Информационная безопасность

Информационная безопасность образовательного учреждения представляет собой комплекс мер различного характера, направленных на реализацию двух основных целей. Первой целью 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.

Действия злоумышленников могут привести к хищению указанных данных. Также при несанкционированном вмешательстве возможны внесения изменений и уничтожение хранилищ знаний, программных кодов, оцифрованных книг и пособий, используемых в образовательном процессе.

В обязанности лиц, отвечающих за информационную безопасность, входит:

- обеспечение сохранности защищаемых данных;

- поддержание информации в состоянии постоянной доступности для авторизованных лиц;
- обеспечение конфиденциальности подлежащих защите сведений, предотвращение доступа к ним со стороны третьих лиц.

Угрозы информационной безопасности

Спецификой обеспечения ИБ в информационных учреждениях является состав характерных угроз. К ним относится не только возможность хищения или повреждения данных хакерами, но также деятельность учащихся. Подростки могут сознательно или ненамеренно повредит оборудование или заразить систему вредоносными программами.

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, конкуренты, хакеры. 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.