**Понятие ИБ в образовательной организации**

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.

Также специалисты по ИБ обязаны не допустить несанкционированные изменения данных и их утрату.

**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.



**Способы несанкционированного доступа**

Для хищения данных, создания нарушений в работе информационной системы и для других действий требуется несанкционированный доступ. Различают следующие виды несанкционированного доступа:

* Человеческий. Предусматривает хищение сведений методом их отправки по электронной почте или копирования на портативные носители, внесение вручную изменений в базы данных при наличии физического доступа к серверу.
* Аппаратный. Применение специального оборудования для хищения данных или внесения изменений в систему. В том числе может применяться оборудование для перехвата электромагнитных сигналов.
* Программный. Применение специального программного обеспечения для перехвата данных, копирования паролей, дешифровки и перенаправления трафика, внесения изменений в функционирование другого софта и т. д.

**Меры защиты**

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

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

Рассмотрим подробнее меры защиты, предпринимаемые на каждом из этих уровней.

**Нормативно-правовой способ защиты**

Основным документом, определяющим степень угроз и меры обеспечения информационной безопасности обучающихся в образовательной организации, является «Национальная стратегия действий в интересах детей». Она предусматривает приоритет мер, направленных на защиту сознания ребенка от информационного воздействия агрессивного характера. Меры по защите информационных систем и баз данных имеют второй уровень приоритетности.

Законодательством определяются данные, которые должны быть защищены от несанкционированного доступа третьих лиц. К числу таких сведений относятся:

* персональные данные;
* конфиденциальные сведения;
* служебная, профессиональная, коммерческая тайна.

Порядок обеспечения безопасности персональных данных регламентируется Трудовым кодексом, Гражданским кодексом, Федеральным законом «Об информации» и другими актами. Конкретные меры по защите данных, используемое для этого аппаратное и методическое обеспечение определяются законами и профильными ГОСТами.

**Морально-этические средства обеспечения информационной безопасности**

Система морально-этических ценностей имеет особое значение в сфере образования. Она служит основой для выработки комплекса мер, направленных на защиту детей и подростков от информации этически некорректного, травмирующего, противозаконного характера. Защита детей от пропаганды основывается на законе «О защите прав ребенка». Этим актом определяются права детей на защиту от информации, которая может стать причиной моральной травмы.

В рамках мер по обеспечению ИБ создаются перечни источников (программ, документов и т. д.) способных травмировать детскую психику. В результате принимаемых мер должен предотвращаться доступ таких источников на территорию образовательного учреждения.

**Меры административно-организационного характера**

Система административно-организационных мер строится на базе внутренних регламентов и правил организации, которыми регламентируется порядок обращения с информацией и ее носителями. В том числе должны быть разработаны:

* должностные инструкции;
* внутренние методики по ИБ;
* перечни не подлежащих передаче данных;
* регламент взаимодействия с уполномоченными государственными органами по запросам о предоставлении информации и т. д.

Разработанными методиками должен определяться порядок доступа учеников в интернет во время занятий в компьютерных классах, меры по предотвращению доступа детей к определенным ресурсам, предотвращение использования ими своих носителей информации и т. д.

**Физические меры**

Ответственность за реализацию мер защиты компьютерной сети и носителей информации физического характера несет непосредственно руководитель образовательной организации и ее IT-персонал. Не допускается перекладывание этих мер на наемные охранные структуры.

К числу физических мер относятся:

* реализация пропускной системы для доступа в помещения, в которых находятся носители данных;
* создание системы контроля и управления доступом;
* определение уровней допуска;
* создание правил обязательного регулярного копирования критически важных данных на жесткие диски ПК, не подключенных к интернету.

Также среди физических мер можно назвать правила по созданию паролей и их периодической замене.

**Технические меры**

Технические меры защиты предусматривают использование специализированного программного обеспечения. В том числе в образовательных организациях рекомендуется использовать DLP и SIEM-системы, которые эффективно обнаруживают угрозы ИБ и обеспечиваю борьбу с ними. При невозможности использования подобных систем по причине бюджетных ограничений, применяются рекомендованные и разрешенные антивирусы и другие виды специального софта.

Применяемое для технической защиты программное обеспечение должно обеспечивать контроль электронной почты, которой пользуются ученики или персонал образовательной организации. Также могут устанавливаться ограничения на копирование данных с жестких дисков компьютеров. Обязательно рекомендуется использование контент-фильтра, с помощью которого ограничивается доступ детей к определенным ресурсам в интернете.