

Нижеприведенные рекомендации по профилактике и противодействию кибербуллингу ориентированы, в первую очередь, на родителей или лиц, их замещающих. В случае, если складывается ситуация, в которой ребенок оказывается вовлеченным в кибертравлю, учитель может поделиться данными рекомендациями с родителями и совместно с ними обеспечивать их выполнение.

1. Родитель должен быть в курсе того, какую активность проявляет ребенок онлайн, какие сайты посещает. Также он ставит ребенка в известность о том, что как человек, который отвечает за его безопасность, он может интересоваться тем, что он делает в Интернете, если будут веские причины для беспокойства.
2. Программу «Родительский контроль» поставить можно, но это не панацея, не стоит на нее полностью полагаться.
3. Если родителю удастся проявить искренний интерес к самым любимым сайтам ребенка и узнать о них побольше (и от ребенка, и покопавшись в них самим), это будет хорошим фактором повышения кибербезопасности ребенка.
4. Хорошо, если ребенок согласится «дружить» с родителем в социальных сетях. Если он отказывается, это его право, но, может быть, он согласится дружить при этом с каким-то другим взрослым, с которым у родителя есть контакт (например, со старшим братом или сестрой, хорошим другом семьи и т.д.).
5. Родитель должен спросить у ребенка пароли от его аккаунтов и пообещать, что воспользуется ими только в случае крайней необходимости. И обязательно сдержать слово. Попытки «шпионить» за детьми приводят зачастую к быстрому разоблачению родителей и полному исчезновению доверия со стороны ребенка. После этого у родителя остается очень мало шансов узнать о происходящем, если ребенок действительно окажется в опасной ситуации.
6. Договориться с ребенком о том, что он сразу же расскажет родителю, если окажется в ситуации кибербуллинга, и заверить его в том, что при этом родитель не отберет у него телефон или компьютер. И сдержать слово.

Родитель должен обучить ребенка некоторым правилам безопасности в сети:

- Научить детей хорошенько думать о том, что они постят в сети. Научить никогда не делиться чем-то, что потом может их поставить в неловкое положение: единожды будучи помещенной в сеть, информация перестает принадлежать автору — это очень важно усвоить.
- Предложить детям задуматься над тем, кому, по их мнению, может иметь доступ к их личной информации: будет ли их страница открыта для всех или только для друзей, или друзей друзей и т.д.

- Научить детей ни с кем (кроме родителя, см. условия выше) не делиться своими паролями.

Если кибербуллинг уже имеет место:

- не отвечать на оскорбительные сообщения и не пересылать их;
- сделать скриншоты, оставить доказательства того, что нападение имело место;
- заблокировать того пользователя, от которого исходят оскорбительные сообщения;
- сообщить провайдеру или руководству соцсети или сайта о том, что правила их сервиса нарушаются (в случае с кибербуллингом это почти всегда так).