ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ
ПО ОБНАРУЖЕНИЮ НЕЖЕЛАТЕЛЬНОГО КОНТЕНТА
НА МОБИЛЬНЫХ УСТРОЙСТВАХ НЕСОВЕРШЕННОЛЕТНИХ

Защита детей от закачки контента с нежелательным содержанием.

1. Операторы предоставляют возможность просмотра всех расходов определенного мобильного номера. Следует договориться с ребенком, что вы будете просматривать эти данные или включить эту услугу без его ведома, но для этого вам нужен телефон ребенка.

2. Выяснив, что ребенок использовал услуги контент-провайдера, следует позвонить в call-центр оператора и узнать:

- какому контент-провайдеру принадлежит этот короткий номер или WAP-портал;
- какого рода информация предоставляется через данный сервис;
- есть ли на этом портале информация запрещенного характера;
- контактный адрес call-центра контент-провайдера.

3. В call-центре контент-провайдера вы можете узнать, какой контент был заказан с номера вашего ребенка, при этом не следует информировать, что это не ваш личный номер. Контент-провайдер может отказаться предоставить такую информацию.

4. Одновременно выясните, какую информацию можно заказать по данному короткому номеру (позвоните на этот номер или зайдите на WAP-портал). Посмотрите в телефоне ребенка сохранилось ли SMS с номером заказанного контента или обратное SMS с WAP-ссылкой либо проверьте историю страниц, которые посещал ребенок в браузере телефона. Если Вы убедились в том, что сервис, которым пользовалась Ваш ребенок содержит запрещенную информацию и эту информацию ребенок уже получил, нужно обратиться к call-центр оператора.

Дети в Интернет.

Проблема безопасности детей в сети Интернет уже не кажется России такой далекой. Никто не может отрицать, что на сегодняшний день она встала особенно остро. Известно, что подростки в период заниженной самооценки ищут поддержки среди своих друзей, а не в семейном кругу. Старшие подростки, желая независимости, нуждаются отождествлять себя с определенной группой и склонны сравнивать ценности своей семьи и своих товарищей.

Что делают подростки в он-лайне.

В он-лайне подростки загружают музыку, используют мгновенные сообщения, электронную почту и играют в онлайновые игры. С помощью поисковых серверов подростки находят информацию любого содержания и качества в сети Интернет. Большинство подростков регистрируются в частных чатах и общаются на любые темы, выдавая себя за взрослых. Дети в этом возрасте предпочитают всё, что выходит за пределы дозволенного: брутальный юмор, насилие, азартные игры, эротические и порно сайты. Девушкам, которые имеют заниженную самооценку, нравится размещать провокационные фото, они склонны на фривольные разговоры, выдавая себя за взрослых женщин, в результате чего становятся жертвами сексуальных домогательств.

Как обеспечить безопасность детей в сети Интернет.

Предлагаем несколько рекомендаций, которые следует принять во внимание:

- размещайте компьютеры с Internet-соединением вне комнаты вашего ребенка;
- поговорите со своими детьми о друзьях, с которым они общаются в он-лайне, узнайте, как они проводят досуг и чем увлекаются;
- интересуйтесь какие веб сайты они посещают и с кем разговаривают;
- изучите программы, которые фильтруют получения информации из сети Интернет, например, родительский контроль в Windows;
- настаивайте на том, чтобы Ваши дети никогда не соглашались встречаться со своим он-лайновым другой без Вашего ведома;
- научите своих детей никогда не предоставлять личную информацию о себе и своей семье в электронной почте и в разных регистрационных формах, предлагаемых владельцами сайтов;
- контролируйте информацию, которую загружает ребенок (фильмы, музыку, игры и т.д.);
- интересуйтесь, не посещают ли дети сайты с агрессивным содержанием;
- научите своих детей ответственному и этическому поведению в он-лайне. Они не должны использовать Интернет для распространения сплетен, угроз другим и хулиганских действий;
- убедитесь, что дети консультируются с Вами, относительно любых финансовых операциях, осуществляя заказ, покупку или продажу через Интернет сеть;
- информируйте детей относительно потенциального риска при их участии в любых играх и развлечениях;
- разговаривайте с детьми как с равными партнерами, демонстрируя свою заботу об общественной морали.

Для недопущения вовлечения несовершеннолетних в противоправную деятельность родителям рекомендуется:

1. **Проверять переписку в социальных сетях** («ВКонтакте», «Одноклассники», «Twitter», «Facebook» и т.п.)

«Вконтакте» **Одноклассники** **Twitter** **Facebook**

и мессенджерах (WhatsApp, Telegram, Signal, Wickr Me) на предмет наличия противоправного контента, а также наличия второго аккаунта.

