1. Законодательный . Это законы, нормативные акты, стандарты и т.п. Нормативно-правовая база определяющая порядок защиты информации:

2. Морально-этический. Всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации.

3. Административный. Действия общего характера, предпринимаемые руководством организации. Такими документами могут быть:

⇒ приказ руководителя о назначении ответственного за обеспечение информационной безопасности;

⇒ должностные обязанности ответственного за обеспечение информационной безопасности;

⇒ перечень защищаемых информационных ресурсов и баз данных;

⇒ инструкцию, определяющую порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников организации.

4. Физический. Механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей.

5. Аппаратно-программный (электронные устройства и специальные программы защиты информации).

Защитите себя и своих детей!

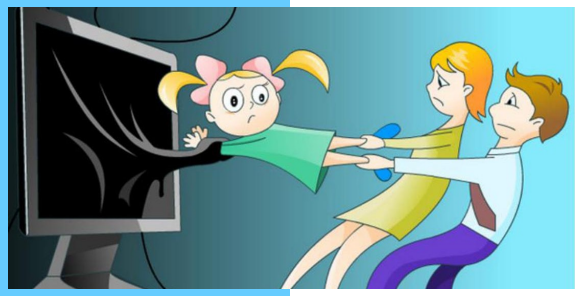
Информационная безопасность

МБДОУ «Детский сад №98»

Информационная безопасность

Говоря об информационной безопасности, мы рассуждаем о том как это может влиять на дошкольников. Дети дошкольного возраста всегда находятся «на контроле» взрослого. Поэтому окружающие дошкольника будут стараться оградить воспитанников от информации, которая может негативно повлиять на его формирование и развитие, то есть о пропаганде различной направленности.

Информационная безопасность детей - это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети "Интернет", вреда из здоровью, физическому, психическому, духовному и нравственному развитию.



На практике важнейшими являются три аспекта информационной безопасности:

⇒ доступность (возможность за разумное время получить требуемую информационную услугу);

⇒ целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

⇒ конфиденциальность (защита от несанкционированного прочтения).

Угроза заражения вредоносным ПО.

Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.

Контакты с незнакомыми людьми с помощью чатов или электронной почты.

Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.

Обеспечение информационной безопасности

Формирование режима информационной безопасности – проблема комплексная. Меры по ее решению можно подразделить на пять уровней: