**МИНИСТЕРСТВО ОБРАЗОВАНИЯ ТУЛЬСКОЙ ОБЛАСТИ**

**Государственное образовательное учреждение среднего**

**Профессионального образования Тульской области**

**«Тульский сельскохозяйственный колледж имени И.С.Ефанова»**

Работа над темой по самообразованию

**«Преступления в сфере высоких технологий».**

2013 г.

***Преступления в сфере информационных технологий****или****киберпреступность***

## Содержание

1. [**1 Виды**](http://ru.wikipedia.org/wiki/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD#.D0.92.D0.B8.D0.B4.D1.8B)
2. [**2 Уголовная ответственность в сфере компьютерной информации за рубежом**](http://ru.wikipedia.org/wiki/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD#.D0.A3.D0.B3.D0.BE.D0.BB.D0.BE.D0.B2.D0.BD.D0.B0.D1.8F_.D0.BE.D1.82.D0.B2.D0.B5.D1.82.D1.81.D1.82.D0.B2.D0.B5.D0.BD.D0.BD.D0.BE.D1.81.D1.82.D1.8C_.D0.B2_.D1.81.D1.84.D0.B5.D1.80.D0.B5_.D0.BA.D0.BE.D0.BC.D0.BF.D1.8C.D1.8E.D1.82.D0.B5.D1.80.D0.BD.D0.BE.D0.B)
	1. [**2.1 Германия**](http://ru.wikipedia.org/wiki/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD#.D0.93.D0.B5.D1.80.D0.BC.D0.B0.D0.BD.D0.B8.D1.8F)
	2. [**2.2 Люксембург**](http://ru.wikipedia.org/wiki/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD#.D0.9B.D1.8E.D0.BA.D1.81.D0.B5.D0.BC.D0.B1.D1.83.D1.80.D0.B3)
3. [**3 Международное сотрудничество**](http://ru.wikipedia.org/wiki/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD#.D0.9C.D0.B5.D0.B6.D0.B4.D1.83.D0.BD.D0.B0.D1.80.D0.BE.D0.B4.D0.BD.D0.BE.D0.B5_.D1.81.D0.BE.D1.82.D1.80.D1.83.D0.B4.D0.BD.D0.B8.D1.87.D0.B5.D1.81.D1.82.D0.B2.D0.BE)
4. **Виртуальная преступность в Тульской области (автор:** [***Рагим Мусаев***](http://www.proza.ru/avtor/ragim)**)**
5. **Содержание**

***Преступления в сфере информационных технологий****или****киберпреступность****—*[*преступления*](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5)*, совершаемые людьми, использующими*[*информационные технологии*](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8)*для преступных целей.*

## Виды

Преступления в сфере информационных технологий включают как распространение вредоносных [вирусов](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81), взлом [паролей](http://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C), кражу номеров [кредитных карточек](http://ru.wikipedia.org/w/index.php?title=%D0%9A%D1%80%D0%B5%D0%B4%D0%B8%D1%82%D0%BD%D1%8B%D0%B5_%D0%BA%D0%B0%D1%80%D1%82%D0%BE%D1%87%D0%BA%D0%B8&action=edit&redlink=1) и других банковских реквизитов ([фишинг](http://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3%22%20%5Co%20%22%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3)), так и распространение противоправной информации ([клеветы](http://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B5%D0%B2%D0%B5%D1%82%D0%B0), материалов [порнографического](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%80%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через [Интернет](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82), коммунальные объекты[[1]](http://ru.wikipedia.org/wiki/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD#cite_note-1).

Кроме того, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием Интернета, является [мошенничество](http://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE). Так, в письме [Федеральной комиссии по рынку ценных бумаг](http://ru.wikipedia.org/wiki/%D0%A4%D0%9A%D0%A6%D0%91) от 20 января 2000 г. N ИБ-02/229, указывается, что инвестирование денежных средств на иностранных фондовых рынках с использованием сети Интернет сопряжено с риском быть вовлеченными в различного рода мошеннические схемы

Другой пример мошенничества - [интернет-аукционы](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%B0%D1%83%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D1%8B%22%20%5Co%20%22%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%B0%D1%83%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D1%8B), в которых сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара.

