**Обеспечение информационной безопасности**

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

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).

Принятые меры по созданию безопасной информационной системы в школе:  
-Обеспечена защита компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.)  
—  Установлен строгий контроль за электронной почтой, обеспечен постоянный контроль за входящей и исходящей корреспонденцией.  
—  Установлены соответствующие пароли на персональные ПК.  
—   Использованы контент-фильтры,  для фильтрации сайтов по их содержимому.

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать. Под защитой должна находиться вся система обработки информации.

Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность.

Надежная система защиты должна быть полностью протестирована и согласована. Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора.

В заключение своего доклада хотелось бы дать некоторые рекомендации по организации работы в информационном пространстве, чтобы уберечь себя и своих близких от интернет-преступников.