Информационная безопасность Методы защиты информации

Информационной безопасностью называют комплекс организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

Информационная безопасность дает гарантию того, что достигаются следующие цели:

- ***конфиденциальность*** информации (свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц);
- ***целостность*** информации и связанных с ней процессов (неизменность информации в процессе ее передачи или хранения);
- ***доступность*** информации, когда она нужна (свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц);
- ***учет*** всех процессов, связанных с информацией.

Обеспечение **безопасности информации** складывается из трех составляющих:

- Конфиденциальности,
- Целостности,
- Доступности.

Точками приложения процесса защиты информации к информационной системе являются:

- аппаратное обеспечение,
- программное обеспечение
- обеспечение связи (коммуникации).

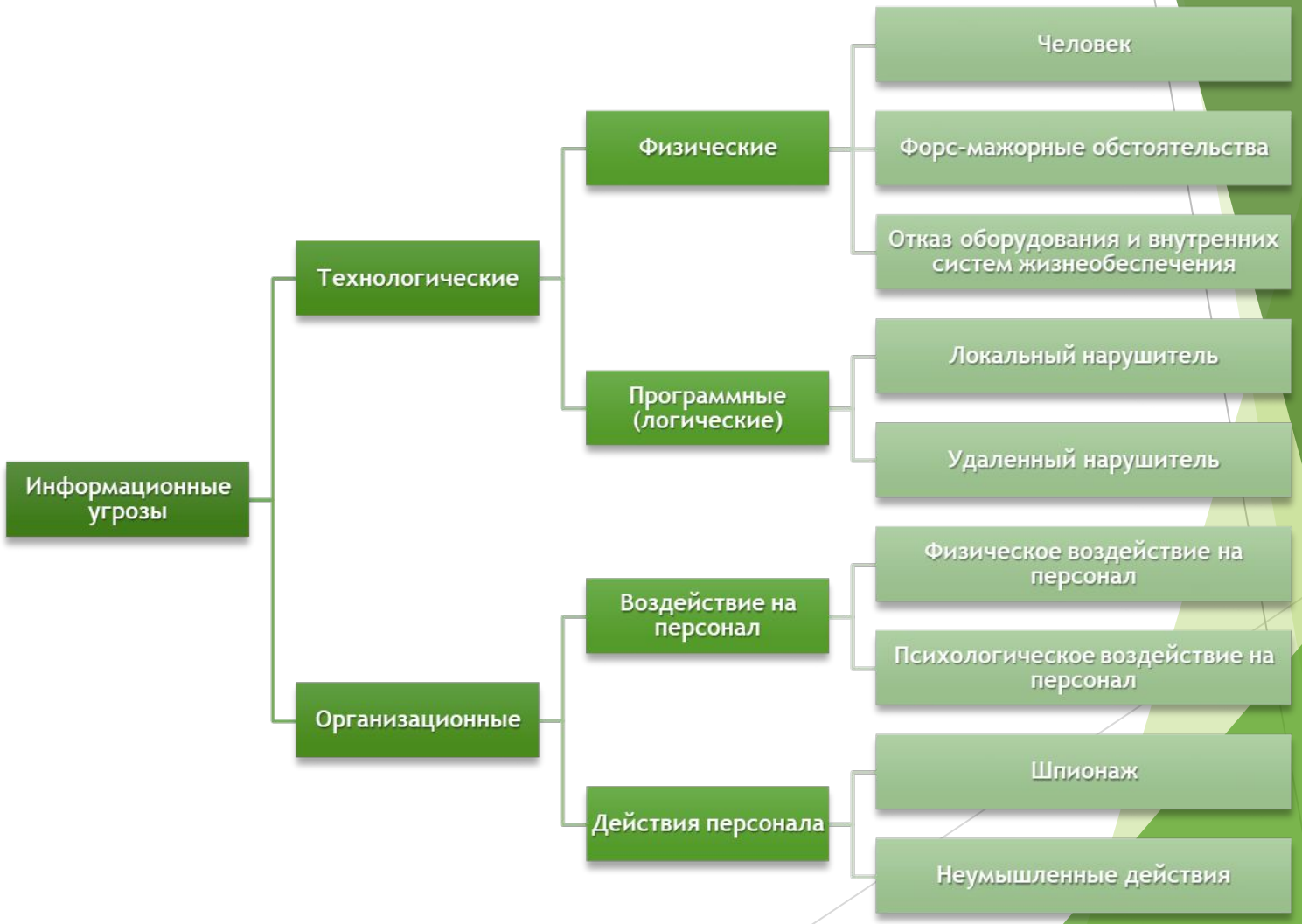
Сами процедуры(механизмы) защиты разделяются на

