Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предотвращения

Информация является **объектом** правового регулирования.

Право собственности состоит из трех важных компонентов:

- *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.

Правонарушение

- это юридический факт (наряду с событием и действием), действия, противоречащие нормам права (антипод правомерному поведению).

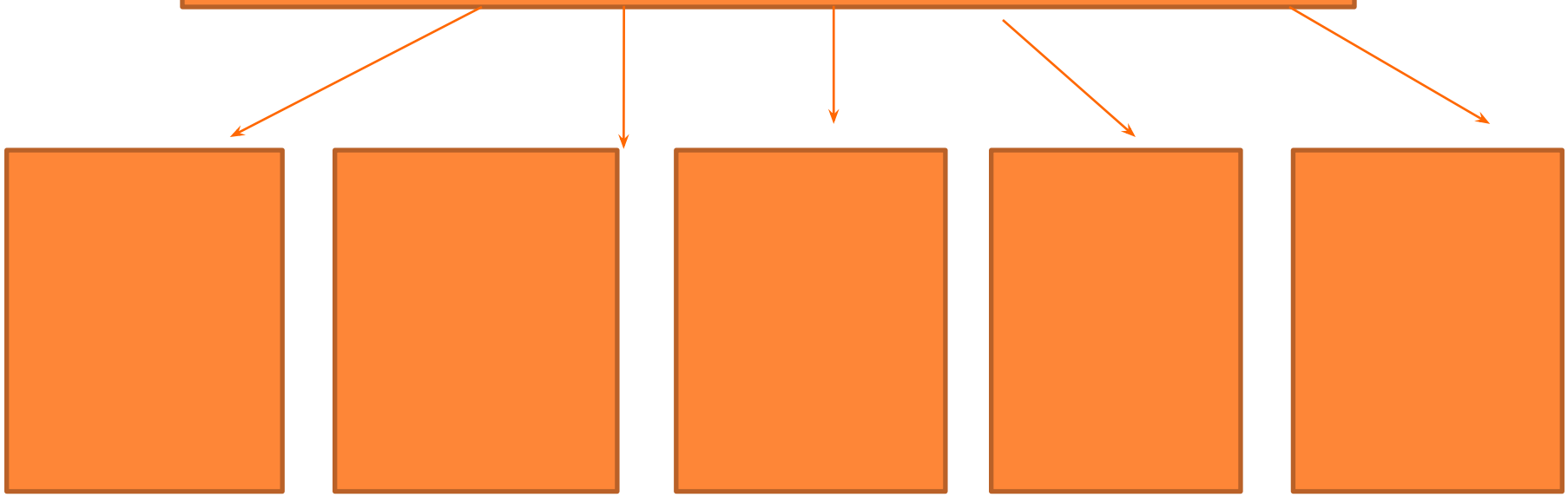
- Правонарушения всегда связаны с нарушением определенным лицом (лицами) действующей нормы (норм) ИП и прав других субъектов информационных правоотношений.

- 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 или киберпреступность

— преступления, совершаемые людьми, использующих информационные технологии для преступных целей.

Преступления в сфере компьютерной информации



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.
- мошенничество с использованием Интернета: инвестирование денежных средств на иностранных фондовых рынках с использованием сети Интернет сопряжено с риском быть вовлеченными в различного рода мошеннические схемы.

Результаты опроса представителей служб безопасности 492 компаний

Виды атак, выявленные за последние 12 месяцев:

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

Правовое регулирование Российской Федерации

- 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.

Правовое регулирование Российской Федерации

Регулирует отношение, возникающее при осуществлении права: поиск, получение, передачу и производство информации.

Применение информационных технологий, обеспечение защиты информации.

В ***Уголовном кодексе РФ*** имеется раздел «Преступления в сфере компьютерной информации».

Он предусматривает наказания за:

1. Неправомерный доступ к компьютерной информации;
2. Создание, использование и распространение вредоносных программ для ЭВМ;
3. Умышленное нарушение правил эксплуатации ЭВМ и их сетей.

