают их с незаконно записанными в память ЭВМ чужими программами. Вот почему подавляющее большинство пользователей персональных компьютеров в нашей стране имеет дело с нелегальными программными продуктами.[[3]](#footnote-3)

По данным Ассоциации производителей компьютерного обеспечения, уровень компьютерного пиратства в России составляет 94%. Уровень пиратства в странах Запада существенно ниже: в Германии - 50%, в США - 35%. Однако и там убытки производителей весьма высоки - только в Европе они оцениваются в 6 млрд.долларов ежегодно.[[4]](#footnote-4)

Особенно страдают американские фирмы - разработчики программного обеспечения.

Необходимость установления уголовной ответственности за причинение вреда в связи с использованием именно компьютерной информации (т.е. информации на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или их сети) вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации по сравнению, скажем, с информацией, зафиксированной на бумаге и хранящейся в сейфе.

Преступное деяние, выразившееся в неправомерном доступе к компьютерной информации, посягает на общественную безопасность и общественный порядок, которые являются видовым объектом всех преступлений в сфере компьютерной информации, предусмотренных гл.28 УК.

Предметом преступления, указанного в ст.272 УК, является не любая информация, находящаяся в компьютерной форме, а только охраняемая законом. В соответствии со ст.2 Федерального закона от 20 февраля 1995 г. "Об информации, информатизации и защите информации" (далее - Закон об информации) информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Охраняемой законом, по смыслу УК, будет являться такая компьютерная информация, доступ к которой ограничен в соответствии с законом. Доступ - возможность совершения одного или ряда следующих действий: знакомиться с содержанием информации, копировать, уничтожать или изменять информацию.

Сегодня применение нормы, содержащейся в ст.272 УК "Неправомерный доступ к компьютерной информации", ограничено правовой и практической неразработанностью вопросов, связанных с использованием и охраной компьютерной информации, но правовая основа уже заложена.

Одной из причин отсутствия реальной борьбы с подобными деяниями в России является распространенное мнение о том, что от них терпят убытки исключительно западные фирмы. По данным МВД РФ, потери российского бюджета от неуплаты налогов продавцами компьютерных программ составляют 85 млн.долларов. Деньги, полученные от продажи, часто уходят в распоряжение криминальных структур. Кроме того, 105 млн.долларов теряют российские предприятия. В области разработки компьютерных программ и баз данных в стране работает около шести тысяч фирм, обеспечивающих занятость более 200 тыс.человек.[[5]](#footnote-5) Если положение не изменится, этой сфере производства грозит стагнация, поскольку программисты попросту потеряют стимулы к созданию новых передовых программных продуктов.

**4 Статистические данные по Новгородской области**

Официальная статистика даёт весьма скудную информационную картину компьютерных преступлений в Новгородской области.

В 1998 году таких преступлений зарегистрировано не было.

В 1999 году впервые выявлено 4 преступления, совершенные в сфере компьютерной информации. В общей массе совершаемых преступлений эти ничтожно малая цифра.

Они совершены тремя лицами. Из них привлечено к уголовной ответственности – 1 человек (25-29 лет), в отношение второго дело было прекращено. Оба – жители Великого Новгорода.

Одно преступление осталось нераскрытым в связи с не установлением лица, совершившего преступление.

В силу в первую очередь технических факторов этот вид преступности характерен для крупных городов.

Отвечает ли официальная статистика реальности?

Нет.

Во-первых, нарушение авторских прав на программное обеспечение необходимо также признавать преступлениями в сфере компьютерной информации. Из материалов органов внутренних дел данные о количестве таких преступлений выявить невозможно.

Во-вторых. Приведённые данные взяты из официальной статистики УВД Новгородской области. Однако указанные преступления относятся в первую очередь к компетенции ФСБ, а эти данные закрыты.

Следует отметить немаловажную деталь, связанную с преступлениями в указанной сфере. Оганы внутренних дел обязательно доводят до сведения общественности данные о раскрытии таких преступлений. Это новый вид деяний, запрещаемых уголовным законодательством, поэтому органам необходимо показать общественности и центральному руководству, что на местах не сидят сложа руки.

**Список литературы**

1 Гарифуллина Р. Ответственность за преступления в сфере финансово-кредитных отношений // "Российская юстиция" – 1997 – № 2

2 Голубев В.В. Компьютеризация и уголовное право // "Законодательство" – 1999 – № 8

3 Гульбин Ю. Преступления в сфере компьютерной информации // "Российская юстиция" – 1997 – № 10

4 Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // "Российская юстиция" – 1999 – № 1

5 Крылов В.В. Информация как элемент криминальной деятельности // "Вестник Московского университета", Серия 11, Право – 1998 – № 4

6 Симкин Л. Как остановить компьютерное пиратство? // "Российская юстиция" – 1996 – № 10

7 Яблоков Н.П. Криминалистическая характеристика финансовых преступлений // "Вестник Московского университета", Серия 11, Право – 1999 – № 1

1. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // "Российская юстиция" – 1999 – № 1 [↑](#footnote-ref-1)
2. Гульбин Ю. Преступления в сфере компьютерной информации // "Российская юстиция" – 1997 – № 10 [↑](#footnote-ref-2)
3. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // "Российская юстиция" – 1999 – № 1 [↑](#footnote-ref-3)
4. "Эксперт". 1996. N 17. С.19 [↑](#footnote-ref-4)
5. "Финансовые известия", 23 мая 1996 г. [↑](#footnote-ref-5)