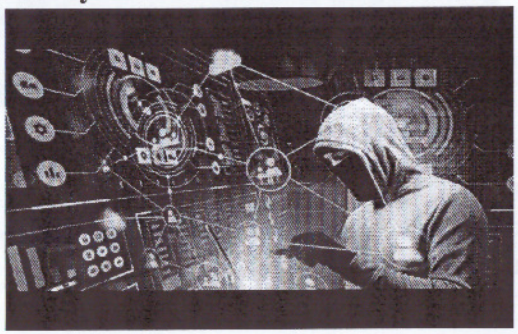
- Не выходить в интернет без разрешения взрослых.
- Не более 30 минут в день перед экраном устройства.
- Разрешено использовать только определенные приложения (например, YouTube с безопасным поиском или веб-браузер с фильтрами).
- Спрашивать разрешения для установки игр.
- Можно записать эти правила и время от времени обновлять их.

Когда ваш ребенок станет старше, ему, вероятно, понадобится дополнительная свобода. **Можно немного расширить правила, чтобы они включали следующее:**

- Никогда не называть свое настоящее имя и адрес в интернете.
- Не авторизовывать платежи в приложениях без разрешения.
- Избегать сомнительных приложений.
- Не публиковать свою личную информацию и интимные фотографии.
- Обратиться к взрослым, если кто-то пытается заставить совершить нежелательные действия.

По мере того, как ребенок вступает в подростковый возраст, придется придумывать правила, поддерживающие его жизнь в сети. С детьми более старшего возраста можно совместно создавать полезные, но не ограничивающие правила.

Выше приведены только примеры правил, которые вы можете использовать. Каждый ребенок индивидуален и имеет уникальные потребности, поэтому вам придется разработать правила, подходящие именно вашему ребенку.



Отрадненский район,
ул. Первомайская, 10
Тел. 8 (86144)3-43-05

МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОГО РАЗВИТИЯ
КРАСНОДАРСКОГО КРАЯ

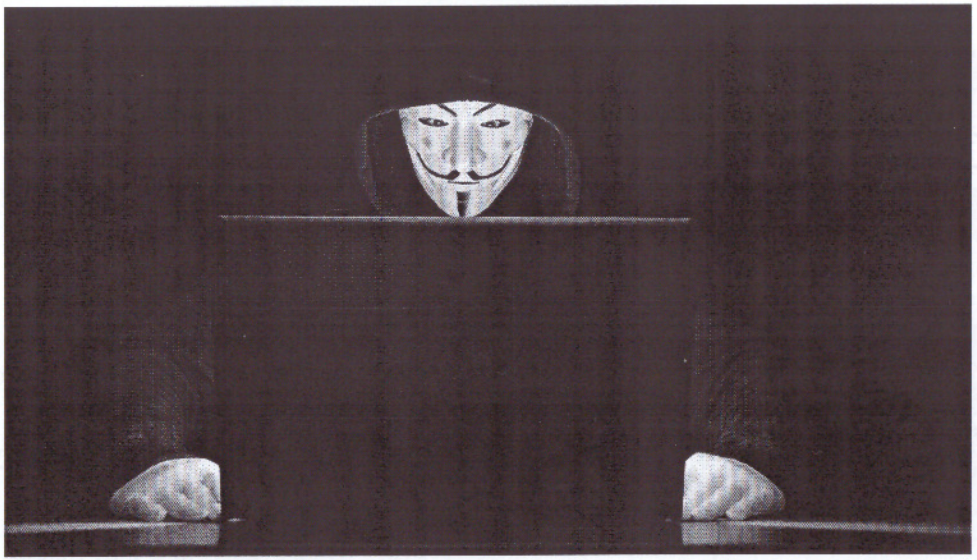
ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ КРАСНОДАРСКОГО КРАЯ «ОТРАДНЕНСКИЙ

СОЦИАЛЬНО РЕАБИЛИТАЦИОННЫЙ ЦЕНТР ДЛЯ НЕСОВЕРШЕННОЛЕТНИХ»

ОТДЕЛЕНИЕ ПОМОЩИ СЕМЬЕ И ДЕТЯМ

Памятка

«Кибертерроризм»



Ст.Отрадная

Кибертерроризм — это запланированная кибератака на информационные системы, программы и данные, приводящая к насильственным действиям, которая направлена на достижение политических или идеологических мотивов преступников.

В целом, существует три категории угроз, с которыми дети сталкиваются в интернете:

Незнакомцы. Злоумышленники скрываются на сайтах, привлекающих детей, таких как сайты социальных сетей и онлайн-игр. Такие злоумышленники часто сами притворяются детьми. Этот метод называется кэтфишинг. Также существуют хакеры и киберпреступники, атакующие всех пользователей с недостаточно высоким уровнем безопасности, не важно, ребенок это или взрослый. Они также могут попытаться обманом выяснить у ребенка пароли или платежную информацию.

Сверстники. Ваш ребенок может подвергаться издевательствам или травле со стороны своих знакомых. Это часто происходит в личных чатах в социальных сетях и приложениях для обмена сообщениями. Иногда другие дети могут публиковать личную информацию вашего ребенка, что доставляет ему сильные страдания. Если такая информация имеет сексуальный характер, например интимные фотографии, это может быть уголовным преступлением.

Самостоятельно. Дети без присмотра могут сами создать для себя опасные ситуации в сети. Они часто нажимают кнопки или устанавливают программное обеспечение, не понимая последствий своих действий, а также публикуют личную информацию, например дату рождения или адрес.

Некоторые из этих угроз являются **социальными угрозами** – они связаны с вымогательством или манипуляциями. Часто незнакомец завоевывает доверие ребенка, а затем пользуется этим. Чтобы защититься от этих угроз, ребенку необходимо знать, как безопасно общаться с другими людьми.

Другой тип угроз – это **цифровые угрозы**, когда кто-то использует технологии для доступа к данным. Это могут быть вредоносные программы (например, для кражи личных данных), или фишинг (вынуждение обманным путем посетить поддельный веб-сайт). Для защиты от такого типа угроз необходимо объяснить ребенку, как правильно использовать интернет и установить надежные антивирусные программы.

Установите основные правила работы в интернете

Интернет – огромное запутанное место, в котором хорошо бы опираться на несколько базовых правил, которые помогут понять, как оставаться в безопасности.

Вместе с ребенком договоритесь о нескольких основных правилах использования им интернета. Для маленьких детей эти правила должны быть понятными и простыми для выполнения. **Например, правила могут быть такими:**