Значимость безопасности информации

Прикладные задачи: сохранность личной информации пользователя

Управленческие задачи: обеспечение полноты управленческих документов

Информационные услуги: обеспечение доступности и безотказной работы

Коммерческая деятельность: предотвращение утечки информации

Банковская деятельность: обеспечение целостности информации

Снижение степени значимости информации для компании и всех заинтересованных лиц

Факторы и условия, которые необходимо учитывать при разработке методов защиты информации

- Расширение областей использования компьютеров и увеличение темпа роста компьютерного парка
- Высокая степень концентрации информации в центрах ее обработки
- Расширение доступа пользователя к мировым информационным ресурсам
- Усложнение программного обеспечения вычислительного процесса на компьютере

Методы защиты информации

Шифрование (криптография) информации

Преобразование (кодирование) слов и т.д. с помощью специальных алгоритмов

Законодатель-ные меры

Контроль доступа к аппаратуре

Вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры

Ограничение доступа к информации

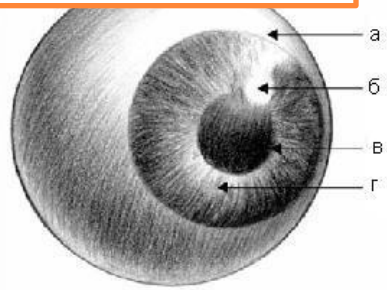
На уровне среды обитания человека: выдача документов, установка сигнализации или системы видеонаблюдения

На уровне защиты компьютерных систем: введение паролей для пользователей

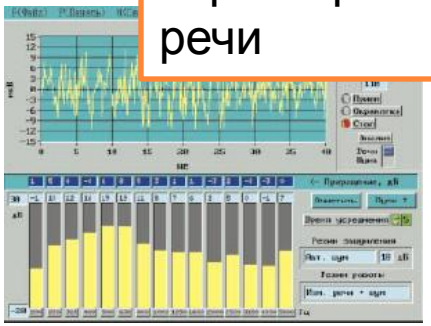
Биометрические системы защиты

По **отпечаткам пальцев**

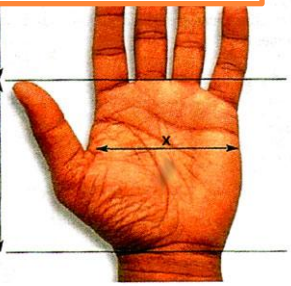
По радужной оболочке глаза



По характеристикам речи

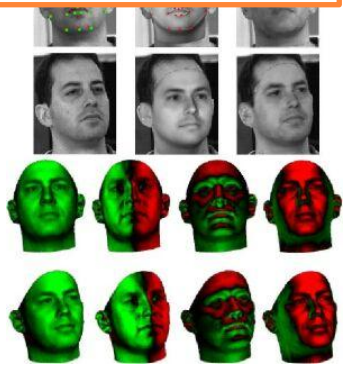


По геометрии ладони руки



X = ширина ладони, Y = длина ладони, Z = длина пальца

По изображению лица




Вредоносные программы
Вирусы, черви, троянские и хакерские программы
Шпионское, рекламное программное обеспечение
Web-черви
Загрузочные вирусы
Почтовые черви
Потенциально опасное программное обеспечение
Файловые вирусы
Троянские утилиты удаленного администрирования
Макровирусы
Рекламные программы
Троянские программы-шпионы
Сетевые атаки
Руткиты
Утилиты взлома удаленных компьютеров

Методы борьбы:

-антивирусные программы,
-межсетевой экран,
-своевременное обновление системы безопасности операционной системы и приложений,
-проверка скриптов в браузере

Межсетево́й экра́н, **сетево́й экра́н** — это комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Скрипт (*script* – англ. «сценарий») – компьютерная программа, представляющая собой последовательность инструкций для работы некоторого приложения.

В веб-программировании скрипт – это программа, исполняемая при взаимодействии Пользователя с веб-сайтом и реализующая функции, которые невозможно реализовать средставами обычного html (статического гипертекста).

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.

Электронное правительство является частью электронной экономики.

Электронное правительство

— система электронного документооборота государственного управления, основанная на автоматизации всей совокупности управленческих процессов в масштабах страны и служащая цели существенного повышения эффективности государственного управления и снижения издержек социальных коммуникаций для каждого члена общества.

Создание электронного правительства предполагает построение общегосударственной распределенной системы общественного управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки.

Домашнее задание

- Выучить основные понятия
- Заполнить таблицу: **Правовые нормы правового регулирования информации.**

	Законы	Краткое содержание
1	Закон «Об информации, информатизации и защите информации»	позволяет защищать информационные ресурсы (личные и общественные) от искажения, порчи, уничтожения.
2	Закон «О правовой охране программ для ЭВМ и баз данных»	
3	Уголовный кодекс раздел "Преступления в сфере компьютерной информации" № 63-ФЗ Дата принятия: 1996г.	
4	"О персональных данных" №152-ФЗ от 27.07.2006г.	
5	Конвенция Совета Европы о преступности в сфере компьютерной информации была подписана в Будапеште. №ETS 185 от 23.10.2001г.	
6	Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи"	
7	Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"	