В зарубежных государствах, в частности США, получили распространение аферы, связанные с продажей [доменных имен](http://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D1%8B%D0%B5_%D0%B8%D0%BC%D0%B5%D0%BD%D0%B0): производится массовая рассылка электронных сообщений, в которых, например, сообщают о попытках неизвестных лиц зарегистрировать доменные имена, похожие на адреса принадлежавших адресатам сайтов и владельцам сайтов предлагается зарегистрировать ненужное им доменное имя, чтобы опередить этих лиц. Так, вскоре после [терактов 11 сентября 2001 г.](http://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D1%80%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D0%B0%D0%BA%D1%82%D1%8B_11_%D1%81%D0%B5%D0%BD%D1%82%D1%8F%D0%B1%D1%80%D1%8F_2001_%D0%B3%D0%BE%D0%B4%D0%B0) Федеральная торговая комиссия США отметила факт массовой продажи доменных имен зоны "usa".

В соответствии с действующим [уголовным законодательством](http://ru.wikipedia.org/wiki/%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%BE%D0%B5_%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%BE%D0%B4%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE) [Российской Федерации](http://ru.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F) под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства[[*источник не указан 297 дней*]](http://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F%3A%D0%A1%D1%81%D1%8B%D0%BB%D0%BA%D0%B8_%D0%BD%D0%B0_%D0%B8%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B8).

Данная группа посягательств являются [институтом](http://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BF%D1%80%D0%B0%D0%B2%D0%B0) особенной части уголовного законодательства, [ответственность](http://ru.wikipedia.org/wiki/%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%B0%D1%8F_%D0%BE%D1%82%D0%B2%D0%B5%D1%82%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C) за их совершение предусмотрена гл. 28 УК РФ[[2]](http://ru.wikipedia.org/wiki/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD#cite_note-.D0.A3.D0.9A-2). В качестве самостоятельного института впервые выделен [УК РФ](http://ru.wikipedia.org/wiki/%D0%A3%D0%9A_%D0%A0%D0%A4) [1996 года](http://ru.wikipedia.org/wiki/1996_%D0%B3%D0%BE%D0%B4). и относится к субинституту «[Преступления против общественной безопасности и общественного порядка](http://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B2_%D0%BE%D0%B1%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D0%B8_%D0%BE%D0%B1%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BF%D0%BE%D1%80%D1%8F%D0%B4%D0%BA%D0%B0&action=edit&redlink=1)». Видовым[объектом](http://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%8A%D0%B5%D0%BA%D1%82_%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) рассматриваемых преступлений являются [общественные отношения](http://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B5_%D0%BE%D1%82%D0%BD%D0%BE%D1%88%D0%B5%D0%BD%D0%B8%D1%8F), связанные с безопасностью информации и систем обработки информации с помощью [ЭВМ](http://ru.wikipedia.org/wiki/%D0%AD%D0%92%D0%9C).

По [УК РФ](http://ru.wikipedia.org/wiki/%D0%A3%D0%9A_%D0%A0%D0%A4) преступлениями в сфере компьютерной информации являются: [неправомерный доступ к компьютерной информации](http://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%BC%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF_%D0%BA_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (ст. 272 УК РФ), Создание, использование и распространение вредоносных компьютерных программ] (ст. 273 УК РФ), [[Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей]] (ст. 274 УК РФ).