WhatsApp

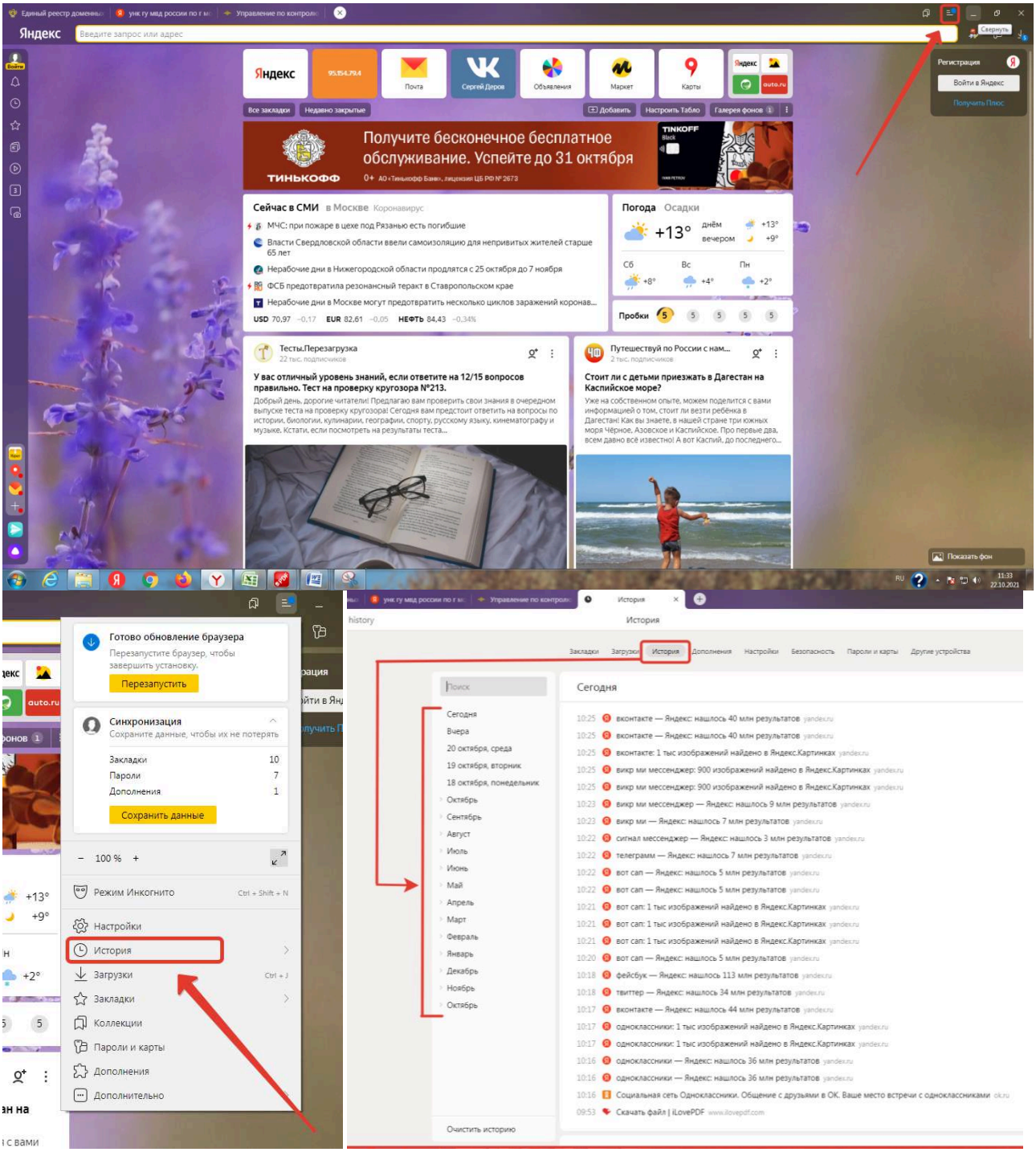
Telegram

Signal

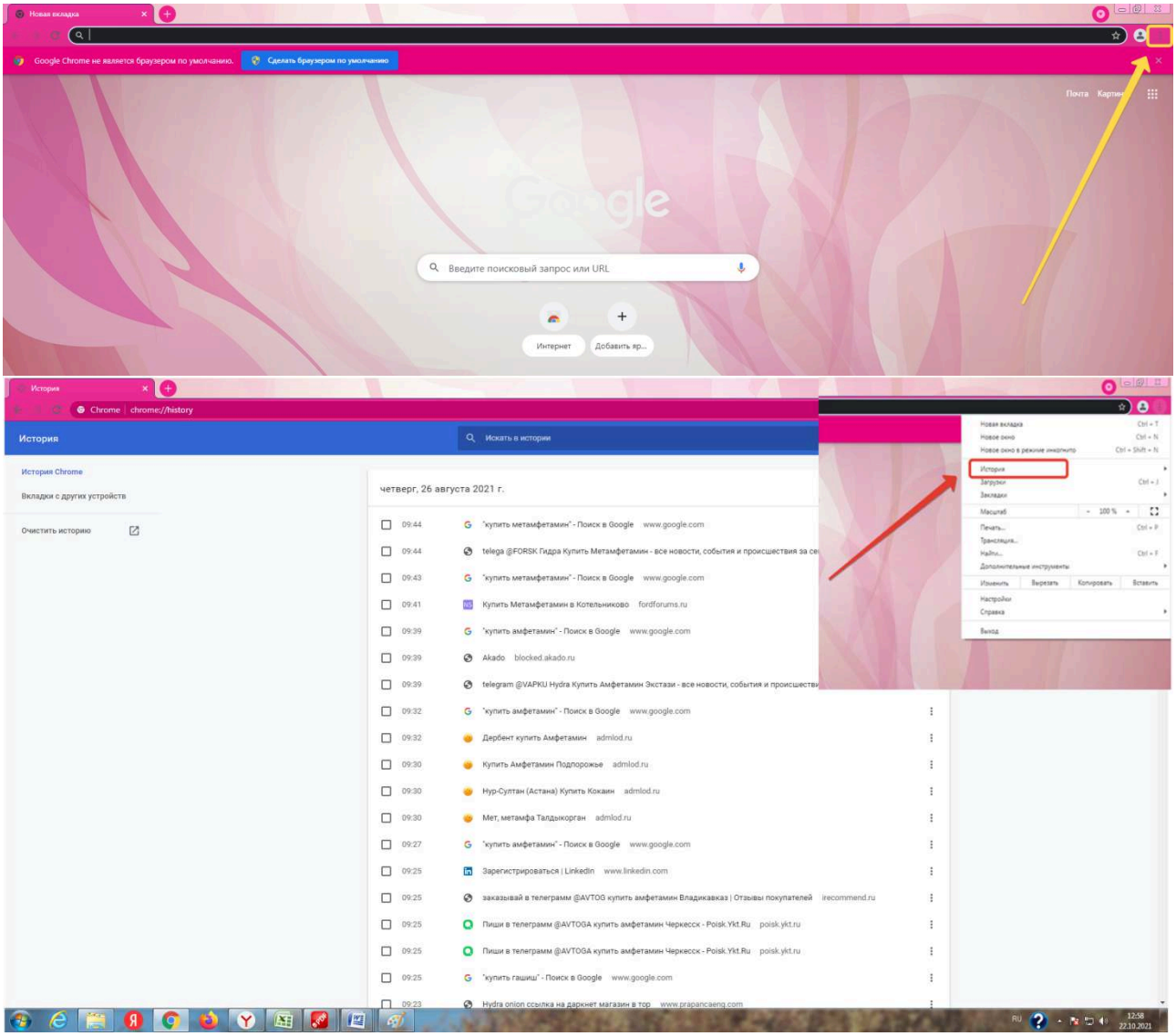
