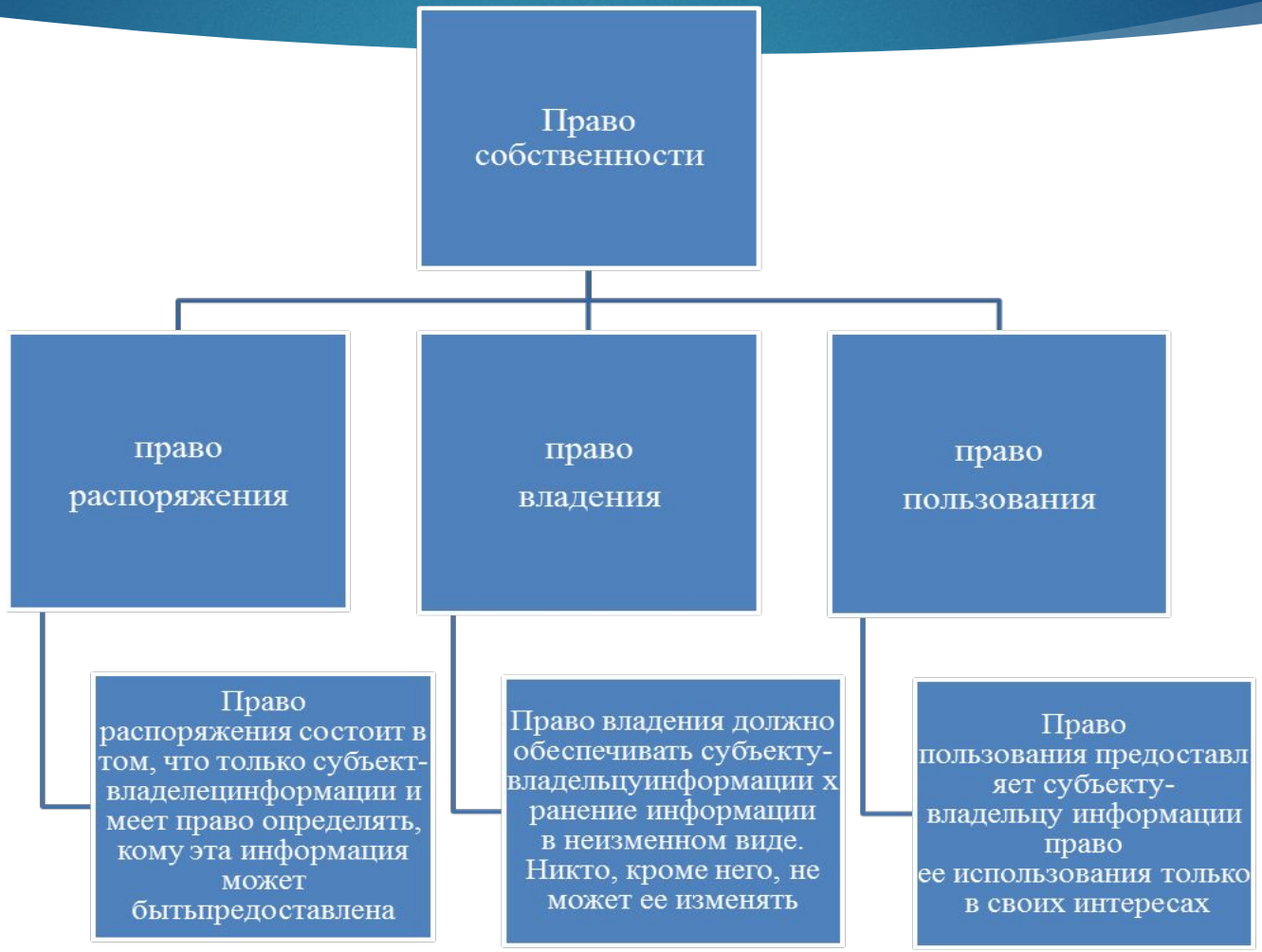
Правовые нормы использования информации и меры их предупреждения

Правовые нормы использования информации

- Информация является объектом правового регулирования. Информация не является материальным объектом, но она фиксируется на материальных носителях.
- Информация практически ничем не отличается от другого объекта собственности, например машины, дома, мебели и прочих материальных продуктов, поэтому следует говорить о наличии подобных прав собственности и на информационные продукты.

