Информатика, право, общество и Интернет

Темы курса:

- Правовая информация, система и информатика.
- Информационная безопасность.
- Информатизация и глобализация общества.
- Электронное правительство.
- Право и Интернет.
- Информационно-правовые системы.

Правовая информация – информация, отражающая, передающая, увеличивающая правовые знания, умения и навыки человека, общества.

Основные свойства правовой информации:

- «Неуменьшаемость»;
- Субъективность;
- Объективность;
- Неотчуждаемость;
- Обособляемость;
- Актуальность;
- Определенность;
- Корректность;
- Достоверность;
- Направленность;
- Конфиденциальность;
- Значимость;
- Массовость;
- Сжатость, лаконичность;
- Защищенность и помехоустойчивость;
- Доступность;
- Необходимость.

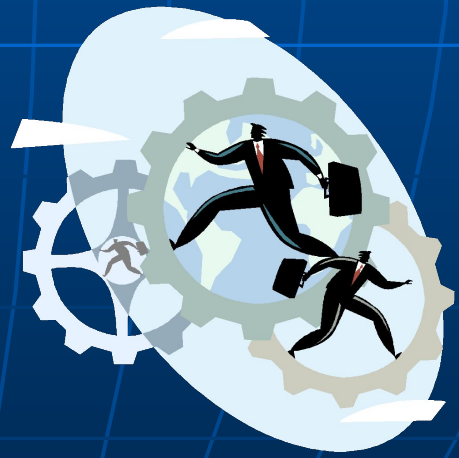
Информация:

- Личностная
- Общественная
- Корпоративная
- Государственная

Правовая система – система правовых идей, норм, явлений и процессов, возникающая и развиваемая в результате их взаимодействий в правовые институты, характеризующая эффективное правовое воздействие на личное и общественное сознание, поведение, воспитание.

Правовая система имеет четыре основные подсистемы:

1) правообразование;
2) правопонимание;
3) правоприменение;
4) правореализация.



Методы получения и актуализации информации в правовых системах:

- Наблюдение
- Сравнение
- Измерение
- Эксперимент
- Опрос, интервью
- Тестирование или испытание
- Анализ
- Синтез
- Композиция
- Декомпозиция
- Индукция
- Дедукция
- Моделирование (простое), использование приборов
- Исторический метод
- Логический метод
- Визуализация
- Мониторинг
- Деловые игры и ситуации
- Экспертные оценки
- Группировка и классификация
- Систематизация
- Эвристики

Правовая информация, система и информатика

Правовая информатика – наука, изучающая информацию, информационные процессы, технологии и системы в сфере права, а также правовые аспекты и особенности информационных процессов и систем.

Предметная область правовой информатики – информационные процессы, системы в области права, системы и языки их описаний, технологии их актуализации.

Мировоззренческая роль правовой информатики состоит, в частности, в том, что она помогает вникать в информационную суть правовых процессов и явлений, выявляет, описывает и исследует такие процессы и явления.

Воспитательная роль правовой информатики состоит, в частности, в развитии творчества, алгоритмического мышления, логичности и строгости суждений, умения выделять главное и игнорировать второстепенное, использовать информационные технологии и др.

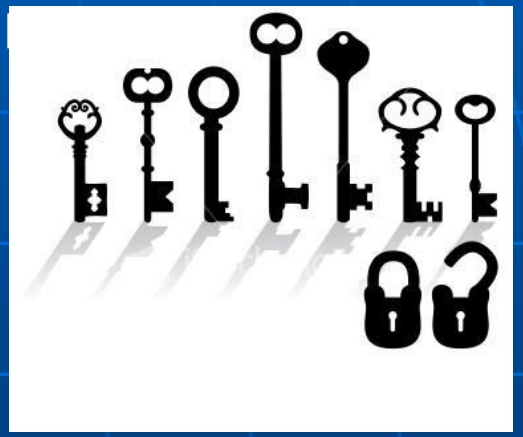
Культурная роль правовой информатики состоит, в частности, в повышении информационной и компьютерной культуры, профессиональной, общей и правовой культуры.

Проблемой защиты и сокрытия информации занимается **криптология** (*криптос* – скрытый, *логос* – наука), имеющая два направления – **криптографию** и **криптоанализ.**

Криптография разрабатывает и исследует математические методы преобразования информации.

Криптоанализ исследует возможности расшифровки информации без ключа.

Взлом шифра – поиск слабого места шрифта, которое позволяет получить доступ к зашифрованному сообщению без полного перебора ключей.