Общественная опасность противоправных действий в области [электронной техники](http://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D0%BA%D0%B0) и [информационных технологий](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8) выражается в том, что они могут повлечь за собой нарушение деятельности [автоматизированных систем управления](http://ru.wikipedia.org/w/index.php?title=%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F&action=edit&redlink=1) и контроля различных объектов, серьёзное нарушение работы [ЭВМ](http://ru.wikipedia.org/wiki/%D0%AD%D0%92%D0%9C) и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию [информации](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) и [информационных ресурсов](http://ru.wikipedia.org/w/index.php?title=%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B9_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81&action=edit&redlink=1), иные формы незаконного вмешательства в [информационные системы](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B), которые способны вызвать тяжкие и необратимые последствия, связанные не только с [имущественным ущербом](http://ru.wikipedia.org/wiki/%D0%98%D0%BC%D1%83%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D1%83%D1%89%D0%B5%D1%80%D0%B1), но и с [физическим вредом](http://ru.wikipedia.org/w/index.php?title=%D0%A4%D0%B8%D0%B7%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B2%D1%80%D0%B5%D0%B4&action=edit&redlink=1) людям.

[Неправомерный доступ к компьютерной информации](http://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%BC%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF_%D0%BA_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (ст. 272 УК РФ), а также [Создание, использование и распространение вредоносных компьютерных программ](http://ru.wikipedia.org/w/index.php?title=%D0%A1%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5,_%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B8_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B2%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D1%8B%D1%85_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC&action=edit&redlink=1) (ст. 273 УК РФ) совершаются только путём действий, в то время как [[Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей]] (ст. 274 УК РФ) — путём как действий, так и бездействием.

[Неправомерный доступ к компьютерной информации](http://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%BC%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF_%D0%BA_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) и [нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети](http://ru.wikipedia.org/w/index.php?title=%D0%9D%D0%B0%D1%80%D1%83%D1%88%D0%B5%D0%BD%D0%B8%D0%B5_%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D0%BB_%D1%8D%D0%BA%D1%81%D0%BF%D0%BB%D1%83%D0%B0%D1%82%D0%B0%D1%86%D0%B8%D0%B8_%D0%AD%D0%92%D0%9C,_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D0%AD%D0%92%D0%9C_%D0%B8%D0%BB%D0%B8_%D0%B8%D1%85_%D1%81%D0%B5%D1%82%D0%B8&action=edit&redlink=1) сформулированы как [преступления](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) с[материальным составом](http://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%81%D1%82%D0%B0%D0%B2_%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F), а [создание либо использование вредоносных программ для ЭВМ](http://ru.wikipedia.org/w/index.php?title=%D0%A1%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BB%D0%B8%D0%B1%D0%BE_%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B2%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC_%D0%B4%D0%BB%D1%8F_%D0%AD%D0%92%D0%9C&action=edit&redlink=1) — с [формальным](http://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%81%D1%82%D0%B0%D0%B2_%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F). В качестве последствий в ст. 272 и 274 УК указываются: уничтожение, модификация, блокирование либо копирование [информации](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F), нарушение работы [ЭВМ](http://ru.wikipedia.org/wiki/%D0%AD%D0%92%D0%9C) или системы ЭВМ, причинение существенного вреда и т. п.

В России борьбой с преступлениями в сфере информационных технологий занимается Управление "К" [МВД РФ](http://ru.wikipedia.org/wiki/%D0%9C%D0%92%D0%94_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8) и отделы "К" региональных управлений внутренних дел,входящие в состав Бюро специальных технических мероприятий МВД РФ.

## Уголовная ответственность в сфере компьютерной информации за рубежом

### Германия

В Германии к преступлениям в сфере оборота компьютерной информации относятся: - действия лиц, неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом (§ 202а); - нарушение тайны телекоммуникационной связи (§ 206); - действия лиц, учиняющих подделку или использующих поддельные технические записи, под которыми, в числе иного, понимаются данные, полностью или частично регистрируемые автоматическими устройствами (§ 268); - аналогичная подделка данных, имеющих доказательственное значение (§ 269); - действия лиц, уничтожающих, изменяющих или утаивающих технические записи (§ 274); - действия лиц, противоправно аннулирующих, уничтожающих, приводящих в негодность или изменяющих данные (§ 303а); - действия лиц, нарушающих обработку данных путем разрушения, повреждения, приведения в негодность установки для обработки данных или носителей информации (§ 303b). - незаконное вмешательство в деятельность телекоммуникационных установок (§ 317).

