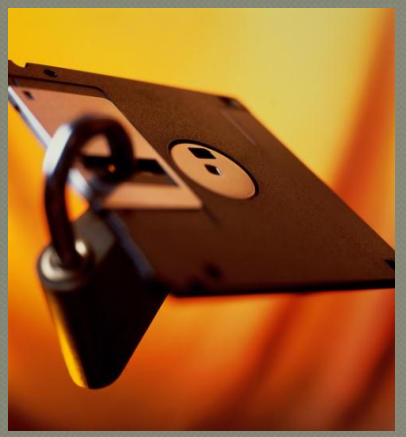
Информационная безопасность

Защита информации

- деятельность, направленная на сохранение государственной, служебной, коммерческой или личной тайн, а также на сохранение носителей информации любого содержания.



Средства защиты информации

1. Технические средства – реализуются в виде электрических, электромеханических, электронных устройств.

Делятся на:

Аппаратные – устройства, встраиваемые непосредственно в аппаратуру;

Физические – реализуются в виде автономных устройств и систем (оборудование охранной сигнализации и наблюдения, замки на дверях, решетки на окнах).

2. Программные средства – программы, специально предназначенные для выполнения функций, связанных с защитой информации.

Средства защиты информации

3. **Организационные средства** – организационно-правовые мероприятия, осуществляемые для обеспечения защиты информации.
4. **Законодательные средства –** законодательные акты страны, которыми регламентируются правила использования и обработки информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.
5. **Морально-этические средства –** всевозможные нормы, которые сложились традиционно или складываются по мере распространения вычислительных средств в данной стране или обществе.

Способы защиты информации

Препятствие – физически преграждает злоумышленнику путь к защищаемой информации.

Управление доступом – идентификация пользователей, персонала и ресурсов системы, проверка полномочий, разрешение и создание условий работы в пределах установленного регламента, регистрация обращений к защищаемым ресурсам, реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.

Способы защиты информации

Маскировка – способ защиты информации путем ее криптографического шифрования.

Регламентация – заключается в разработке и реализации комплексов мероприятий, создающих такие условия при которых возможности несанкционированного доступа к защищаемой информации сводились бы к минимуму.

Принуждение – пользователи и персонал вынуждены соблюдать правила обработки и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Основные виды компьютерных преступлений

Несанкционированный доступ к информации, хранящейся в компьютере.

Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

Разработка и распространение компьютерных вирусов. Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер. Варианты вирусов зависят от целей, преследуемых их создателем.

Основные виды компьютерных преступлений

Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

Подделка компьютерной информации.

Хищение компьютерной информации.

КОМПЬЮТЕРНЫЕ ВИРУСЫ -

это программы, которые могут «размножаться» и скрытно внедрять свои копии: в файлы,
в загрузочные секторы дисков, в документы.

При этом копии могут сохранять способность дальнейшего распространения. Вирус может дописывать себя везде, где он имеет шанс выполниться.

По величине вредных воздействий
вирусы можно разделить на:

- **неопасные,** *действие которых приводит к:*
  - ✔ уменьшению свободной памяти на диске,
  - ✔ графическим и звуковым эффектам;
- **опасные,** *действие которых приводит к:*
  - ✔ сбоям и зависанию компьютера;
- **очень опасные,** *действие которых приводит к:*
  - ✔ потере программ и данных (изменению или удалению файлов и каталогов)
  - ✔ форматированию винчестера и т.д.

По «среде обитания»

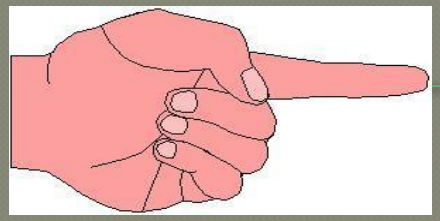
вирусы можно разделить на:

- **файловые** - *внедряются в исполняемые файлы (программы) и активизируются при их запуске (не заражают файлы со звуком и изображением);*
- **загрузочные** - *записывают себя в загрузочный сектор диска;*
- **макровирусы** - *заражают файлы документов Word и электронных таблиц Excel;*
- **сетевые** – *распространяются и заражают компьютеры по сети. Интернет-черви (передаются в почтовых сообщениях) и скрипт-вирусы (передаются через программы на языках JavaScript, VBScript).*

АНТИВИРУСНЫЕ ПРОГРАММЫ

- **Программы-детекторы** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
- **Программы-доктора**, или фаги, «лечат» зараженные программы или диски, «выкусывая» из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.
- **Программы-ревизоры** сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий об этом сообщается пользователю.
- **Доктора-ревизоры** – это гибриды ревизоров и докторов, т.е программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.
- **Программы-фильтры** располагаются резидентно в оперативной памяти компьютера, они перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.
- **Программы вакцины**, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает эти программы и диски уже зараженными.