Wickr Me

2. Проверять истории браузера:

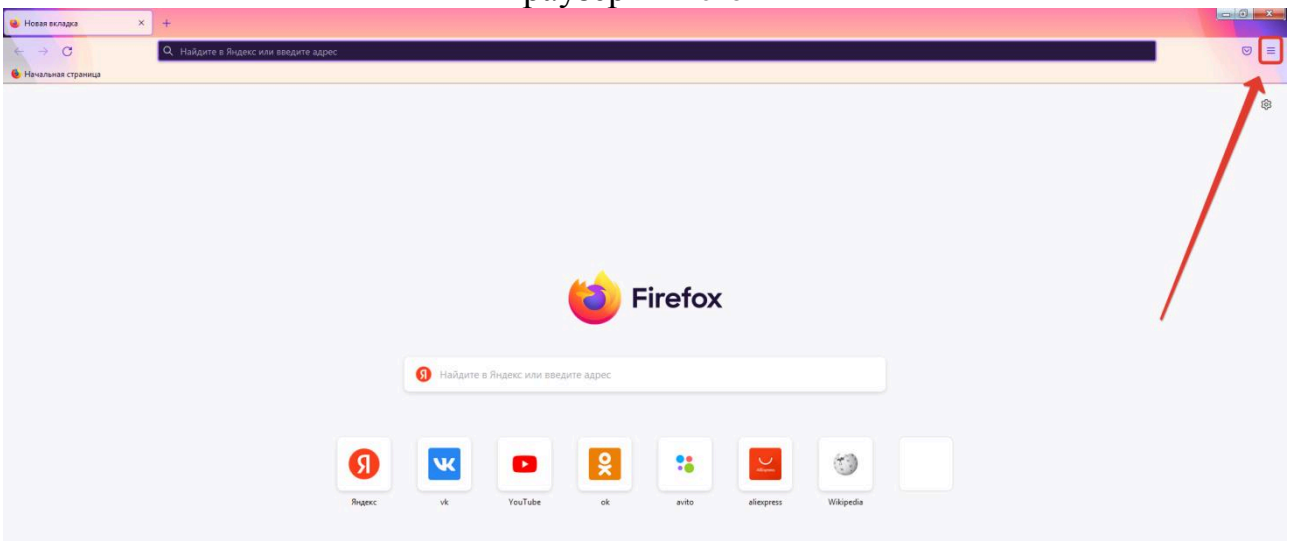
Браузер «Яндекс»