Кроме того, германское законодательство устанавливает уголовную ответственность за компьютерное мошенничество, под которым понимается умышленное деяние с намерением получить для себя или третьих лиц имущественную выгоду, заключающееся в причинении вреда чужому имуществу путем воздействия на результат обработки данных путем неправильного создания программ, использования неправильных или данных, неправомочного использования данных или иного воздействия на результат обработки данных (§ 263а).

### Люксембург[[править](http://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B2_%D1%81%D1%84%D0%B5%D1%80%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9&veaction=edit&section=4) | [править исходный текст](http://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B2_%D1%81%D1%84%D0%B5%D1%80%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9&action=edit&section=4)]

Нормы о киберпреступлениях содержатся в ст. ст. 509-1, 509-2, 509-3, 524 УК Люксембурга.

Статья 509-1 УК Люксембурга предусматривает ответственность за неправомочный доступ к системе или части системы обработки данных и незаконное пребывание в такой системе. Санкция за это преступление предусмотрена в виде штрафа или заключения на срок от 2 месяцев до года. Если указанные действия повлекли изменение или уничтожение данных, содержащихся в системе, то верхний предел срока заключения увеличивается до 2 лет.

Статья 509-2 запрещает преднамеренное затруднение или изменение функционирования системы автоматической обработки данных. Наказание – штраф или лишение свободы на срок от 3 месяцев до 3 лет.

Статья 509-3 направлена на охрану целостности и качества данных. Она устанавливает, что лицо, умышленно и без надлежащих полномочий вводящее данные в электронную систему их обработки, удаляющее или изменяющее данные, находящиеся в этой системе, изменяющее действие системы или способ передачи данных, подлежит уголовной ответственности (штраф или заключение на срок от 3 месяцев до 3 лет). Согласно ст. 524 УК Люксембурга, любое вмешательство в телекоммуникации является преступлением, за которое лицо может быть подвергнуто штрафу или заключению от 1 месяца до 3 лет.

## Международное сотрудничество

Преступления в сфере информационных технологий очень часто являются международными, то есть преступники действуют в одном государстве, а их жертвы находятся в другом государстве. Поэтому для борьбы с такими преступлениями особое значение имеет международное сотрудничество.

Конвенция [Совета Европы](http://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%B2%D0%B5%D1%82_%D0%95%D0%B2%D1%80%D0%BE%D0%BF%D1%8B) о преступности в сфере компьютерной информации ETS N 185 была подписана 23 ноября 2001 г. в [Будапеште](http://ru.wikipedia.org/wiki/%D0%91%D1%83%D0%B4%D0%B0%D0%BF%D0%B5%D1%88%D1%82). Она открыта для подписания как государствами - членами Совета Европы, так и не являющимися его членами государствами, которые участвовали в ее разработке. В частности, ее подписали США и Япония. Россия на настоящий момент не подписала Конвенцию[[3]](http://ru.wikipedia.org/wiki/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD_%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD#cite_note-3).

Конвенция Совета Европы о киберпреступности подразделяет преступления в киберпространстве на четыре группы.

* В первую группу преступлений, направленных против конфиденциальности, целостности и доступности компьютерных данных и систем, входят: незаконный доступ (ст. 2), незаконный перехват (ст. 3), воздействие на компьютерные данные (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных) (ст. 4) или системы (ст. 5). Также в эту группу преступлений входит противозаконное использование специальных технических устройств (ст. 6) - компьютерных программ, разработанных или адаптированных для совершения преступлений, предусмотренных в ст. 2 - 5, а также компьютерных паролей, кодов доступа, их аналогов, посредством которых может быть получен доступ к компьютерной системе в целом или любой ее части). Нормы ст. 6 применимы только в том случае, если использование (распространение) специальных технических устройств направлено на совершение противоправных деяний.
* Во вторую группу входят преступления, связанные с использованием компьютерных средств. К ним относятся подлог и мошенничество с использованием компьютерных технологий (ст. 7 - 8). Подлог с использованием компьютерных технологий включает в себя злонамеренные и противоправные ввод, изменение, удаление или блокирование компьютерных данных, влекущие за собой нарушение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных.
* Третью группу составляет производство (с целью распространения через компьютерную систему), предложение и (или) предоставление в пользование, распространение и приобретение [детской порнографии](http://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%82%D1%81%D0%BA%D0%B0%D1%8F_%D0%BF%D0%BE%D1%80%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F), а также владении детской порнографией, находящейся в памяти компьютера (ст. 9).
* Четвертую группу составляют преступления, связанные с нарушением [авторского права](http://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D1%81%D0%BA%D0%BE%D0%B5_%D0%BF%D1%80%D0%B0%D0%B2%D0%BE) и смежных прав.