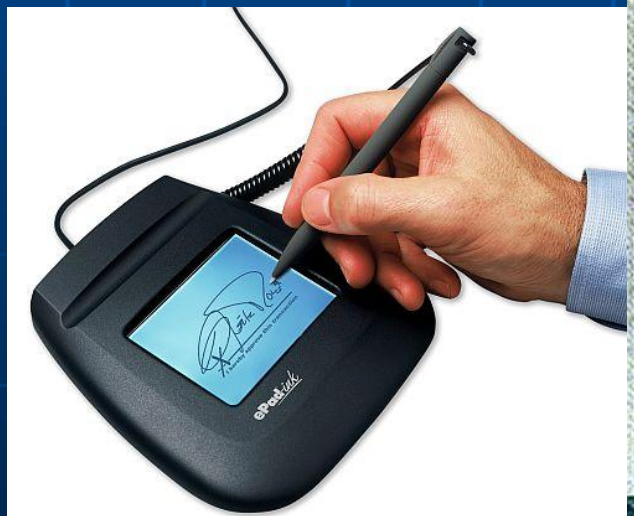
Попытка взлома (криптоанализа) – шифр.

Надежность шифра – способность противостоять взлому шифра.

Электронной (цифровой) подписью (ЭЦП) называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста проверить авторство и подлинность сообщения.

К ЭЦП предъявляются два основных требования:

- легкость проверки подлинности подписи;
- высокая сложность подделки подписи.



Информационная безопасность

Информационная безопасность системы – защищенность актуализируемой системой информации от внутренних или внешних угроз, то есть обеспечение устойчивого функционирования, целостности и эволюции системы.

Виды угроз информационной безопасности системы:

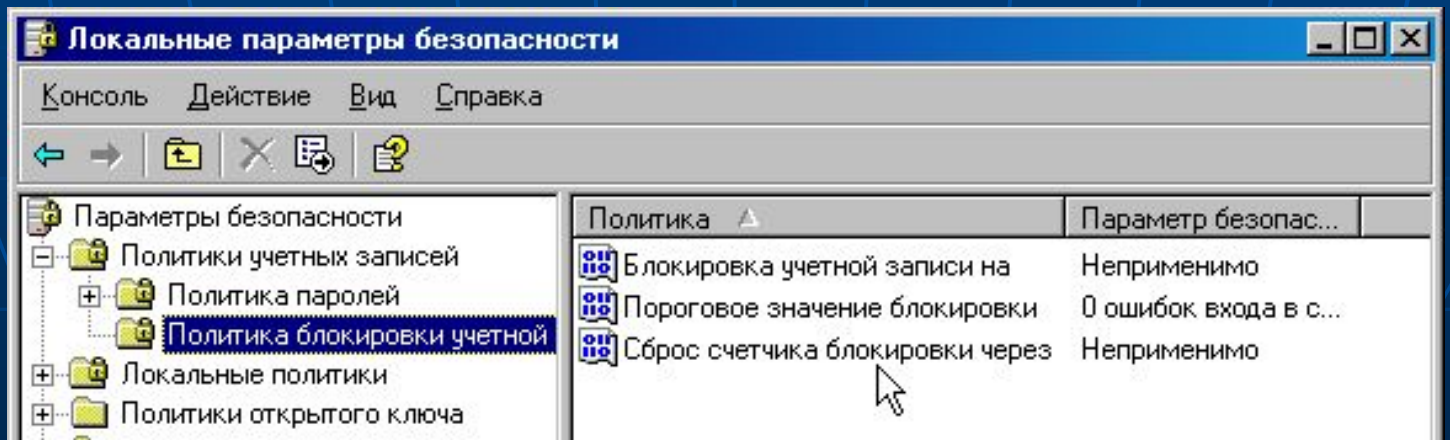
- непрофессиональные действия;
- преднамеренные действия;
- шпионаж, терроризм, преступные группы, хакеры;
- стихийные бедствия и аварии;
- сбои и отказ технического обеспечения системы;
- нелегальное копирование и использование нелицензионных программ;
- заражения вирусами и др.

