# АЛГОРИТМ
## выявления противоправного контента на мобильных устройствах несовершеннолетних

В современных условиях родитель должен работать на опережение той противоправной информации, которая консолидируется в мобильном устройстве «гаджете» нашего ребенка, не упустить момент, когда можно предотвратить негативные последствия. И дело здесь не в доверии или недоверии к собственному ребенку. Дело в том, что сейчас как раз преступный элемент работает на опережение, предлагая нашим детям в изобилии противоправный контент (предложения так называемого «трудоустройства» «закладчики», «кладмены»., агрессивная реклама противоправного поведения несовершеннолетнего, популяризация преступного образа жизни и.т.д).

В связи с этим прошу Вас обратить внимание на следующую информацию, так называемый «Алгоритм» выявления противоправного контента на мобильных устройствах несовершеннолетних.

**ПРИЗНАКИ.**

**1.** Что такое Мессенджер – это программа, мобильное приложение или веб-сервис для мгновенного обмена сообщениями. (Первопричина, по которой преступный элемент использует именно нижеперечисленные мессенджеры, это их защищенность и прогрессивные алгоритмы шифрования, проще говоря их нельзя взломать).

Итак, для Вашего обозрения представлены мессенджеры, наиболее часто используемые в преступной деятельности (если в «гаджете» вашего ребенка есть подобный мессенджер стоит обратить на это внимание):

- **Telegram;**
- **Signal;**
- **Jabber;**
- **Vipole.**

**2.** Что такое Браузер – в основе браузера лежит технология анонимизации пользователей, другими словами это программы создающие подложный ip-адрес (ананимайзер). Принцип анонимизации заключается в том, что информация об адресе предыдущего узла на каждом новом узле, куда пришли данные, отсутствует. Таким образом, никто не может узнать откуда пришел запрос на сервер, то есть откуда и с какого ПК человек выходил в сеть.

Обратите внимание на наличие скаченного браузера TOR и VPN-сервиса. Данные программы предназначены для работы в так называемом Даркнете (темной, скрытой сети) для ухода в глубокий вэб. Таким образом, файлообмен и иная передача данных происходит в Даркнете анонимно (поскольку IP адреса недоступны публично, следовательно пользователи могут общаться без опасений и гос.вмешательства + IP адрес другого государства, а это проблемы с блокировкой данного контента. Соответственно Роскомнадзор не сможет заблокировать. В большинстве случаев данные браузеры связаны с незаконной деятельностью и инакомыслием.

МЕХАНИЗМ — Скачивается приложение TOP или иные (Регистрация) — выход на торговую площадку Амазон (своеобразный виртуальный торговый центр) — оплата (карта, биткоины) — после получение координатов закладки и фотографии места.

ЧТО ДЕЛАТЬ —

1. Обеспечить контроль гаджета вашего ребенка, изучать переписки и установленные программы.
2. Ограничить контент в гаджете вашего ребенка, использовать функциональные возможности сервиса iCloud (так называемого облачного хранилища) и использование средств родительского контроля на iPhone, iPad и iPod touch (это для системы «яблочных» устройств. Для системы Андроид существует аналогичный механизм.
3. Установить приложения, которые родители могут самостоятельно установить на мобильные устройства своих детей или домашние компьютеры, так и продукты, предназначенные для фильтрации трафика на уровне операторов связи.