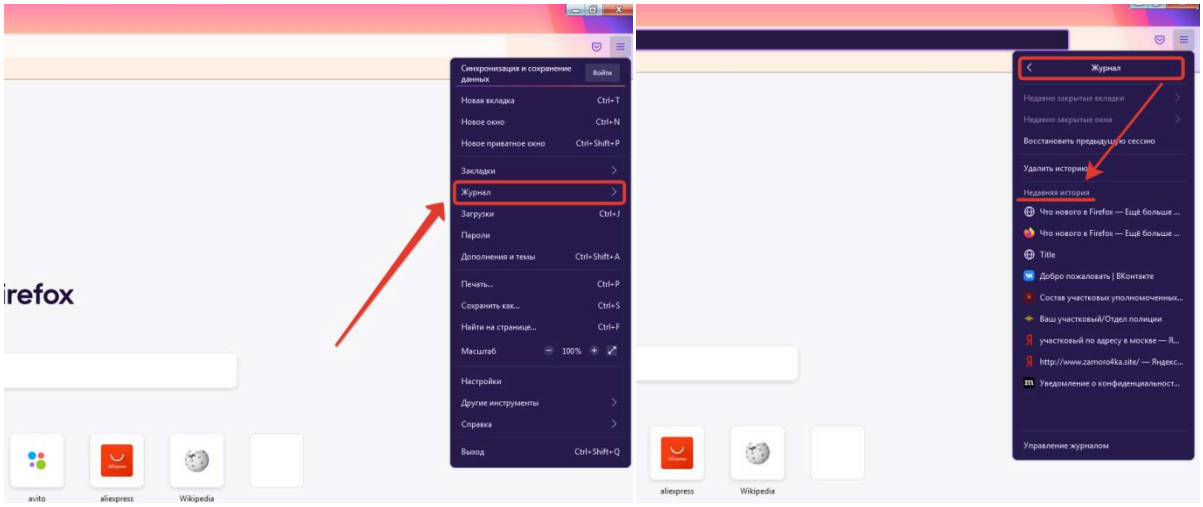


Браузер «Google»



Браузер «Firefox»