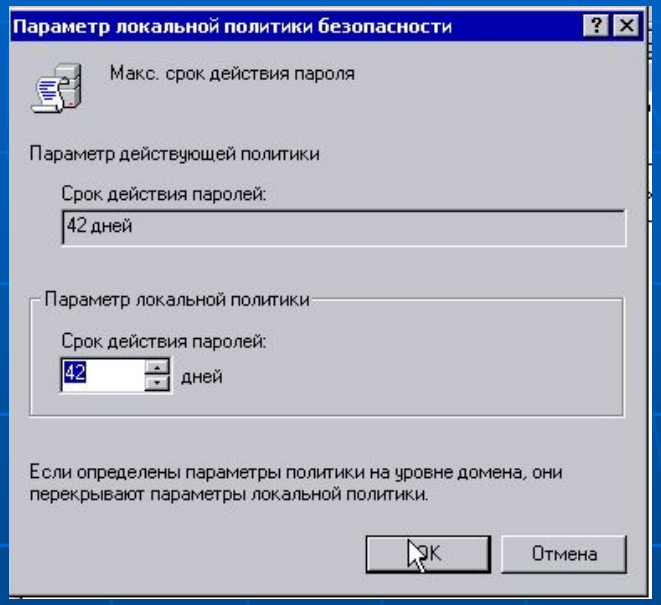
Основные **виды угроз для компьютерных систем и сетей:**

- неумышленные или некомпетентные действия;
- использование неизвестных игровых и других программ с вирусами;
- разглашение, передача, утрата ключей, паролей, программ;
- внесение изменения в используемую архитектуру и технологию или их игнорирование;
- отключение, расшифровка средств и методов защиты;
- использование некорректных данных, режимов работы, адресов и др.

Меры по безопасности информационных систем зависят от вида угрозы, и среди эффективных мер можно назвать следующее:

- Приоритетный доступ по паролю и регулярный контроль паролей;
- Разграничение прав и доступа;
- Надежный подбор персонала;
- Многоуровневая обработка и защита данных;
- Регулярная проверка и анализ работы персонала;
- Использование современных антивирусных пакетов.





Политика безопасности – неукоснительно выполняемые правила доступа, использования, распределения, защиты и хранения ценной информации.

При определении **политики безопасности в правовой информационной системе** необходимо:

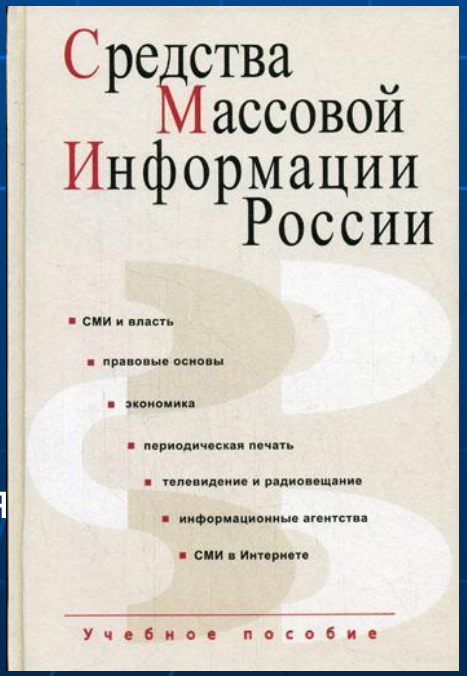
- для каждого документа, объекта определить режимы допуска и руководствоваться ими;
- регистрировать все события по допуску (например, в электронном журнале) и в последующем оперативно анализировать эту информацию (этот журнал).

Информационная безопасность

Обеспечение **информационной безопасности личности** означает, с одной стороны, ее право на объективную и конфиденциальную информацию для развития и жизненных целей и, с другой стороны, - защиту человека от любого информационного воздействия, препятствующего свободному формированию и развитию личности.

<u>В качестве таких воздействий на личность могут выступать:</u>

- информационное давление (СМИ);
- распространение недостоверной информации (СМИ);
- распространение вредной информации (сеть Интернет);
- умышленное использование неадекватного восприятия информации человеком (на митингах) и др.



Информационная безопасность

Цель информационного противоборства в современном мире – установление и удержание контроля над базовыми информационными ресурсами государства, а следовательно, над остальными видами ресурсов.

Задачи информационного противоборства – внедрение в жизненно важные информационные ресурсы, их контроль, защита собственных информационных ресурсов.

<u>В основу государственной политики информационной безопасности РФ положены следующие принципы:</u>

- комплексное рассмотрение проблем информационной безопасности;
- создание законодательной базы обеспечения информационной безопасности;
- финансирование теоретических, научно-практических работ по обеспечению безопасности.

Классы безопасности компьютерных систем (классы защиты систем):

- *системы минимальной защиты (класс D);*
- *системы с защитой по усмотрению пользователя (класс C);*
- *системы с обязательной защитой (класс B);*
- *системы с гарантированной защитой (класс A).*

Значки сетевой безопасности