**Рекомендации родителям по техническому контролю**

1. Используйте инструменты родительского контроля. Функции родительского контроля можно использовать как в браузерах, так и в антивирусных программах. Например, в ESET NOD32 SmartSecurity, KasperskyInternetSecurity предусмотрен модуль «Родительский контроль». Кроме того, вы можете выбрать специальное мобильное приложение – ESET NOD32 Parental Control для Android. Существуют подобные инструменты для игровых приставок, таких как NintendoWii, Playstation и Xbox 360. Особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local Microsoft\Windows\Temporary InternetFiles в операционной системе).

2. Не разрешайте детям публиковать в интернете личную информацию. Запомните и объясните детям, что конфиденциальная информация никогда не запрашивается по электронной почте или в чате.

3. Не удаляйте сообщения агрессора, история сообщений послужит доказательством акта воздействия.

4. Объясните подростку, что далеко не вся информация в интернете достойна доверия.

5. Ведите с ребенком открытый диалог. Ключевую роль в обеспечении безопасности детей играет общение с ними. Разговоры о безопасности, страхах и проблемах намного эффективнее наказаний. Доброжелательная атмосфера в семье и открытый диалог способствуют успешному развитию ребенка.

6. Все, что попало в интернет, останется там навсегда. Объясните детям, что информация, проиндексированная поисковыми системами, навсегда останется в Сети. Хуже того, после публикации пользователь теряет контроль над своими данными, любой может использовать и распространять эту информацию. Пусть дети возьмут за правило никогда не публиковать фотографии, статусы и другой контент, который они не хотели бы показывать родителям или родственникам. Это распространяется на соцсети, мессенджеры, блоги и другие сервисы.

7. Не рекомендуется создавать для ребенка учетную запись с правами администратора. Учетная запись с правами администратора должна использоваться только взрослыми. Для детей – учетная запись с правами обычного пользователя.

8. Настройте использование https. Убедитесь в том, что ваш ребенок открывает сайты с защищенным протоколом https (наименование протокола отображается в адресной строке браузера). Это позволит избежать перехвата информации – данные передаются в зашифрованном формате, который не распознают вредоносные программы. Посоветуйте детям-подросткам использовать эти настройки и при доступе к соцсетям через публичный Wi-Fi.

9. Используйте надежные пароли. Напомните детям, что пароли нельзя передавать или давать на время даже лучшим друзьям.

10. Настройте параметры безопасности для социальных сетей. Параметры безопасности в соцсетях, установленные по умолчанию, не гарантируют безопасности. Рекомендуется посвятить немного времени их правильной настройке и проверить, какая информация находится под угрозой утечки.

11**. Не забывайте про периодический контроль виртуальных друзей и сообществ, с которыми подросток общается.**

**По интересующим Вас вопросам Вы всегда можете обратиться к специалистам социально-психолого-педагогической службы колледжа по тел. 98-53-50 или прийти на консультацию.**