Согласно Конвенции каждое государство-участник обязано создать необходимые правовые условия для предоставления следующих прав и обязанностей компетентным органам по борьбе с киберпреступностью: выемка компьютерной системы, ее части или носителей; изготовление и конфискация копий компьютерных данных; обеспечение целостности и сохранности хранимых компьютерных данных, относящихся к делу; уничтожение или блокирование компьютерных данных, находящихся в компьютерной системе.

Конвенция также требует создать необходимые правовые условия для обязания Интернет-провайдеров проводить сбор и фиксацию или перехват необходимой информации с помощью имеющихся технических средств, а также способствовать в этом правоохранительным органам. При этом рекомендуется обязать провайдеров сохранять полную конфиденциальность о фактах подобного сотрудничества.

В начале 2002 г. был принят Протокол N 1 к Конвенции о киберпреступности, добавляющий в перечень преступлений распространение информации расистского и другого характера, подстрекающего к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающегося на расовой, национальной, религиозной или этнической принадлежности.

## Критика Конвенции о киберпреступности

Ряд общественных организаций подписались под совместным протестом против принятия вышеуказанной Конвенции. В их число вошли международная организация [Internet Society](http://ru.wikipedia.org/wiki/Internet_Society%22%20%5Co%20%22Internet%20Society), организации [Electronic Frontier Foundation](http://ru.wikipedia.org/wiki/Electronic_Frontier_Foundation%22%20%5Co%20%22Electronic%20Frontier%20Foundation) (США), [Cyber-Rights & Cyber-Liberties](http://ru.wikipedia.org/w/index.php?title=Cyber-Rights_%26_Cyber-Liberties&action=edit&redlink=1" \o "Cyber-Rights & Cyber-Liberties (страница отсутствует)) (Великобритания), [Kriptopolis](http://ru.wikipedia.org/w/index.php?title=Kriptopolis&action=edit&redlink=1" \o "Kriptopolis (страница отсутствует)) (Испания) и другие. Авторы обращения возражают против положений, требующих от провайдеров Интернета вести записи о деятельности их клиентов. Во введении ответственности провайдеров за содержание информации авторы усматривают "бессмысленную обузу, которая поощряет слежку за частными коммуникациями". В обращении отмечается также, что положение об обеспечении государственных органов шифровальными ключами может стать основанием для свидетельствования пользователей против самих себя, что противоречит статье 4 [Европейской конвенции о защите прав человека](http://ru.wikipedia.org/w/index.php?title=%D0%95%D0%B2%D1%80%D0%BE%D0%BF%D0%B5%D0%B9%D1%81%D0%BA%D0%B0%D1%8F_%D0%BA%D0%BE%D0%BD%D0%B2%D0%B5%D0%BD%D1%86%D0%B8%D1%8F_%D0%BE_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5_%D0%BF%D1%80%D0%B0%D0%B2_%D1%87%D0%B5%D0%BB%D0%BE%D0%B2%D0%B5%D0%BA%D0%B0&action=edit&redlink=1).

Общественность, кроме того, выступает против того, что за нарушение авторских прав должна непременно следовать уголовная ответственность.

