

Педагогам

Когда речь заходит об информационной безопасности, обычно мы начинаем думать о компьютерах, сетях, интернете и хакерах. Но для образовательной среды проблема стоит шире: в ограждении учащегося от информации, которая может негативно повлиять на его формирование и развитие, то есть о пропаганде различной направленности.

Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются три аспекта информационной безопасности:

- доступность (возможность за разумное время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения).

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

Обеспечение информационной безопасности

1. Объясните учащимся правила поведения в Интернете. Расскажите о мерах, принимаемых к нарушителям, ответственности за нарушение правил поведения в сети.
2. Совместно с учащимися сформулируйте правила поведения в случае нарушения их прав в Интернете.
3. Приучайте несовершеннолетних уважать права других людей в Интернете. Объясните им смысл понятия «авторское право», расскажите об ответственности за нарушение авторских прав.
4. Проявляйте интерес к "виртуальной" жизни своих учеников, и при необходимости сообщайте родителям о проблемах их детей.
5. Научите учеников внимательно относиться к информации, получаемой из Интернета. Формируйте представление о достоверной и недостоверной информации. Наставляйте на посещение проверенных сайтов.
6. Обеспечьте профилактику интернет-зависимости учащихся через вовлечение детей в различные внеклассные мероприятия в реальной жизни (посещение театров, музеев, участие в играх, соревнованиях), чтобы показать, что реальная жизнь намного интереснее виртуальной.
7. Периодически совместно с учащимися анализируйте их занятость и организацию досуга, целесообразность и необходимость использования ими ресурсов сети для учебы и отдыха с целью профилактики интернет-зависимости и обсуждайте с родителями результаты своих наблюдений.
8. В случае возникновения проблем, связанных с Интернет-зависимостью, своевременно доводите информацию до сведения родителей, привлекайте к работе с учащимися и их родителями психолога, социального педагога.
9. Проводите мероприятия, на которых рассказывайте о явлении Интернет-зависимости, ее признаках, способах преодоления.
10. Систематически повышайте свою квалификацию в области информационно-коммуникационных технологий, а также по вопросам здоровьесбережения.

11. Станьте примером для своих учеников. Соблюдайте законодательство в области защиты персональных данных и информационной безопасности. Рационально относитесь к своему здоровью. Разумно используйте в своей жизни возможности интернета и мобильных сетей.

Start

Безопасный Интернет



С осторожностью добавляйте незнакомцев в «друзья» и отказывайтесь от личных встреч с людьми, с которыми вы познакомились в Интернете. Обязательно расскажите взрослым и своим друзьям о запросе на такую встречу. Виртуальные друзья могут на самом деле быть не теми, за кого они себя выдают.



Клевета, оскорбление, незаконное копирование продуктов труда других людей и другие противоправные действия, совершенные в виртуальном мире, влекут за собой реальное привлечение к административной, гражданской правовой или даже уголовной ответственности.



Заведите отдельный почтовый адрес для регистрации в социальных сетях, форумах и прочих сервисах - придумайте к нему сложный пароль.



Относитесь с подозрением к сайтам, где запрашивают пароль, адрес, данные паспорта и т.д., просят прислать sms, фотографию, ввести номер телефона.



Если у вас есть вопросы по безопасности в сети Интернет, позвоните на телефон «горячей линии»
8 800 25 000 15



Незнакомые сайты и письма от неизвестных адресатов могут содержать вредоносные программы.



Всё, что вы сообщите о себе в социальных сетях, чатах или форумах, может быть использовано с мошенническими намерениями.



Подумайте прежде, чем разместить фотографии или рассказать о чем-нибудь в онлайн-среде. Фотография, размещенная несколько лет назад, может стать причиной отказа принять вас на работу в будущем.



Оставляйте в сети минимум информации о себе и своих близких, используйте логины и сложные пароли – новые для каждого сайта – чаще их меняйте!



Помните, что в безопасных играх и квестах никогда не предлагается выполнять задания в реальной жизни или в ночное время. Избегайте таких игр.



Если у вас есть вопросы по безопасности в сети Интернет, зайдите на сайт «Дети России онлайн»
www.detonline.com