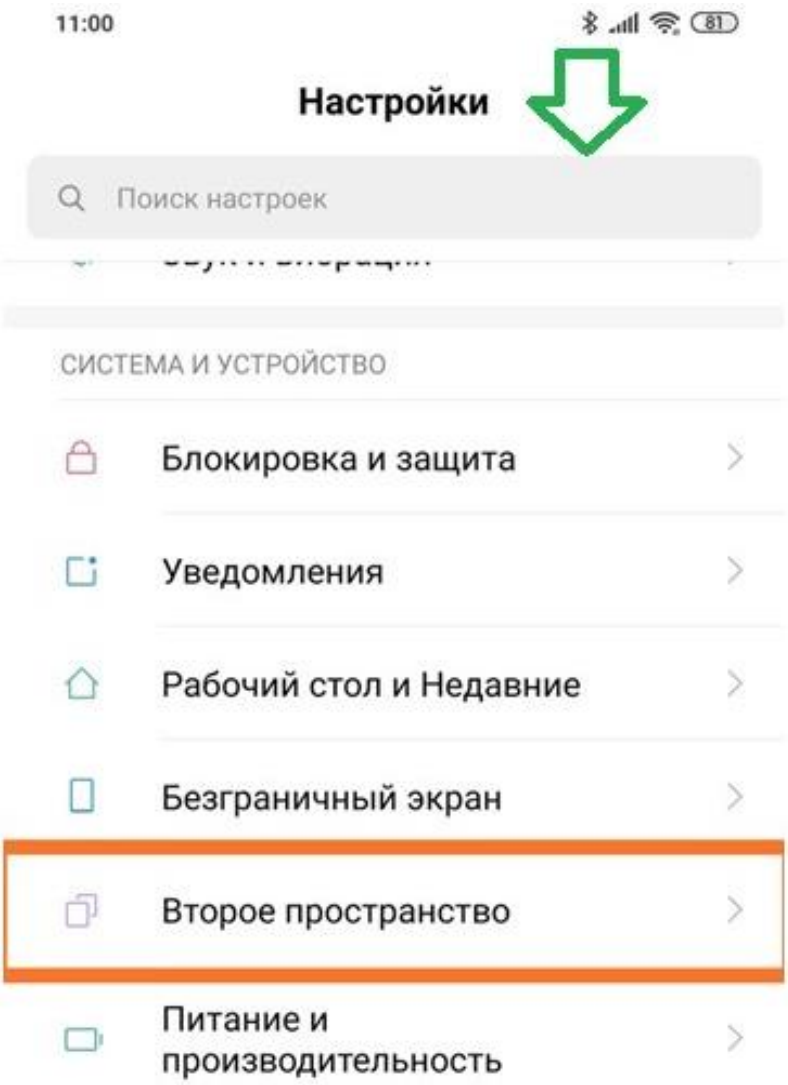




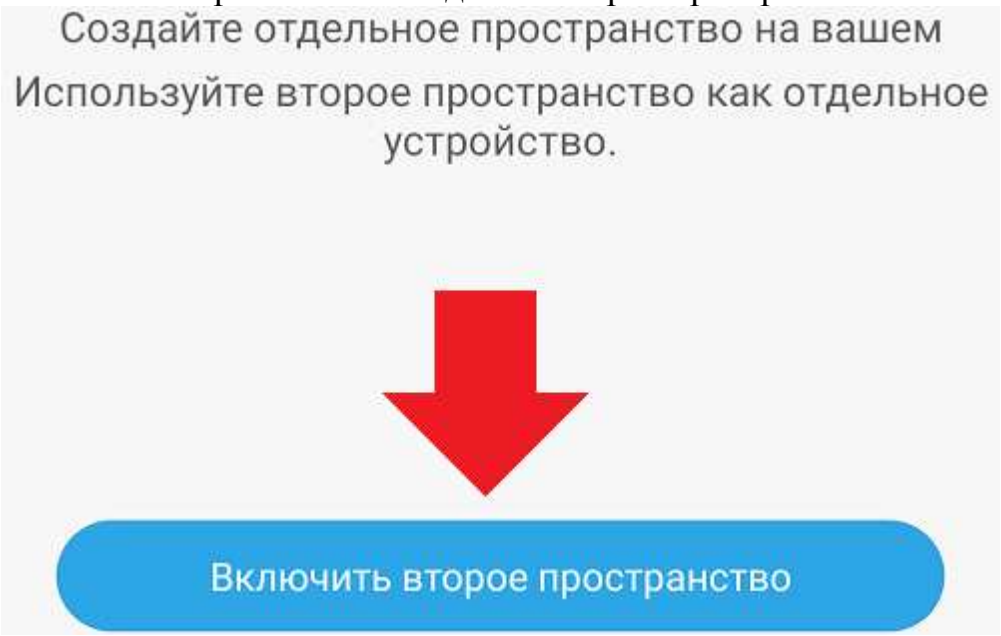
3. Проверьте наличие второго пространства:

- зайдите в меню настроек

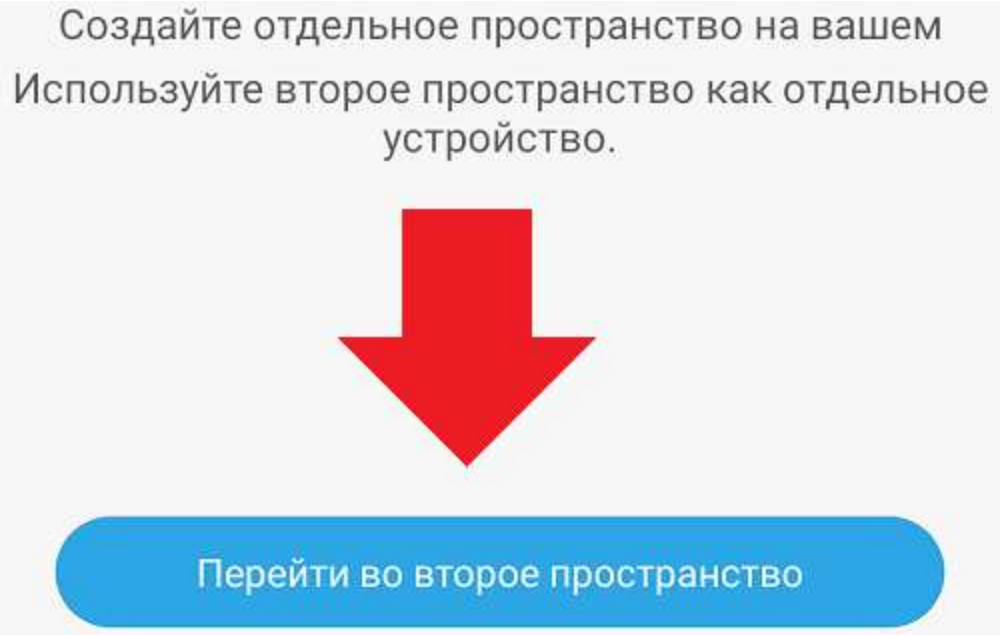
- найдите раздел «Второе пространство» (если в настройках нет кнопки «Второе пространство», то в строке «Поиск настроек», введите слово «второе» и кнопка «Второе пространство» сразу появится)



- в данном разделе вы можете узнать есть ли на телефоне Вашего ребенка «Второе пространство», для этого необходимо зайти в данный раздел. Если появилась кнопка «Включить второе пространство», значит в телефоне Вашего ребенка не создано «Второе пространство».



Если появилась кнопка «Перейти во второе пространство», значит на телефоне Вашего ребенка есть «Второе пространство».



Для того что бы перейти во «Второе пространство», необходимо нажать на кнопку «Перейти во второе пространство». При нажатии на кнопку появится окно для ввода пароля от «Второго пространства», постарайтесь узнать у Вашего ребенка пароль.

