|  |  |
| --- | --- |
|  | **Открытые Wi-Fi сети**– это общедоступные беспроводные сети, используемые для подключения к сети Интернет в общественных местах (кафе, библиотеки, метро, гостиницы и т.д.). |

**Как защитить себя и свои данные при работе с такими сетями через мобильные устройства (сотовые телефоны, планшеты, ноутбуки):**

1. Не доверяйте таким сетям, особенно если для подключения к ним отсутствует пароль. Однако, даже его наличие не гарантия вашей безопасности. Ими можно пользоваться только для просмотра новостей, фильмов, статей.
2. Нельзя во время их использования подключаться к Госуслугам, социальным сетям, сервисы покупки авиа- или железнодорожных билетов – к тем сервисам, в которых хранится или вводится информация, связанная с вашей личной жизнью.
3. Проверяйте названия таких сетей перед подключением. Злоумышленник может создать копию сети, изменив название на один знак, букву или цифру.
4. Отключите на ваших устройствах в настройках Wi-Fi автоматическое подключение к таким сетям. В этих же настройках через функцию «Забыть сеть» исключите уже известные устройству сети. Лучше вообще отключать Wi-Fi подключение, если вы им не пользуетесь.
5. Не запрещено, но не рекомендуется пользоваться VPNсервисами (приложениями), которые «шифруют» вас от злоумышленников. ОДНАКО! Есть ряд заблокированных Роскомнадзором сервисов, которые нарушают требования российского законодательства: **Hola!VPN, ExpressVPN, KeepSolid VPN Unlimited, Nord VPN, Speedify VPN, IPVanish VPN, VyprVPN, OperaVPN**.
6. Используйте средства защиты информации, типа антивирусов Kaspersky или Dr.Web на временной или постоянной основе.
7. Помните про правила «цифровой гигиены».