

**ПРАВОВЫЕ НОРМЫ,
ОТНОСЯЩИЕСЯ К ИНФОРМАЦИИ,
ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ
СФЕРЕ, МЕРЫ ИХ ПРЕДУПРЕЖДЕНИЯ.
ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО**

Информация является объектом правового регулирования. Информация не является материальным объектом, но она фиксируется на материальных носителях.



Принимая во внимание, что информация практически ничем не отличается от другого объекта собственности, например машины, дома, мебели и прочих материальных продуктов, следует говорить о наличии подобных же прав собственности и на информационные продукты.

**Право
собственности**

право
распоряжени

право
владения

право
пользования

я

- **Право распоряжения** состоит в том, что только субъект-владелец информации имеет право определять, кому эта информация может быть предоставлена.
- **Право владения** должно обеспечивать субъекту-владельцу информации хранение информации в неизменном виде. Никто, кроме него, не может ее изменять.
- **Право пользования** предоставляет субъекту-владельцу информации право ее использования только в своих интересах.

Любой субъект-пользователь
обязан приобрести эти права,
прежде чем воспользоваться
интересующим его информационным
продуктом



Любой закон о праве собственности регулирует отношения между субъектом-владельцем и субъектом-пользователем.

Законы должны защищать как права **собственника**, так и права **законных владельцев**, которые приобрели информационный продукт законным путем.

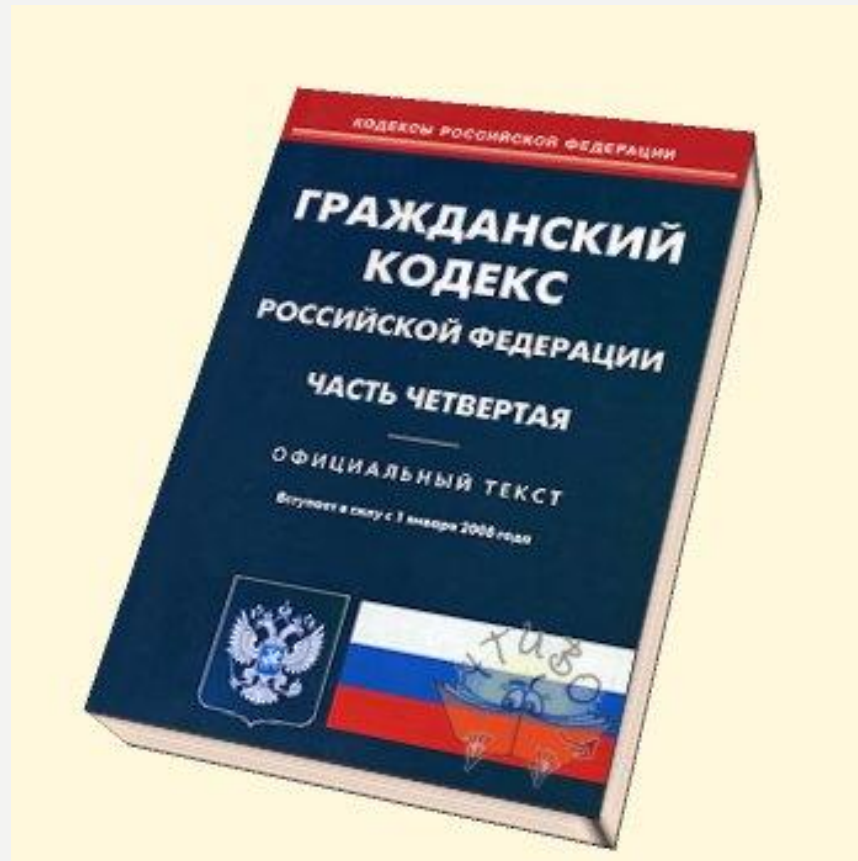
ПРАВОВЫЕ НОРМЫ, ОТНОСЯЩИЕСЯ К ИНФОРМАЦИИ

Нормативно-правовую основу необходимых мер составляют юридические документы: законы, указы, постановления, которые обеспечивают цивилизованные отношения на информационном рынке

Законодательство Российской Федерации об авторском праве и смежных правах основывается на **Конституции Российской Федерации** и состоит из:

- Гражданского кодекса Российской Федерации,
- Закона Российской Федерации от 23 сентября 1992 г. N 3523-1 "О правовой охране программ для электронных вычислительных машин и баз данных",
- федеральных законов.

Действующие нормы об авторском праве и смежных правах содержатся в главах 70 - 71 части четвертой Гражданского кодекса РФ



"Об информации, информационных технологиях и защите информации" №149-ФЗ от 27.07.2006г.

Регулирует отношение, возникающее при :

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Уголовный кодекс Глава 28 раздел
"Преступления в сфере компьютерной
информации" определяет меру наказания за
"Компьютерные преступления":

- неправомерный доступ к компьютерной информации
- создание, использование и распространение вредоносных программ для ЭВМ
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

"О персональных данных" №152-ФЗ от
27.07.2006г.

Его целью является обеспечить защиту прав и свобод человека и гражданина при обработке его персональных данных и обеспечить право на защиту частной жизни.

