Рекомендации

В Костромской области, как и в ряде других регионов России, продолжается периодическое временное ограничение скорости мобильного интернета, при этом ограничивается передача данных, вследствие чего становится невозможным осуществление безналичных платежей, передачи данных в государственные информационные системы (ЕГАИС, Честный знак, УФНС, Меркурий). Соответствующие меры безопасности вводятся для защиты от угрозы БПЛА и FPV-дронов украинского режима.

В качестве альтернативного способа доступа организаций Костромской области могут использовать проводной доступ к сети «Интернет» и организованные на его основе точки доступа Wi-Fi. По информации федеральных органов исполнительной власти, блокировка сетей Wi-Fi не планируется.

На территории Костромской области услуги фиксированного доступа к сети «Интернет» предоставляют:

Провайдер	Официальный сайт	Телефон
ПАО «Ростелеком»	https://kostroma.rt.ru	8 800 300 67 81
ОАО «КГТС»	https://kostroma.net	8 (4942) 45-07-07
ООО «ЛокалНет+»	https://loc-net.ru	8 (4942) 49-40-28
АО «Цифровая сеть «Логос»	https://logos-ktv.ru	8 (4942) 49-60-40 8 (4942) 49-62-42
ООО «МедиаЛан»	https://medialan.ru	8 (4942) 49-41-66
ООО «Связь-энерго»	https://sv-en.ru	8 (4942) 49-40-02
ООО «Аксиома»	https://aksioma-kos.ru	8 (800) 505-38-98

Согласно российскому законодательству, (Федеральный закон от 07.07.2003 № 126-ФЗ «О связи», Постановление Правительства РФ от 31.12.2021 № 2607 «Об утверждении Правил оказания телематических услуг связи», Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию») для подключения к точке доступа Wi-Fi требуется идентификация пользователя. Она может производиться несколькими способами: подтверждение по номеру телефона, SMS с кодом, авторизация через портал госуслуг. При организации общедоступной точки Wi-Fi данную идентификацию обеспечивает оператор связи, который может организовать данную идентификацию и организациям, планирующим организовать такую точку доступа.

Меры безопасности при подключении к открытым точкам Wi-Fi

Общественные Wi-Fi-сети не рекомендуется использовать для передачи важных сведений. Эксперты предупреждают, что злоумышленники могут получить доступ к личной информации, включая логины и пароли, платежные данные, документы и переписку. Также необходимо внимательно проверять названия точек доступа. Мошенники создают фишинговые сети с похожими именами, чтобы перехватить данные пользователей. Рекомендуется отключать автоматическое подключение к Wi-Fi и удалять из памяти мобильного устройства общественные сети после использования. Это снижает

риск случайного подключения к вредоносной сети. Важно также регулярно обновлять операционные системы мобильных телефонов, а для дополнительной безопасности - установить антивирусные программы для защиты от вредоносных программ.