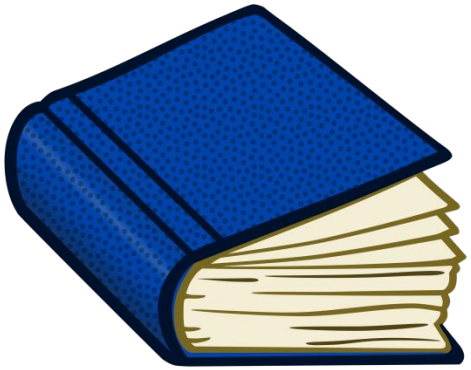
Государственное автономное профессиональное образовательное учреждение Самарской области
«Колледж технического и художественного образования г. Тольятти»

# Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предупреждения.

# Содержание

1. Информация как объект правового регулирования
2. Правонарушения в информационной сфере
3. Правовые нормы правового регулирования информации
4. Предупреждение компьютерных преступлений

**1. Информация** является **объектом правового регулирования**. Информация не является материальным объектом, но она фиксируется на материальных носителях: книгах, дисках и др.

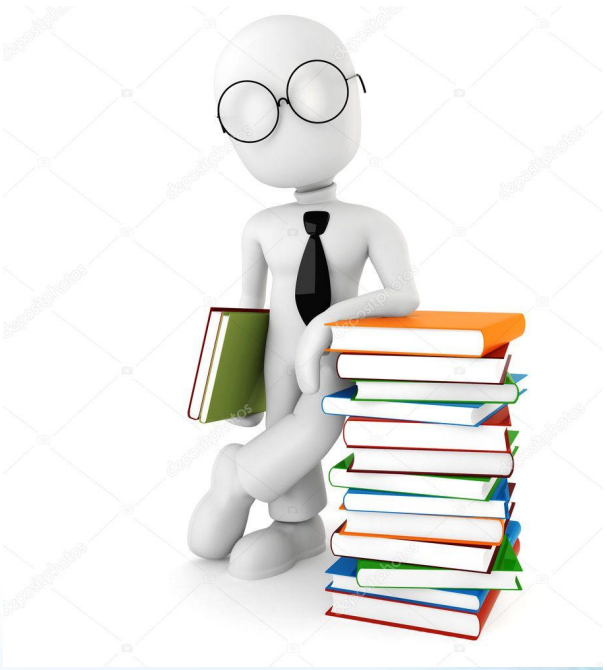




**Информация практически ничем не отличается от другого объекта собственности** (например машины, дома, мебели и прочих материальных продуктов), поэтому **следует говорить о наличии подобных же прав собственности и на информационные продукты**

# Право собственности

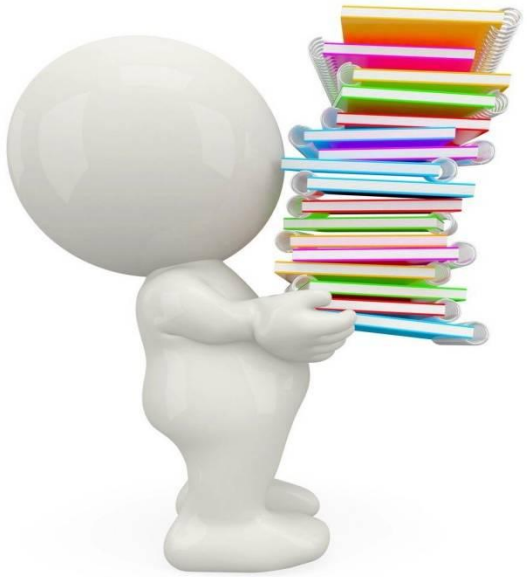
- право распоряжения
- право владения
- право пользования



- **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 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.



# 2. Правонарушения в информационной сфере

**Под правонарушением обычно понимается противоправное виновное нарушение субъектом действующей нормы информационного права (ИП), в результате чего наносится существенный вред интересам личности, государства, общества в информационной сфере.**

# Преступления в сфере информационных технологий

- распространение вредоносных вирусов;
- взлом паролей;
- кража номеров кредитных карточек и других банковских реквизитов (фишинг);
- распространение противоправной информации (клеветы, 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. Разработка и распространение компьютерных вирусов
3. Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определённых условий и частично или полностью выводят из строя компьютерную систему
4. Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям
5. Подделка компьютерной информации
6. Хищение компьютерной информации

# 3. Правовые нормы, относящиеся к информации

**1) "Об информации, информационных технологиях и защите информации" № 149-ФЗ от 27.07.2006 г.**
**2) Уголовный кодекс РФ раздел "Преступления в сфере компьютерной информации" № 63-ФЗ от 1996 г. (глава 28, статьи 272, 273, 274, 274.1)**
**3) Федеральный закон "О персональных данных" №152-ФЗ от 27.07.2006 г.**
**4) «Конвенция о преступности в сфере компьютерной информации», подписана в Будапеште № ETS 185 от 23.10.2001 г.**
**5) Федеральный закон "Об электронной подписи" от 06.04.2011 г. N 63-ФЗ.**
**6) Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".**

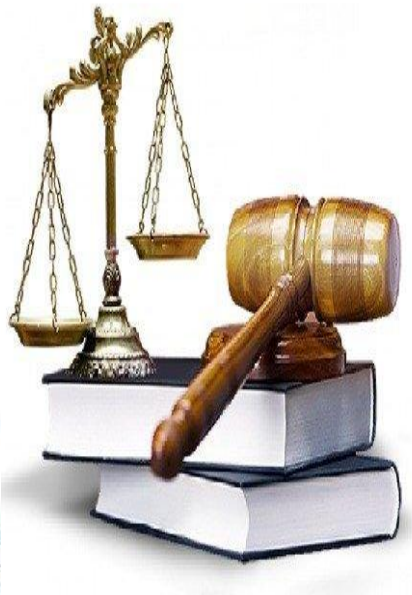



# 4. Меры по предупреждению компьютерных преступлений

**ТЕХНИЧЕСКИЕ**

**ОРГАНИЗАЦИОННЫЕ**


**ПРАВОВЫЕ**



# Технические меры

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

# Организационные меры

- охрана вычислительного центра,
- тщательный подбор персонала,
- исключение случаев ведения особо важных работ только одним человеком,
- наличие плана восстановления работоспособности центра после выхода его из строя,
- организация 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.

# Правовые меры

- разработка 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.

# СПАСИБО ЗА ВНИМАНИЕ!