|  |
| --- |
|    УТВЕРЖДАЮ Заместитель директора по учебно- |
|  методической работе ГУДО «Центр |
|  творчества «Эверест» г.Могилева» |
|  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.В.Голодникова |
|  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2020г. |

**ПРАВИЛА №\_\_30\_\_**

по безопасности учащихся

в сети Интернет

**Общие правила работы в сети Интернет**

1.    Не входите на незнакомые сайты.
2.    Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
3.    Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
4.    Никогда не посылайте никому свой пароль.
5.    Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
6.    При общении в Интернет не указывайте свои личные данные, а используйте псевдоним (ник)
7.    Без контроля взрослых ни в коем случае не встречайтесь с людьми, с которыми познакомились в сети Интернет.
8.    Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.
9.    Не всей  информации, которая размещена в Интернете, можно верить.
10.  Не оставляйте без присмотра компьютер с важными сведениям на экране
11.  Не сохраняйте важные сведения на общедоступном компьютере.

**Классификация интернет-угроз**

Во Всемирной паутине существует следующие виды опасности юных пользователей:

- суицид-сайты;
-сайты-форумы потенцинальных самоубийц;
-наркосайты (интернет пестрит новостями о «пользе» употребления марихуаны, рецептами и советами изготовления «зелья»);
-сайты, разжигающие национальную рознь и расовое неприятие (экстремизм, национализм, фашизм);
-сайты порнографической направленности;
-сайты знакомств (виртуальное общение разрушает способность к реальному общению, у подростков теряются коммуникативные навыки);
-сайты, пропагандирующих экстремизм, насилие и девиантные формы поведения, прямые угрозы жизни и здоровью школьников от незнакомцев, предлагающих личные встречи, а также различные виды мошенничества;
-секты (виртуальный собеседник может повлиять на мировоззрение подростка).

**Правила по безопасности в сети Интернет для детей 7-8 лет**

•    Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
•    Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
•    Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
•    Используйте специальные детские поисковые машины, типа MSN Kids Search.
•    Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
•    Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.
•    Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.
•    Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
•    Научите детей не загружать файлы, программы или музыку без вашего согласия.
•    Не разрешайте детям использовать службы мгновенного обмена сообщениями.
•    В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
•    Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.
•    Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
•    Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
•    Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
•    Используйте специальные детские поисковые машины, типа MSN Kids Search.
•    Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
•    Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
•    Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.
•    Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
•    Научите детей не загружать файлы, программы или музыку без вашего согласия.
•    Не разрешайте детям использовать службы мгновенного обмена сообщениями.
•    В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
•    Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.
•    Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

**Правила по безопасности в сети Интернет для детей от 9 до 12 лет**

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств родительского контроля.

•    Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
•    Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.
•    Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
•    Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
•    Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
•    Не забывайте беседовать с детьми об их друзьях в Интернет.
•    Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет.
•    Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
•    Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.
•    Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
•    Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
•    Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
•    Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
•    Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

**Правила по безопасности в сети Интернет для детей от 13 до 17 лет**

Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах).
•    Компьютер с подключением к сети Интернет должен находиться в общей комнате.
•    Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
•    Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
•    Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
•    Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
•    Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.
•    Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
•    Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
•    Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
•    Приучите себя знакомиться с сайтами, которые посещают подростки.
•    Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
•    Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Заместитель директора по УВР

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Н.В. Харкевич