К наиболее популярным антивирусным программам относятся: Dr.Web, Norton Antivirus, NOD 32, Антивирус Касперского, ADinf, AVP.



Безопасность

Конфиденциальность

Целостность

Доступность

- ***Информационная безопасность*** — это состояние защищённости информационной среды.

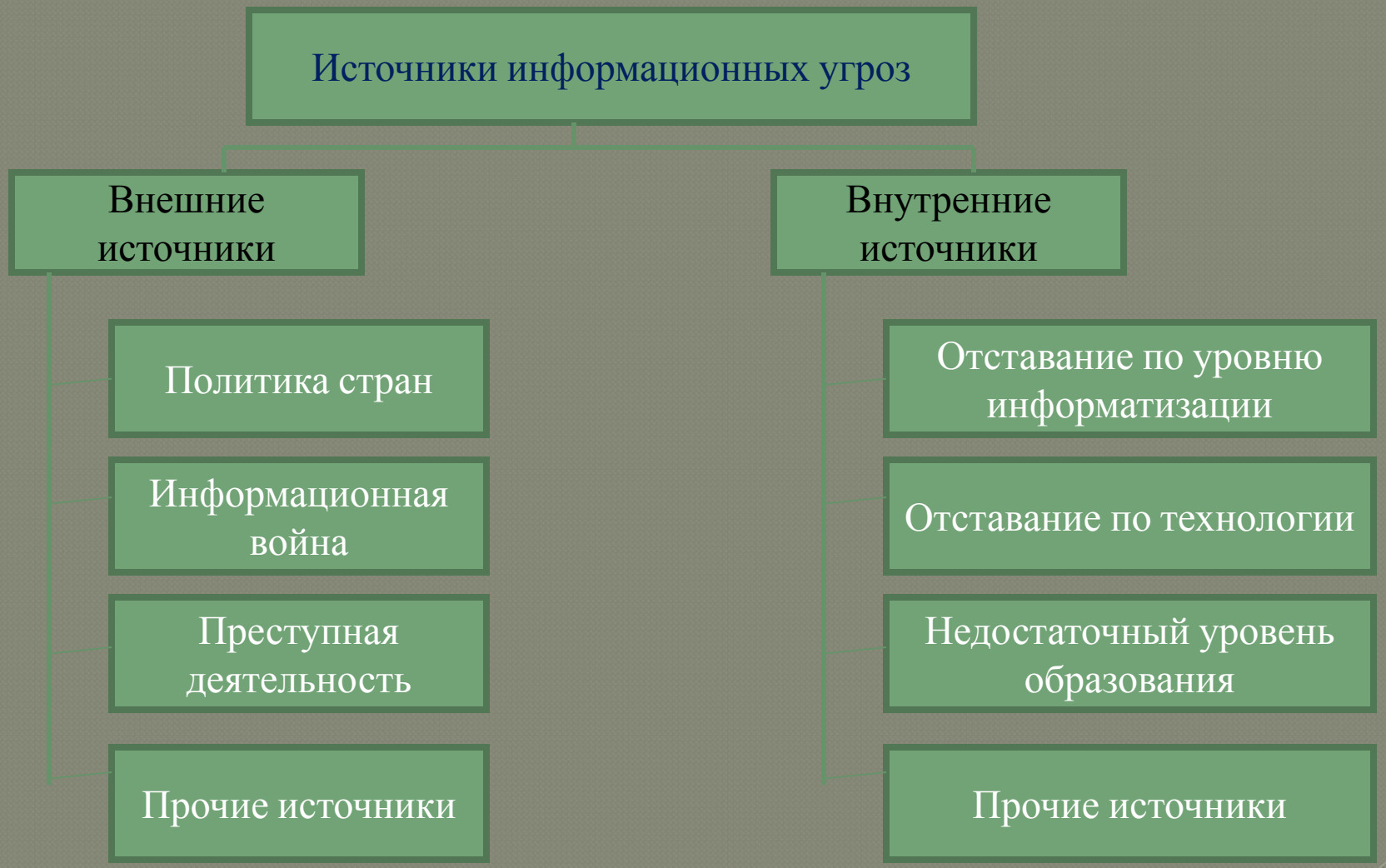
- ***Информационная безопасность*** – это совокупность мер по защите информационной среды общества и человека.