- защиту физического уровня,
- защиту персонала
- организационный уровень.

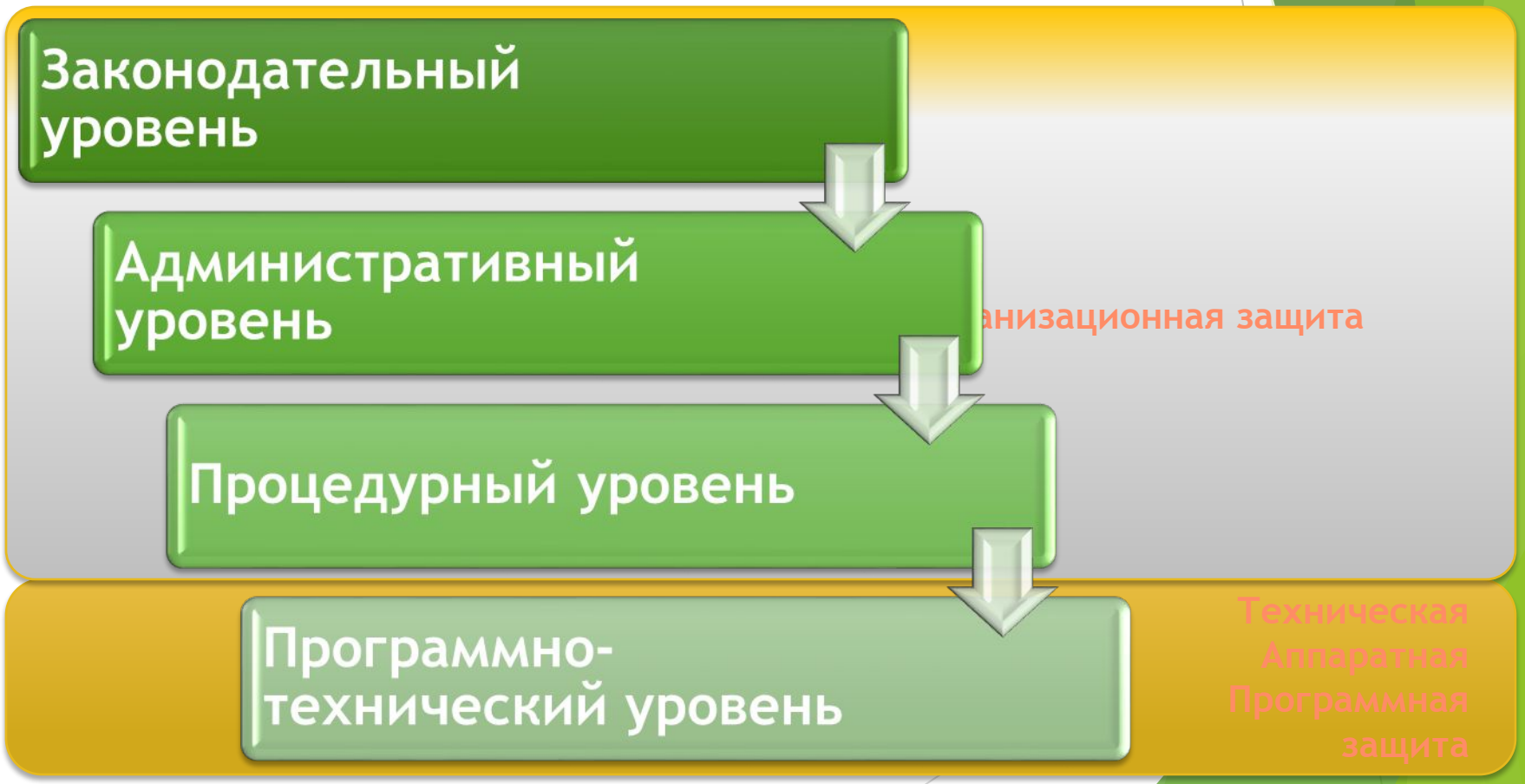
Угроза безопасности компьютерной системы - это потенциально возможное происшествие (преднамеренное или нет), которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Анализ угроз проведенных агентством национальной ассоциацией информационной безопасности (National Computer Security Association) в 1998 г. в США выявил следующую статистику:

Виды информационных угроз



Политика безопасности - это комплекс мер и активных действий по управлению и совершенствованию систем и технологий безопасности, включая информационную безопасность.



Организационная защита

- ***организация режима и охраны.***
- ***организация работы с сотрудниками*** (подбор и расстановка персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.)
- ***организация работы с документами*** и документированной информацией (разработка, использование, учет, исполнение, возврат, хранение и уничтожение документов и носителей конфиденциальной информации)
- ***организация использования технических средств*** сбора, обработки, накопления и хранения конфиденциальной информации;
- ***организация работы по анализу внутренних и внешних угроз*** конфиденциальной информации и выработке мер по обеспечению ее защиты;
- ***организация работы по проведению систематического контроля за работой персонала*** с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Технические средства защиты информации

Для защиты периметра информационной системы создаются:

- системы охранной и пожарной сигнализации;
- системы цифрового видео наблюдения;
- системы контроля и управления доступом (СКУД).

Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:

- использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;
- установкой на линиях связи высокочастотных фильтров;
- построение экранированных помещений («капсул»);
- использование экранированного оборудования;
- установка активных систем зашумления;
- создание контролируемых зон.

Аппаратные средства защиты информации

- Специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- Устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
- Устройства для шифрования информации (криптографические методы).
- Системы бесперебойного питания:
  - Источники бесперебойного питания;
  - Резервирование нагрузки;
  - Генераторы напряжения.

Программные средства защиты информации

- Средства защиты от несанкционированного доступа (НСД):
  - Средства авторизации;
  - Мандатное управление доступом;
  - Избирательное управление доступом;
  - Управление доступом на основе ролей;
  - Журналирование (так же называется Аудит).
- Системы анализа и моделирования информационных потоков (CASE-системы).
- Системы мониторинга сетей:
  - Системы обнаружения и предотвращения вторжений (IDS/IPS).
  - Системы предотвращения утечек конфиденциальной информации (DLP-системы).
- Анализаторы протоколов.
- Антивирусные средства.

Программные средства защиты информации

- Межсетевые экраны.
- Криптографические средства:
  - Шифрование;
  - Цифровая подпись.
- Системы резервного копирования.
- Системы аутентификации:
  - Пароль;
  - Ключ доступа (физический или электронный);
  - Сертификат;
  - Биометрия.
- Инструментальные средства анализа систем защиты:
  - Мониторинговый программный продукт.

ВИДЫ АНТИВИРУСНЫХ ПРОГРАММ

- Детекторы позволяют обнаруживать файлы, заражённые одним из нескольких известных вирусов. Некоторые программы-детекторы также выполняют эвристический анализ файлов и системных областей дисков, что часто (но отнюдь не всегда) позволяет обнаруживать новые, не известные программе-детектору, вирусы.
- Фильтры - это резидентные программы, которые оповещают пользователя о всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях.
- Программы-доктора или фаги не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние.
- Ревизоры запоминают сведения о состоянии файлов и системных областей дисков, а при последующих запусках – сравнивают их состояние исходным. При выявлении несоответствий об этом сообщается пользователю.
- Сторожа или фильтры располагаются резидентно в оперативной памяти компьютера и проверяют на наличие вирусов запускаемые файлы и вставляемые USB-накопители.
- Программы-вакцины или иммунизаторы модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже заражёнными.