(ВАЖНО! После нескольких неудачных попыток ввода пароля «Второе пространство» будет автоматически блокировано или удалено)

4. Проверять устройства, которыми пользуется ребенок на наличие следующего программного обеспечения: браузер «Tor», специальное

программное обеспечения позволяющее обходить блокировки РКМ (VPN/Proxy) Thunder VPN, NordVPN, VPN Master, fiGate VPN & Proxy, Turbo VPN, VPN Booster, Fastway VPN, UFO VPN.

Tor

VPN Proxy Master

Thunder VPN

NordVPN

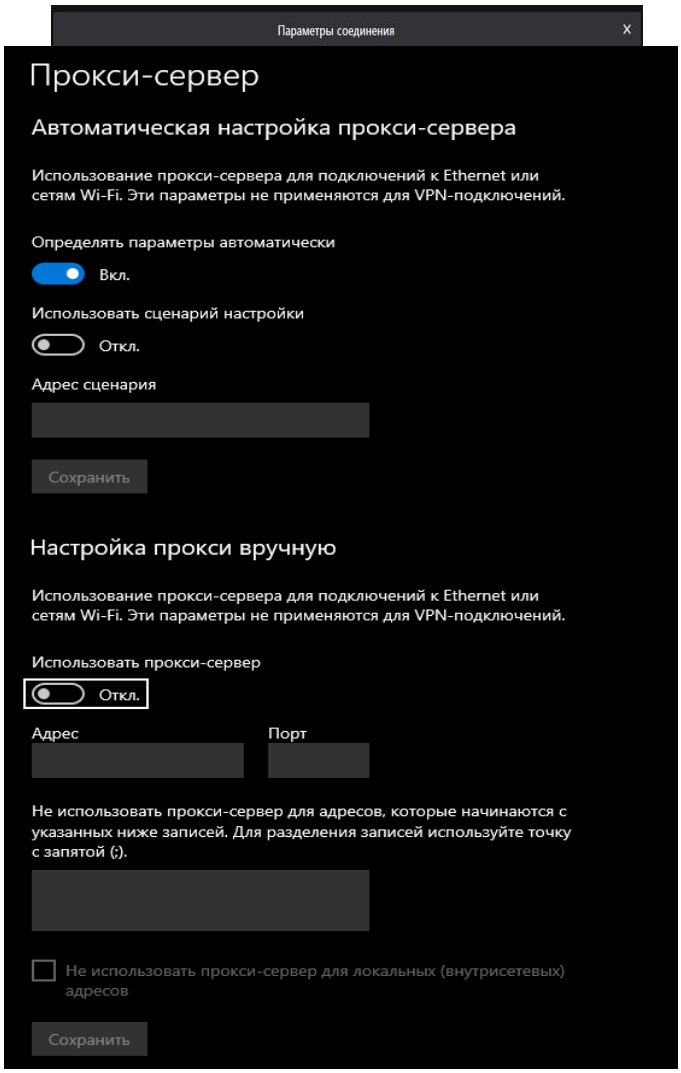
Ultimate VPN

Turbo VPN

VPN Booster

UFO VPN

5. Проверять настройки устройства и браузера на наличие встроенного Proxy/VPN.



6. Проверять установленные **платежные системы** и транзакции, которые осуществляются с их помощью,

Qiwi-кошелек **ЮМани** **Payeer** **PayPal** **WebMoney**

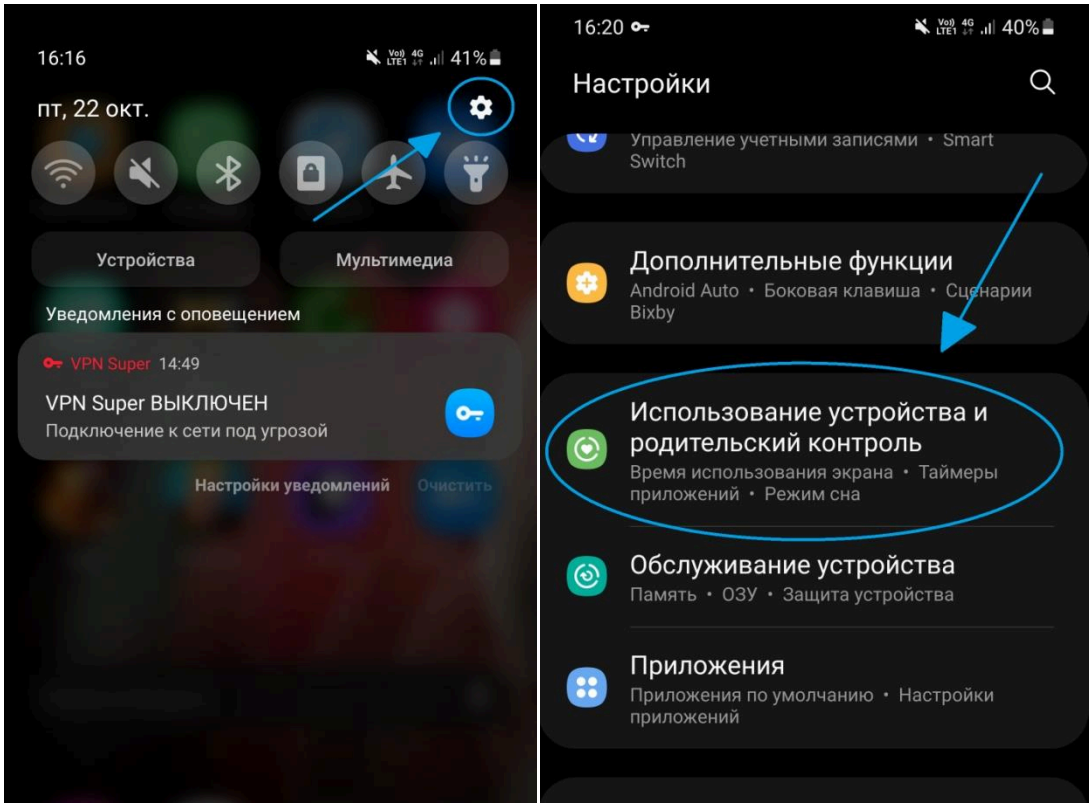
а также **специальное программное обеспечение**, позволяющее взаимодействовать с криптовалютой (Далее, для примера, представлены лишь некоторые программные обеспечения. Если при проверки телефона Вашего ребенка Вы нашли подозрительное приложение, введите его название в интернете, для получения полной информации о нем):