Цели информационной безопасности

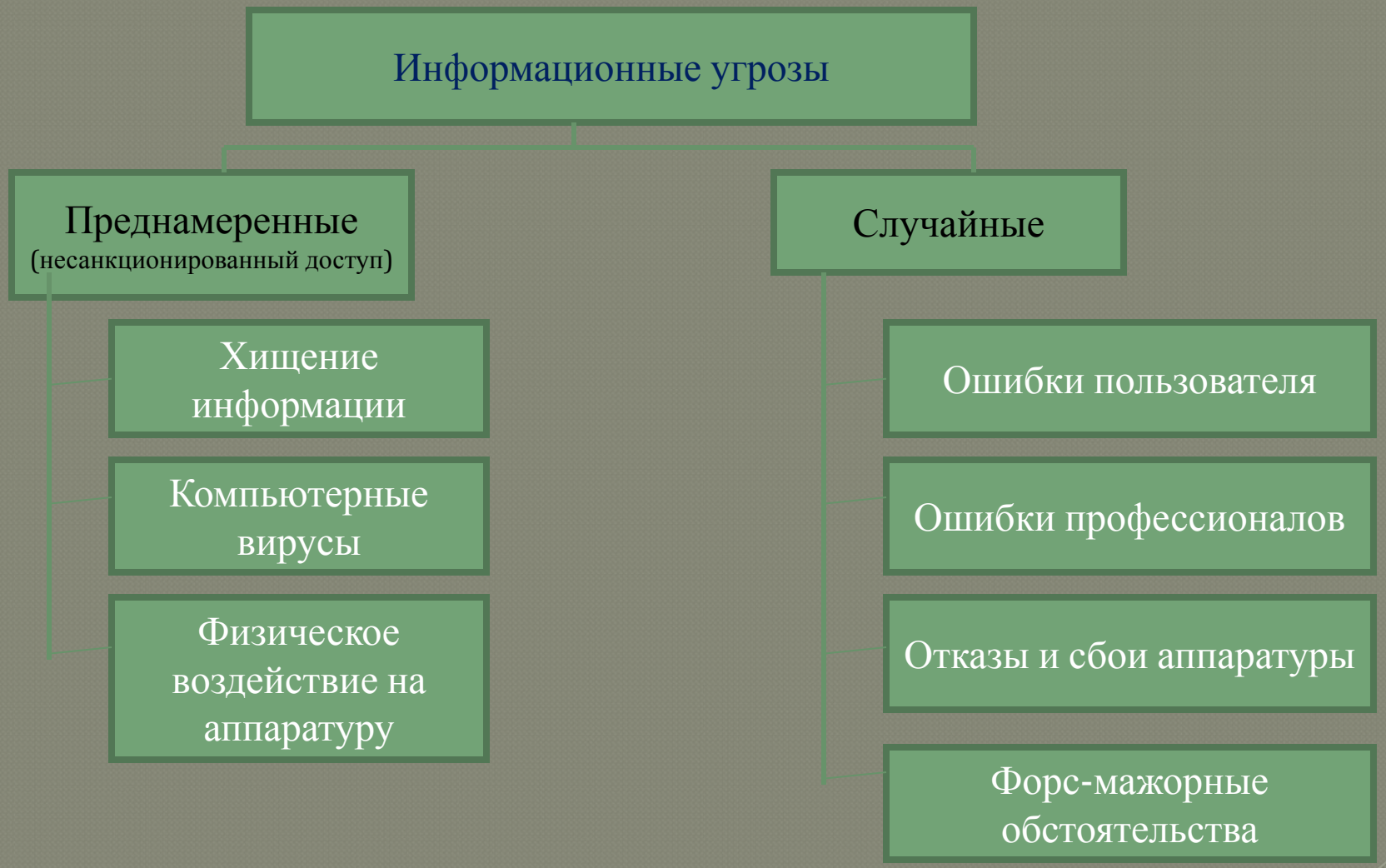
- Защита национальных интересов;
- Обеспечение человека и общества достоверной и полной информацией;
- Правовая защита человека и общества при получении, распространении и использовании информации.