1. **Виртуальная преступность в Тульской области**

(автор [***Рагим Мусаев***](http://www.proza.ru/avtor/ragim))

        Удивительно, но факт: какие-то пятнадцать – двадцать лет назад мы вполне обходились без сотовой связи, компьютеров и Интернета. Сегодня мобильники есть даже у дошкольников, а виртуальный мир заменил многим мир реальный. В сети ведется деловая переписка, заключаются договоры, проводятся банковские операции, оказываются государственные услуги. Естественно, что в таких условиях внедрение новейших информационных технологий и развитие телекоммуникационных систем не прихоть, а одна из основных государственных задач, реализуемая под личным контролем Президента Российской Федерации.

В виртуальном мире и преступность виртуальная, таящаяся под вымышленными именами – «никами», помогающими остаться неузнанными лучше любой шапки-невидимки. Да и следы в сети удаляются порой одним нажатием клавиши. Не мудрено, что расследовать такие преступления способны только следователи принципиально новой формации.
        Идя в ногу со временем, начальник СУ УМВД России по Тульской области Лопушанский И.Б. принял решение о создании в следственной части областного Следственного управления первого в стране отдела по расследованию организованной преступной деятельности в сфере высоких технологий и интеллектуальной собственности, наделив его исключительным правом расследования всех уголовных дел этой категории в Тульской области.
        Возглавить вновь созданное подразделение поручили полковнику юстиции Елене Анатольевне Инкиной. Коллеги характеризуют ее коротко: «Много в полиции женщин-полковников?» За ее плечами почти двадцать лет добросовестной работы, на ее счету сотни расследованных и направленных в суд сложных дел. В 2007 году Е.А.Инкина была награждена медалью ордена «За заслуги перед Отечеством» II степени.

Началось все в 1994 году. Елену Анатольевну называют в управлении первооткрывателем. Когда налоговые преступления после расформирования налоговой службы передали в органы внутренних дел, в СУ создали новый отдел, который возглавила Инкина. Они столкнулись сразу с рядом проблем. Во-первых, для проведения расследования необходимо было знать не только уголовный, но и налоговый кодексы. Во-вторых, в отличие от общеуголовных, такие преступления нужно было научиться как доказывать, так и выявлять. Быстро наработали практику и смогли поднять это направление на высокий уровень – 2 место по ЦФО и 3 по России, передавали опыт коллегам из других регионов.

Для нового отдела подбирали следователей опытных и коммуникабельных, способных найти общий язык и с оперативниками, и с участниками процесса. Следователям предстояло поставить на поток выявление, документирование и расследование преступлений, до сих пор считающихся многими редкими.

