Информационная безопасность цифровой образовательной среды школы

Гусарова О.В.
МОУ СШ№3

Тутаев 22

Цель ЦОС МОУ СШ№3

- Создание в образовательной организации современной и безопасной цифровой образовательной среды, обеспечивающей высокое качество и доступность образования всех видов и уровней

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.

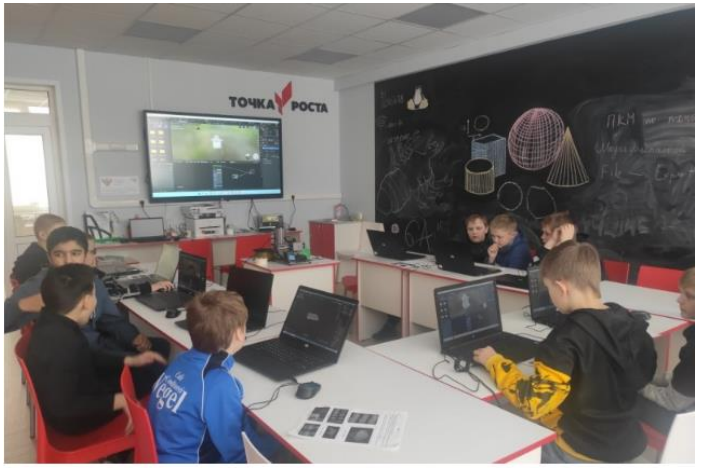
Конфиденциальность

Ст. 2 ФЗ «Об информации, информационных технологиях и защите информации

Персональные данные участников ЦОС:

- ФИО
- Дата рождения
- Адрес
- Контактные телефоны
- Адреса электронной почты
- Паспортные данные
- Данные свидетельства о рождении

Целостность



- Правильность
- Неискаженность
- Неизменность

Методы обеспечения целостности:

- Резервирование и зеркалирование данных оборудования
- Резервное копирование и электронная архивация информации
- Криптографическая защита

Доступность

- Право на чтение, изменение, хранение, копирование, уничтожение информации
- Право на изменение, использование, уничтожение информационных ресурсов

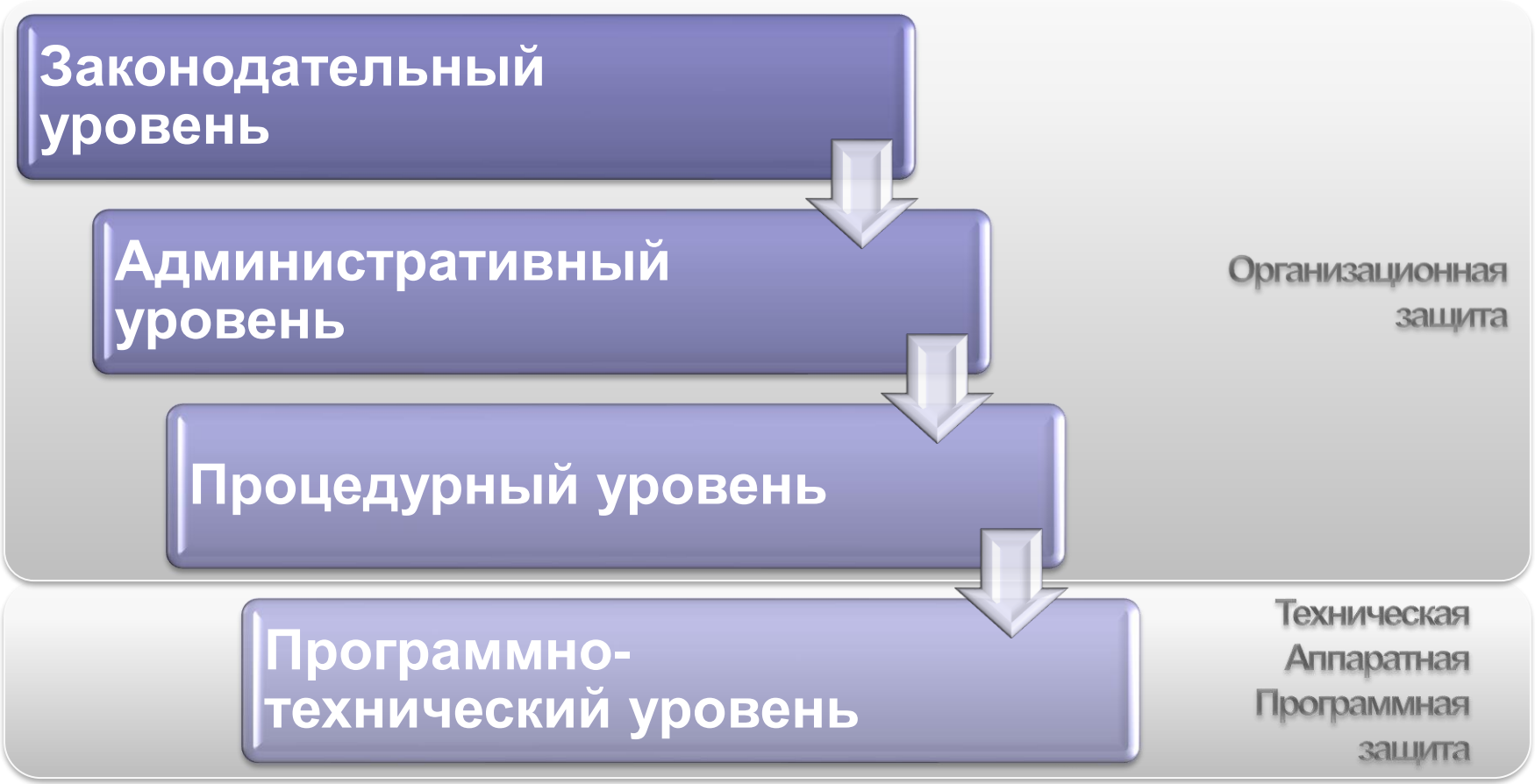
Точками приложения процесса защиты информации к информационной системе являются:

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

Сами процедуры(механизмы) защиты разделяются на

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

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 операционных систем
- Антивирусные средства
- 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.

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.

Спасибо

за

внимание!!!