



Утверждаю.

Директор МАОУ гимназии № 40

Е.В. Качаловская

Приказ от 17.03.2026 № 133

Инструкция № 4 по правилам безопасного поведения в сети интернет

Правило 1. Храните тайны

В информационном пространстве нам часто приходится вводить свои данные: ФИО, адрес, дату рождения, номера документов. Безопасно ли это?

Персональные данные (имя, фамилия, адрес, дата рождения, номера документов) можно вводить только на государственных сайтах или на сайтах покупки билетов. И только в том случае, если соединение устанавливается по протоколу https. Слева от адреса сайта должен появиться значок в виде зеленого замка — это означает, что соединение защищено.

Вряд ли ребенку потребуется регистрация на государственных сайтах, но даже если она нужна, делать это в любом случае надо под руководством родителей. Важно помнить, что ни в коем случае нельзя передавать через Сеть данные любых документов и банковских карт. Даже (и тем более) если кто-то об этом просит, старается убедить в том, что возникла критическая ситуация, торопит и повторяет, что нужно срочно прислать информацию.

Если такая ситуация возникла, ребенку нужно сразу связаться с родителями. Если ему говорят, что никому ничего сообщать нельзя, и пугают неприятными последствиями, тем более следует срочно обо всем рассказать семье. Запугивание и попытки во что бы то ни стало получить сведения говорят о том, что перед вами мошенники.

Правило 2. Будьте анонимны

Создавая свой профиль в социальных сетях, нужно максимально избегать привязки к «физическому» миру.

Нельзя указывать свой адрес, дату рождения, школу, класс. Лучше использовать очевидный псевдоним: по нему должно быть ясно, что это не настоящее имя (ведь использовать ложные данные: «Алексей» вместо «Александр» — по правилам соцсетей запрещено).

Не надо ставить свою фотографию на аватар, если вам не исполнилось хотя бы 15-16 лет. Все дети и подростки младше этого возраста, публикуя свою фотографию, рискуют стать жертвой злоумышленника.

Правило 3. Не Разговаривайте с незнакомцами

Есть несколько главных опасностей, с которыми можно столкнуться в интернете. По большому счету они мало отличаются от тех, что угрожают нам в реальной жизни. Злоумышленники здесь просто используют другие средства.

Буллинг. Ребенка обзывают или травят в интернете — чаще всего без какой-либо причины, «потому что так весело». К жертве могут прицепиться из-за фотографии в профиле или из-за поста в соцсетях.

Мошенники. Пытаются завладеть данными пользователя или втянуть ребенка в опасную финансовую авантюру.

Главное средство защиты от всех этих угроз — конфиденциальность. Нельзя выкладывать свои фотографии в Сеть. Следует ограничить доступ к информации о всех сторонах своей жизни, будь то онлайн или офлайн. Сообщать их можно только проверенным людям: родным, близким и людям, которые знакомы вам лично, а не через интернет.

Тех, кто пытается вас как-то задеть и обидеть (так называемых троллей), нужно просто игнорировать!

Правило 4. Распознайте злоумышленника

На что надо обратить внимание прежде, чем вступить в диалог? Что сигнализирует об опасности?

Вы не знакомы с этим человеком в реальной жизни. Ваш собеседник явно взрослее вас. У него нет или очень мало друзей в соцсети. Собеседник о чем-то просит: сфотографироваться, прислать какие-то данные и т. д.

Правило 5. Храните фото в недоступном месте

Правила публикации собственных фотографий очень простые — если вы не хотите, чтобы они стали достоянием общественности, нельзя выкладывать их в интернет и отправлять кому-то с его помощью. Вообще. Даже мессенджеры «умеют» копировать переписку в «облако», так что вы можете потерять контроль над своими снимками.

Если что-то куда-то было отправлено или где-то опубликовано, это ушло в Сеть. Важно помнить, что ни в коем случае нельзя выкладывать фотографии документов — своих или чужих. А фото других людей стоит выкладывать только в случае, если они на это согласны.

Правило 6. Будьте бдительны

Плохая новость — удалить ничего не получится.

Все, что попало в Сеть или даже в смартфон, останется там навсегда. Как правило, стереть данные из Сети невозможно. Единственный способ избежать утечки информации — не делиться ею.

Правило 7. Не сообщайте свое местоположение

Данные геолокации позволяют всему миру узнать, где вы живете и учитесь, проводите свободное время, в каких акциях участвуете, какие шоу и спектакли любите, как отдыхаете. Отследить местоположение человека теперь не составляет труда.

Для ребенка это может представлять большую опасность. Но полностью отключить геолокацию на детском телефоне нельзя. Родителям полезно использовать специальные программы, чтобы знать, где находится ребенок.

Чтобы сделать геолокацию максимально безопасной, нужно следить за тем, чтобы местоположение не отображалось на «искабельных» объектах — особенно на фотографиях. На телефонах, в настройках камеры, как правило, можно запретить геометки.

Правило 8. Внимание — на игры

Правила безопасности есть не только в соцсетях и мессенджерах. Все основные угрозы могут исходить и от онлайн-игр.

Там вы даже более уязвимы, поскольку вами проще манипулировать: игровые объекты, членство в командах, внутриигровые социальные связи — все это может стать механизмом манипуляции для мошенников, педофилов или даже вербовщиков различных экстремистских группировок. Вот почему в игре нужно вести себя особенно внимательно.

Правило 9. Главный секрет безопасности в сети

Не нужно делать в интернете ничего, что бы вы не стали бы делать в физическом мире. Разница между виртуальной и реальной действительностью минимальна.

Ответственный за ТБ



Е.Н. Невкипелова