(ФЗ от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

Источники основных информационных угроз для России



Основные виды информационных угроз



Несанкционированный доступ

Несанкционированный доступ - действия, нарушающие установленный порядок доступа или правила разграничения, доступ к программам данным, который получают абоненты которые не прошли регистрацию и не имеют права на ознакомление или работу с этими ресурсами.

Для предотвращения несанкционированного доступа осуществляется контроль доступа.

Защита с использованием паролей

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются ***пароли***.

Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль.

Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам.

При этом может производиться регистрация всех попыток несанкционированного доступа.

Защита с использованием пароля используется при загрузке операционной системы

Вход по паролю может быть установлен в программе **BIOS Setup**, компьютер не начнет загрузку операционной системы, если не введен правильный пароль. Преодолеть такую защиту нелегко.

От несанкционированного доступа может быть защищены

- каждый диск,
- каждая папка,
- каждый файл локального компьютера.

Для них могут быть установлены определенные права доступа

- полный доступ,
- возможность внесения изменений,
- только чтение,
- запись и др.

Права могут быть различными для различных пользователей.

Биометрические системы защиты

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются ***биометрические системы идентификации.***

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

К биометрическим системам защиты информации относятся системы идентификации:

- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза;
- по изображению лица;
- по геометрии ладони руки.

Идентификация по отпечаткам пальцев

Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а также применяются в виде отдельных внешних устройств и терминалов (например, в аэропортах и банках).

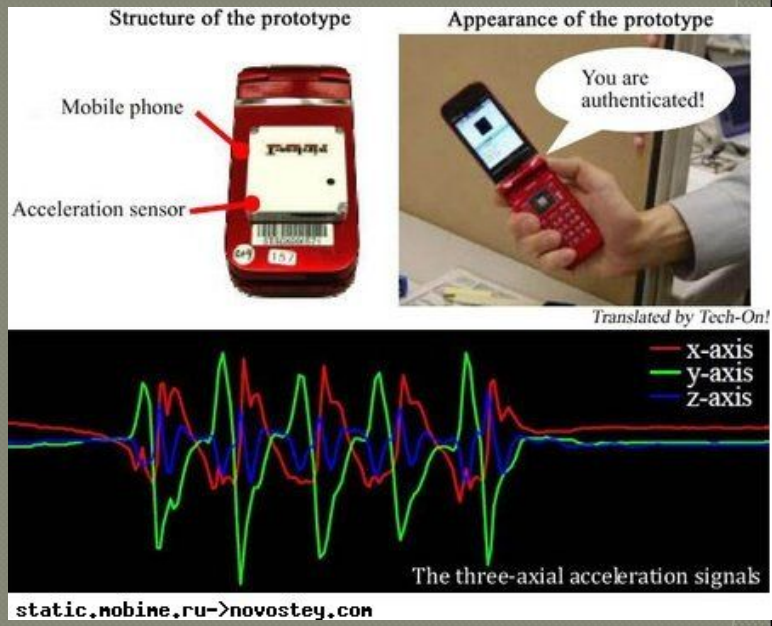
Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.

. Оптический сканер отпечатка пальца, вмонтированный в ноутбук

Идентификация по характеристикам речи

Идентификация человека по голосу — один из традиционных способов распознавания, интерес к этому методу связан и с прогнозами внедрения голосовых интерфейсов в операционные системы.

Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи.



Идентификация по радужной оболочке глаза

Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.

Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих-кодов. Результатом является матрица, индивидуальная для каждого человека.

Для идентификации по радужной оболочке глаза применяются специальные сканеры, подключенные к компьютеру.

Идентификация по изображению лица

Для идентификации личности часто используются технологии распознавания по лицу. Распознавание человека происходит на расстоянии.

Идентификационные признаки учитывают форму лица, его цвет, а также цвет волос. К важным признакам можно отнести также координаты точек лица в местах, соответствующих смене контраста (брови, глаза, нос, уши, рот и овал).

В настоящее время начинается выдача новых загранпаспортов, в микросхеме которых хранится цифровая фотография владельца.

Идентификация по ладони руки

В биометрике в целях идентификации используется простая геометрия руки — размеры и форма, а также некоторые информационные знаки на тыльной стороне руки (образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Сканеры идентификации по ладони руки установлены в некоторых аэропортах, банках и на атомных электростанциях .

Самостоятельная работа по теме «Информационная безопасность»

Выполнить задания:

- Найти в Интернете законы, указы, постановления об авторском праве на программный продукт.
- Найти в Интернете названия справочников, журналов, газет и т.п., в которых можно найти информацию о программных продуктах, о компьютерах, об информационных системах.