Binance **Perfect Money** **CEX.IO** **Changelly**

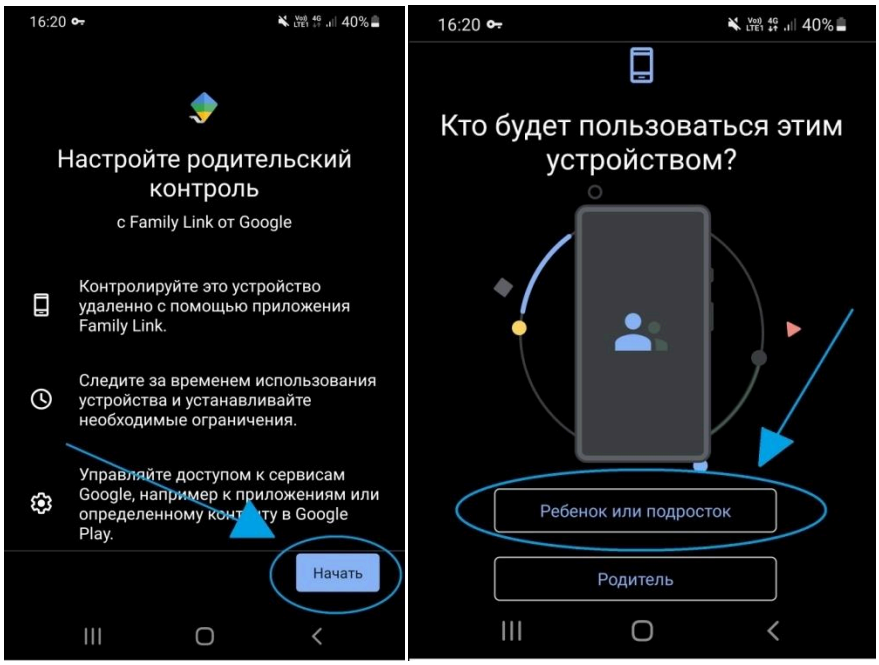
7. Подключите функцию **«Родительский контроль»** на телефоне Вашего ребенка. Данная функция предназначена для того, чтобы оградить Вашего ребенка от противоправного контента, расположенного в открытом доступе в сети Интернет.

Инструкция подключения «Родительского контроля» на ОС Android:

- Откройте «Настройки» на телефоне ребенка и выберете раздел «Использование устройства и родительский контроль» (для быстрого поиска данного раздела, Вы можете воспользоваться строкой «Поиск»)