Елена Анатольевна Инкина для начала села за парту вместе со своими следователями. Рядом усадили и оперативных сотрудников, ведь не секрет, что без налаженного взаимодействия эффективной работы не видать.
        Прежде всего, проводили практические занятия по документированию конкретных преступлений, совершенных с использованием сетей Интернет и интранет, программ Internet Explorer, и иных браузеров, связанных с работой провайдеров и хостеров. Следователям предстояло не просто познакомиться с непривычными терминами, а перейти с ними на «ты».
        Проблемой стало и почти полное отсутствие судебно-следственной практики. Учась на собственных ошибках расследовали, к примеру, первые дела о неправомерном доступе к компьютерной информации.
        Сегодня это одно из самых латентных преступлений. Жертвы могут и не подозревать, что перебои в работе Интернета связаны вовсе не с качеством услуг провайдера. С помощью специальной программы-шпиона преступник узнает и модифицирует охраняемые законом персональные данные пользователей сети и использует оплаченный ими трафик в своих целях. Хорошо, если эти цели не вредят общественной безопасности. Ведь компьютерные программы управляют движением поездов и самолетов, работой огромных предприятий и объектов жизнеобеспечения. От такого преступления не застрахованы ни физические, ни юридические лица.
        Сотрудники отдела «К» и ФСБ помогают установить IP-адреса преступников, однако этого недостаточно. Задача следователя - доказать, что через этот адрес процессами в виртуальном мире управлял реальный человек. Только после выработки такого механизма скепсис прокуроров и судей сменился уверенностью, и суды Тульской области начали выносить обвинительные приговоры по все еще редкому в России преступлению, предусмотренному статьей 272 УК РФ.
Еще одна удача отдела – наработка практики реализации результатов оперативных разработок по фактам распространения в Интернете порнографических материалов с изображением малолетних, способствующих распространению педофилии. По всем делам данной категории преступники не только были осуждены, но и получили реальные сроки лишения свободы.
        В том числе в 2011 году суд приговорил к 3 годам колонии общего режима Мишуру Р.А., который с февраля 2010 по июнь 2011 года систематически распространял через локальную файлообменную сеть одного из Интернет-провайдеров порнографические изображения несовершеннолетних. Преступник в открытую говорил следователю не только о том, что ему нравится смотреть порноролики с детьми, но и о том, что он бы с удовольствием воплотил увиденное на экране в жизнь, вот только случая пока не представилось.
В 2012 году суд вынес приговор в отношении членов организованной группы, распространявших порнографические видеозаписи с участием младенцев и животных. Следователям удалось установить любителей специфического видео в нескольких десятках регионах страны.
        Преступления в сфере высоких технологий неразрывно связаны с нарушением авторских прав. В большинстве они связаны с распространением пиратских дисков с фильмами, реже – с программными продуктами. Выявление, документирование и расследование этих преступлений имеет свои сложности, поэтому такие уголовные дела не всегда доходят до суда. Успешная работа специализированного отдела разрушила в Тульской области этот стереотип, доказав, что дела, которым раньше не придавали значения, могут влиять на ситуацию в обществе.
        В 2012 году суд вынес обвинительный приговор по делу об одном из крупнейших в России области изъятии контрафактных дисков. В результате внезапной операции, проведенной в выходной день одновременно в 15 сетевых магазинах Тулы и области, 50 следователей, экспертов и сотрудников отдела «К» изъяли более 130 000 дисков с нелицензионными программными продуктами.
Прослушивание телефонных разговоров членов организованной группы позволило установить склад на окраине Тулы, где на специальном оборудовании обычные DVD-болванки превращали в «лицензионные». Обыски длились почти сутки. На упаковку фальшивок ушло более 1000 мешков.
        Один только осмотр изъятого растянулся на месяцы. При этом выяснилась неприятная деталь: постоянный контакт с дисками, представляющими собой результат деятельности химической промышленности, не полезен для здоровья. Поэтому работать следователям пришлось в перчатках и респираторах.
        Ущерб корпорациям Microsoft, Corel и Autodesk Incorporated составил более 45 миллионов рублей. Так, рыночная стоимость только 1 лицензионного диска со всем знакомой операционной системой Microsoft Windows XP Professional составляет 12 тысяч рублей, стоимость 1 лицензионного диска профессиональной графики для дизайнеров Corel DESIGNER Technical Suite X4 – 38 тысяч рублей, 1 лицензионного диска для проектирования и строительства Autodesk 3ds Max 2010 - 135 тысяч рублей.
        Членам организованной группы предъявили обвинение в совершении незаконного использования объектов авторского права в особо крупном размере. Контрафакт традиционно уничтожили на Косогорском металлургическом заводе. Эффектное зрелище заливки пиратской продукции раскаленным до 3000 градусов шлаком собрало толпу журналистов.
        Средства массовой информации широко освещали весь ход расследования этого и других дел отдела. Успешная работа, систематически освещаемая прессой, привела к закрытию в Тульской области ряда крупных магазинов, торговавших поддельными дисками.
               Очевидно, что проводимое под контролем Президента Российской Федерации дальнейшее внедрение новейших информационных технологий, приведет к увеличению количества и появлению новых видов преступлений в сфере высоких технологий. Поэтому работа тульских следователей по противодействию виртуальной преступности - это серьезный шаг на пути в безопасное и законопослушное будущее Интернета.