Информационная безопасность (ИБ) образовательного учреждения представляет собой комплекс мер различного характера, направленных на реализацию двух основных целей.

Первой целью ИБ - является защита персональных данных и информационного пространства от несанкционированных вмешательств, хищения информации и изменения конфигурации системы со стороны третьих лиц.

Вторая цель ИБ – защита учащихся от любых видов пропаганды, рекламы, запрещенной законом информации.

Информационная безопасность в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим трем группам:

- Персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы.
- Обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса.
- Защищенная законом интеллектуальная собственность.

Угрозы информационной безопасности

Угрозам намеренного или ненамеренного воздействия могут подвергаться следующие группы объектов:

! Компьютерное и другое оборудование образовательной организации, в отношении которого возможны воздействия вредоносного ПО, физические и другие воздействия.
! Программное обеспечение, применяемое в учебном процессе или для работы системы.
! Данные, которые хранятся на жестких дисках или портативных носителях.
! Дети и подростки, которые могут подвергаться стороннему информационному воздействию.
! Персонал, поддерживающий работу ИТ-системы.

Угрозы информационной безопасности образовательного учреждения могут носить непреднамеренный и преднамеренный характер.

К угрозам первого типа относятся:

- ✓ Аварии и чрезвычайные ситуации – затопление, отключение электроэнергии и т. д.
- ✓ Программные сбои.
- ✓ Ошибки работников.
- ✓ Поломки оборудования.
- ✓ Сбои систем связи.

Особенностью непреднамеренных угроз является их временное воздействие. В большинстве случаев результаты их реализации предсказуемы, достаточно эффективно и быстро устраняются подготовленным персоналом.

Намного более опасными являются угрозы информационной безопасности намеренного характера.

Обычно результаты их реализации невозможно предвидеть.

Намеренные угрозы могут исходить от
- учащихся,
- персонала организации,
- конкурентов,
- хакеров.

Лицо, осуществляющее преднамеренное воздействие на компьютерные системы или программное обеспечение, должно быть достаточно компетентным в их работе. Наиболее уязвимыми являются сети с удаленным в пространстве расположением компонентов. Злоумышленники могут достаточно легко нарушать связи между такими удаленными компонентами, что полностью выводит систему из строя.

Существенную угрозу представляет хищение интеллектуальной собственности и нарушение авторских прав. Также внешние атаки на компьютерные сети образовательной организации могут предприниматься для воздействия на сознание детей. Наиболее серьезная угроза – возможность вовлечения детей в криминальную или террористическую деятельность.

Меры защиты

Современные технологии информационной безопасности образовательной организации предусматривают обеспечение защиты на 5 уровнях:

- нормативно-правовой;
- морально-этический;
- административно-организационный;
- физический;
- технический.