Правовые нормы использования информации



Правовые нормы использования информации

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

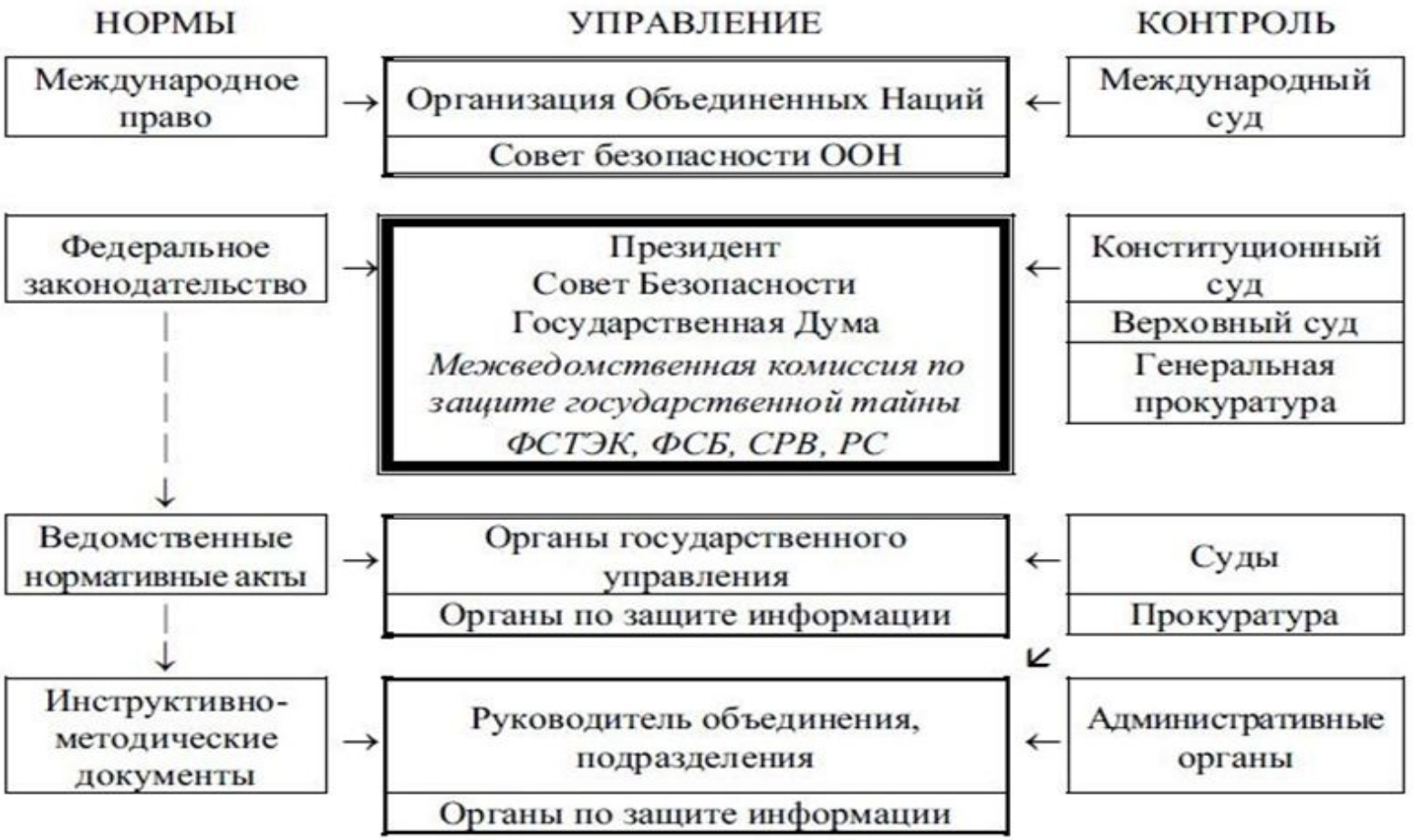
Правовые нормы правового регулирования информации

- **«Об информации, информационных технологиях и защите информации» №149-ФЗ от 27.07.2006г.** *(Регулирует отношение, возникающее при осуществление права: поиск, получение, передачу и производство информации. Применение информационных технологий. обеспечение защиты информации.)*
- **Уголовный кодекс раздел «Преступления в сфере компьютерной информации» № 63-ФЗ Дата принятия: 1996г.** *(Определяет меру наказания за «Компьютерные преступления». Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ для ЭВМ. Нарушение правил эксплуатации ЭВМ или сети.)*
- **«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.)*

Правовые нормы правового регулирования информации

- **Конвенция Совета Европы о преступности в сфере компьютерной информации была подписана в Будапеште. №ETS 185 от 23.10.2001г.** *(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»**

Структура государственной системы информационной безопасности



Правонарушения в информационной сфере

- **Правонарушение** – юридический факт (наряду с событием и действием), действия, противоречащие нормам права (антипод правомерному поведению).
- Правонарушения всегда связаны с нарушением определенным лицом (лицами) действующей нормы (норм) ИП и прав других субъектов информационных правоотношений. При этом эти нарушения являются общественно опасными и могут влечь для тех или иных субъектов трудности, дополнительные права и обязанности.

Преступления в сфере информационных технологий:

- 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 *(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)*.
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.
5. Подделка компьютерной информации.
6. Хищение компьютерной информации.

Предупреждение компьютерных преступлений

- Организационные меры
- Юридические меры
- Программно-технические меры

Организационные меры:

- повышение квалификации персонала;
- контролируемые каналы распространения информации;
- разделение прав доступа, уничтожение ненужных копий документов;
- соблюдение коммерческой тайны персоналом;
- 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 обеспечивать безопасность центра.

Юридические 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.

Юридические меры:

- Закон «О правовой охране программ для ЭВМ и баз данных»;
- Закон «Об авторском праве и смежных правах».

Уголовный Кодекс содержит статьи:

- ст. 272 «О неправомерном доступе к компьютерной информации»;
- ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ»;
- ст. 274 «Нарушение правил эксплуатации ЭВМ, систем ЭВМ или сети ЭВМ».

Программно-технические меры:

- защита от компьютерных вирусов;
- шифрование данных;
- резервное копирование данных;
- ограничение доступа к устройствам и файловой системе;
- контроль трафика с помощью межсетевых экранов (брандмауэров);
- 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 для обнаружения и тушения пожара, оборудования для обнаружения воды;
- принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установка резервных систем электропитания;
- оснащение помещений замками, установку сигнализации и многое другое.

Наивысшая угроза

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%.

Контрольные вопросы

1. Какие нормативные правовые акты являются основополагающими в информационной сфере?
2. Что является основанием для возникновения юридической ответственности за правонарушение
3. Сформулируйте определение «информационное правонарушение» или «правонарушение в информационной сфере».
4. Какие виды юридической ответственности предусмотрены за несоблюдение информационно-правовых норм?
5. Что понимается под информационным преступлением?
6. Какие составы преступлений в сфере экономики можно отнести к информационным?
7. Какие составы преступлений против общественной безопасности и общественного порядка следует отнести к информационным?

Практическая работа

Задание №1. Найти в Интернет закон РФ «Об информации, информатизации и защите информации» и выделить определения понятий:

информация	
информационные технологии	
информационно-телекоммуникационная сеть	
доступ к информации	
конфиденциальность информации	
электронное сообщение	
документированная информация	

Практическая работа

Задание №2. Изучив источник «Пользовательское соглашение» Яндекс ответьте на следующие вопросы:

Вопрос	Ответ
По какому адресу находится страница с пользовательским соглашением Яндекс?	
В каких случаях Яндекс имеет право отказать пользователю в использовании своих служб?	
Каким образом Яндекс следит за операциями пользователей?	
Что подразумевается под термином «контент» в ПС?	
Что в ПС сказано о запрете публикации материалов, связанных с: нарушением авторских прав и дискриминацией людей; рассылкой спама; обращением с животными; размещением и пропагандой порнографии	
Какого максимального объема могут быть файлы и архивы, размещаемые пользователями при использовании службы бесплатного хостинга?	
Ваш почтовый ящик на Почте Яндекса будет удален, если Вы не пользовались им более	

Практическая работа

Задание №3. Изучив программное обеспечение компьютера, за которым Вы работаете, заполните список:

- Перечень программ Microsoft Office:

_____

_____

_____

- Перечень стандартных программ:

_____

_____

_____

Домашняя работа

- Подготовить сообщение на тему **«Информационное общество нашего времени».**