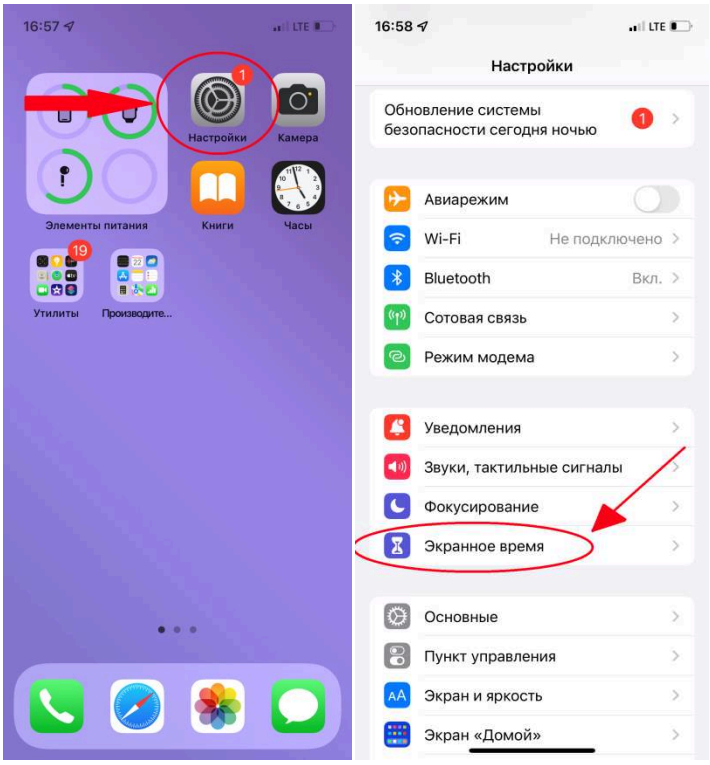
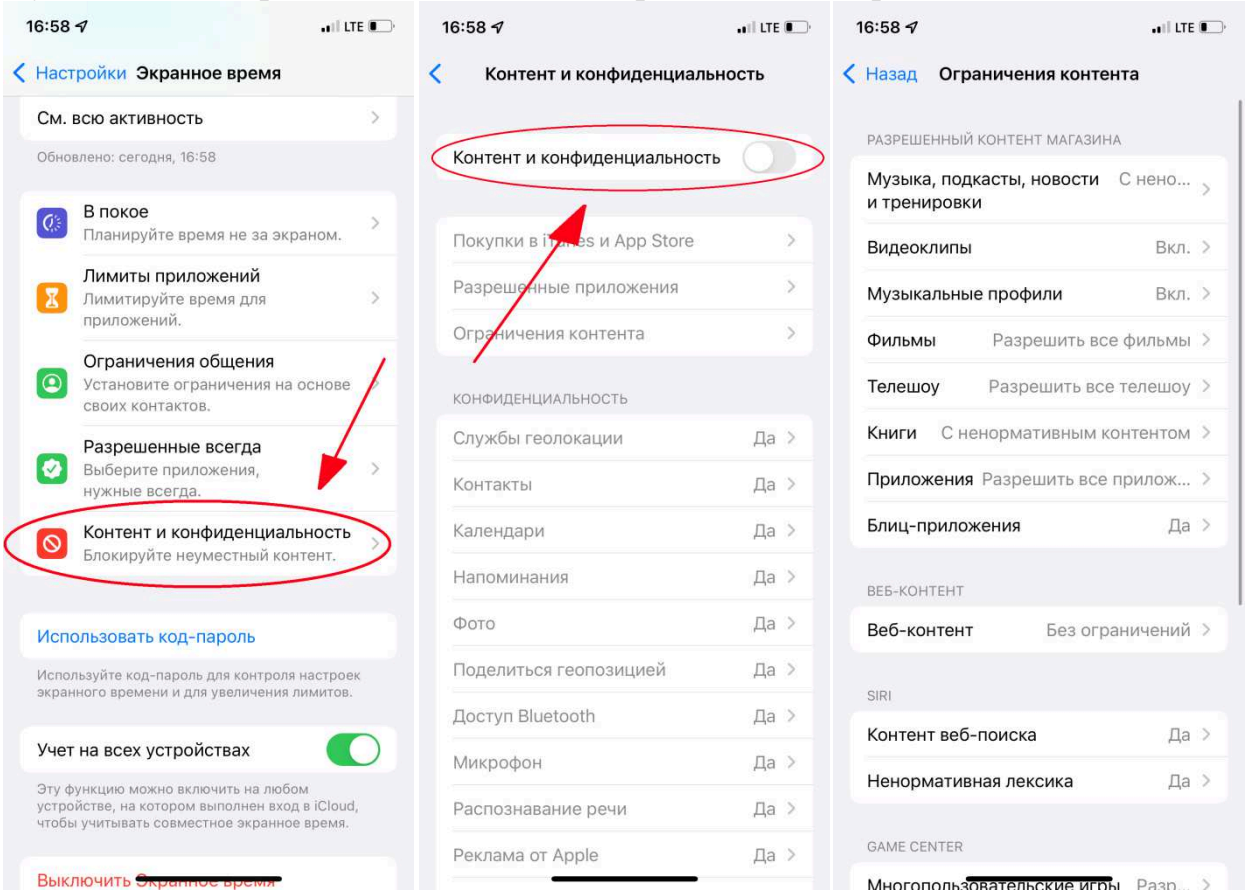
- После перехода в раздел «Использование устройства и родительский контроль» нажмите кнопку «Начать», выберете кто будет пользоваться устройством.



Инструкция подключения «Родительского контроля» на ОС IOS:

Чтобы включить автоматическую фильтрацию содержимого веб-сайтов, ограничить доступ к материалам для взрослых в Safari и приложениях на устройстве Вашего ребенка, выполните указанные ниже действия:

- Перейдите в меню «Настройки» и выберите функцию «Экранное время», нажмите «Контент и конфиденциальность»



- Затем «Ограничение контента». В зависимости от предоставленного доступа может потребоваться добавить определенный адрес веб-сайта и тд.