МБОУ СОШ №18, дошкольное отделение «Семицветик»

Консультация

Тема:

«Обеспечение информационной безопасности и воспитание информационной культуры как приоритетное направление работы современного образовательного учреждения»



Выполнила:

Воспитатель

Клецко Т.Г.

Серпухов 2023

Консультация

Тема: «Обеспечение информационной безопасности и воспитание информационной культуры как приоритетное направление работы современного образовательного учреждения».

Цель: создание условий для обеспечения информационной безопасности детей.

Информационная безопасность современного 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 информационной безопасности 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.



**Воспитание** **информационной** **культуры** –

это специфический вид воспитания, направленный на подготовку информационно-технологической деятельности и воспитательным управлением развития личностных и профессиональных качеств человека. Воспитанием информационной культуры, как и ее формированием, необходимо заниматься системно с раннего возраста и на протяжении всей жизни.

Особую роль в этом процессе играет образование. В процессе обучения в школе должны формироваться не только навыки работы с компьютером, информацией, но понимание важности такой деятельности для самого человека, получения им личностно-значимой информации. При этом не следует забывать о воспитательном аспекте, соблюдении правил и этических норм при получении и создании информации. Это имеет особое значение при использовании Интернет, нахождении в социальных сетях. В них имеются специфические ресурсы и формы социальных взаимодействий, что не должно исключать свойств общего социального пространства, а значит, и общепринятых норм и правил поведения.

Информационная культура есть сложный многоуровневый продукт взаимоотношений общества, науки, техники и человека.

Маленький человек появляется на свет. Он окружен заботой и вниманием, помощью и поддержкой. Он познает мир с помощью родных и близких, но ему все больше нравится делать это самому. Родителей удивляет, что ребенок все чаще отвергает их помощь и пытается постичь тайны предметов и явлений самостоятельно.

По мере взросления информационное поле ребенка расширяется, его познавательные устремления становятся более активными. Зачастую родителей это раздражает, они отмахиваются от его вопросов, твердят: подрастешь - узнаешь, рано тебе об этом знать, не твоего ума это дело.

Ребенок подрастает, приходит в школу и ждет, когда же он сможет познать то, что еще не знает. Малыши-первоклассники, затаив дыхание, ждут встреч со своим учителем, который вводит их в мир неизведанной и непонятной им информации, в мир знаний. В этот мир войти помогают и родители, и воспитатели сообща только в том случае, если педагог подходит к проблеме развития познавательной активности, детского интереса и любознательно­сти системно и ответственно.

Однако можно наблюдать довольно грустную картину: дети задают вопросы, ждут ответа, а взрослый, который призван по­мочь им найти ответ, отмахивается от них, злится, не считает это для себя важным делом. И постепенно интерес гаснет, дети уже не задают вопросы, только отвечают на них, при этом делают это без огонька, без задора, без радости.

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**

**ПО ОБУЧЕНИЮ ВОСПИТАННИКОВ ПРАВИЛАМ БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ, ПРОФИЛАКТИКЕ ИНТЕРНЕТ-ЗАВИСИМОСТИ**

Методические рекомендации разработаны с целью обеспечения реализации образовательными организациями системы мероприятий, направленных на обучение воспитанников правилам безопасного поведения в интернет-пространстве, профилактику интернет-зависимости, националистических проявлений в молодежной среде и устранение риска вовлечения подростков в противоправную деятельность.

Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 No 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

В Интернете, как и в реальной жизни, воспитанников подстерегают опасности: доступность нежелательного контента в социальных сетях, обман и вымогательство денег, платные СМС на короткие номера, пропаганда насилия и экстремизма, игромания и интернет-зависимость, склонение к суициду и т. п.

Интернет-зависимость — это навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире.

Задача педагогов в связи с имеющимися рисками состоит в том, чтобы указать на эти риски, предостеречь от необдуманных поступков, сформировать у воспитанников навыки критического отношения к получаемой в Интернете информации, воспитать культуру безопасного использования Интернет. Также следует обратить внимание на гигиенические требования, которые необходимо соблюдать при работе с компьютером:

* школьникам среднего и старшего возраста можно проводить перед монитором до двух часов в день, устраивая 10-15-минутные перерывы каждые полчаса;
* ребенок младшего возраста может находиться за компьютером не более 15 минут в день, в условиях классно-урочной деятельности – не более одного урока, а при наличии противопоказаний офтальмолога – только 10 минут, не более 3 раз в неделю;
* лучше работать за компьютером в первой половине дня;
* комната должна быть хорошо освещена;
* при работе за компьютером следить за осанкой, мебель должна соответствовать росту;
* расстояние от глаз до монитора – 60 см;
* периодически делать зарядку для глаз.

В соответствии с федеральными государственными образовательными стандартами общего образования в структуру основной образовательной программы основного общего образования включена программа воспитания и социализации учащихся, которая содержит такое направление, как формирование культуры здорового и безопасного образа жизни. В рамках этой программы может осуществляться информационно-просветительская работа среди школьников, пропагандирующая важность владения навыками безопасной работы в сети Интернет.

В образовательных организациях необходимо проводить занятия для воспитанников по основам информационной безопасности («основы медиа- безопасности»); знакомить родителей с современными программно- техническими средствами (сетевыми фильтрами, программами «родительский контроль»), ограничивающими доступ детей и подростков к ресурсам сети Интернет, несовместимыми с задачами воспитания; проводить специальные мероприятия по вопросам информационной безопасности несовершеннолетних.