Недостатки антивирусных программ

- Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов.
- Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах.
- Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).
- Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.
- Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.[8]

Понятие компьютерного вируса

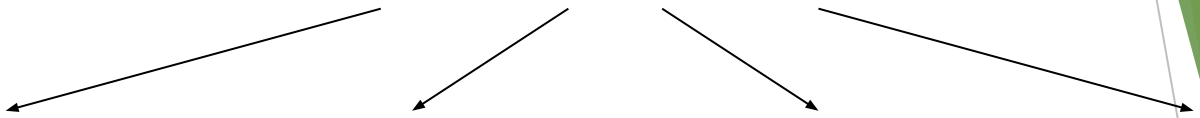
Компьютерный вирус – это специальная программа, наносящая заведомый вред компьютеру, на котором она запускается на выполнение, или другим компьютерам в сети.

Основной функцией вируса является его размножение.

Классификация компьютерных вирусов

- **по среде обитания;**
- **по операционным системам;**
- **по алгоритму работы;**
- **по деструктивным возможностям.**

1) По среде обитания



Файловые вирусы

Наносят вред файлам. Создают файл-двойник с именем оригинала.

Загрузочные вирусы

внедряются в загрузочный сектор диска. Операционная система при этом загружается с ошибками и сбоями

Макро-вирусы

«Портят» документы Word, Excel и других прикладных программ операционной системы Windows.

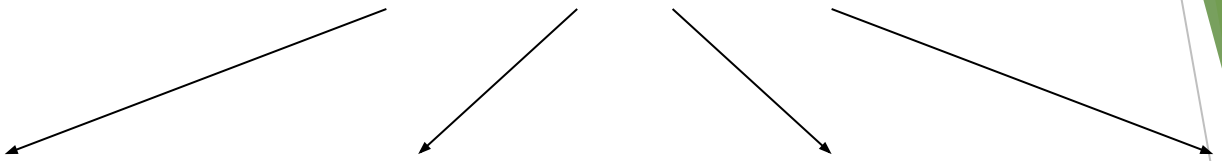
Сетевые вирусы

Распространяются по Internet через электронные письма или после посещения сомнительных сайтов.

2) По операционным системам

Для каждой операционной системы создаются свои вирусы, которые будут «работать» только в ней. Но существуют и универсальные вирусы, которые способны внедряться в различные операционные системы.

3) По алгоритму работы



Резидент-ность

Вирусы, обладающие этим свойством действуют постоянно пока компьютер включен.

Самошифро вание и полимор-физм

Вирусы-полиморфики изменяют свой код или тело прог-раммы, что их трудно обнаружить.

Стелс–алгоритм

Вирусы-невидимки «прячутся» в оперативной памяти и антивирусная программа их не может обнаружить.

Нестан-дартные приемы

Принципиаль но новые методы воздействия вируса на компьютер.

4) По деструктивным возможностям

Безвред-ные
не наносят никакого вреда ни пользовате-лю, ни компьютеру, но занимают место на жестком диске.

Неопасные
наносят моральный ущерб пользователю Вызывают визуальные графические или звуковые эффекты.

Опасные
уничтожают информацию в файлах. «Портят» файлы, делают их несчитыва-емыми и т.д.

Очень опасные
сбивают процесс загрузки ОС, после чего требуется ее переустановка; или «портят» винчестер, что его требуется форматировать

Вредоносные программы

- ***Троянский конь*** - это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Виды деструктивных действий:
  - Уничтожение информации. (Конкретный выбор объектов и способов уничтожения зависит только от фантазии автора такой программы и возможностей ОС. Эта функция является общей для троянских коней и закладок).
  - Перехват и передача информации. (паролей, набираемых на клавиатуре).
  - Целенаправленное изменение программы.
- ***Червями*** называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т.к. ему в любой момент может подвергнуться любой из компьютеров, подключенных к этой сети. Основная функция вирусов данного типа – взлом атакуемой системы, т. е. преодоление защиты с целью нарушения безопасности и целостности.

- **идентификация** — это называние лицом себя системе;
- **аутентификация** — это установление соответствия лица названному им идентификатору;
- **авторизация** — предоставление этому лицу возможностей в соответствие с положенными ему правами или проверка наличия прав при попытке выполнить какое-либо действие