Конвенция о преступности в сфере компьютерной информации (ets n 185) (будапешт, 23 ноября 2001 года)

Дала классификацию компьютерным преступлениям, рассмотрела меры по предупреждению компьютерных преступлений, заключила согласие на обмен информацией между странами Европы по компьютерным преступлениям.

Федеральный закон от 06.04.2011 N 63-ФЗ
«Об электронной подписи»



Федеральный закон от 29.12.2010 N 436-ФЗ
«О защите детей от информации, причиняющей
вред их здоровью и развитию»



ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

Правонарушение — виновное противоправное деяние (действие или бездействие), противоречащее требованиям правовых норм и совершенное правоспособным лицом или лицами.

Влечет за собой
юридическую
ответственность



ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ВКЛЮЧАЮТ:

- распространение вредоносных вирусов;
- взлом паролей;
- кражу номеров кредитных карточек и других банковских реквизитов (фишинг);
- распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет

ОСНОВНЫЕ ВИДЫ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ВМЕШАТЕЛЬСТВОМ В РАБОТУ КОМПЬЮТЕРОВ:

1. Несанкционированный доступ к информации, хранящейся в компьютере



2. ВВОД В ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«ЛОГИЧЕСКИХ БОМБ», КОТОРЫЕ
СРАБАТЫВАЮТ ПРИ ВЫПОЛНЕНИИ
ОПРЕДЕЛЁННЫХ УСЛОВИЙ И ЧАСТИЧНО ИЛИ
ПОЛНОСТЬЮ ВЫВОДЯТ ИЗ СТРОЯ
КОМПЬЮТЕРНУЮ СИСТЕМУ



3. РАЗРАБОТКА И РАСПРОСТРАНЕНИЕ



4. ПРЕСТУПНАЯ НЕБРЕЖНОСТЬ В
РАЗРАБОТКЕ, ИЗГОТОВЛЕНИИ И
ЭКСПЛУАТАЦИИ ПРОГРАММНО-
ВЫЧИСЛИТЕЛЬНЫХ КОМПЛЕКСОВ,
ПРИВЕДШАЯ К ТЯЖКИМ
ПОСЛЕДСТВИЯМ



5. ПОДДЕЛКА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ



6. ХИЩЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ



МЕРЫ ПО ПРЕДУПРЕЖДЕНИЮ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

```
graph TD; A[МЕРЫ ПО ПРЕДУПРЕЖДЕНИЮ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ] --- B[технические]; A --- C[организационные]; A --- D[правовые]
```

технические

организационные

правовые

К ТЕХНИЧЕСКИМ МЕРАМ ОТНОСЯТ:

- защиту от несанкционированного доступа к системе,
- резервирование особо важных компьютерных подсистем,
- организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев,
- установку оборудования обнаружения и тушения пожара,
- оборудования обнаружения воды,
- принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания,
- оснащение помещений замками, установку сигнализации и многое другое.

К ОРГАНИЗАЦИОННЫМ МЕРАМ ОТНОСЯТ:

- охрану вычислительного центра,
- тщательный подбор персонала,
- исключение случаев ведения особо важных работ только одним человеком,
- наличие плана восстановления работоспособности центра после выхода его из строя,
- организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра,
- универсальность средств защиты от всех пользователей (включая высшее руководство),
- возложение ответственности на лиц, которые должны обеспечить безопасность центра.

К ПРАВОВЫМ МЕРАМ ОТНОСЯТ:

- разработку норм, устанавливающих ответственность за компьютерные преступления,
- защита авторских прав программистов,
- совершенствование уголовного, гражданского законодательства и судопроизводства.
- общественный контроль за разработчиками компьютерных систем и принятие международных договоров об ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение.

РЕЗУЛЬТАТЫ ОПРОСА ПРЕДСТАВИТЕЛЕЙ СЛУЖБ БЕЗОПАСНОСТИ 492 КОМПАНИЙ, ДАЕТ ПРЕДСТАВЛЕНИЕ О НАИБОЛЕЕ ОПАСНЫХ СПОСОБАХ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ.

Виды атак, выявленные за последние 12 месяцев :

- Вирус 83%
- Злоупотребление сотрудниками компании доступом к Internet 69%
- Кража мобильных компьютеров 58%
- Неавторизованный доступ со стороны сотрудников компании 40%
- Мошенничество при передаче средствами телекоммуникаций 27%
- Кража внутренней информации 21%
- Проникновение в систему 20%

Допускалось несколько вариантов ответов.

ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО

Электронное правительство - «способ предоставления информации и оказания уже сформировавшегося набора государственных услуг гражданам, бизнесу, другим ветвям государственной власти и государственным чиновникам, при котором личное взаимодействие между государством и заявителем минимизировано и максимально возможно используются информационные технологии».

В рамках этой мировой тенденции в начале XXI века в нашей стране также была разработана целевая программа «Электронная Россия», принятая постановлением Правительства РФ от 28.01.2002 г. № 65 «О Федеральной целевой программе «Электронная Россия (2002–2010 годы)».