

*Бочкарев Кирилл Олегович,
студент магистратуры,
1 курс, факультет «Информационные технологии и управление»
Южно-Российский государственный политехнический университет
Россия, г. Новочеркасск
Каплина Марина Сергеевна,
канд.экон.наук. доцент, кафедры автоматике и телемеханики,
ЮРГПУ (НПИ) им. М.И. Платова
Россия, г. Новочеркасск*

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОЙ СВЯЗИ

***Аннотация:** В статье рассмотрены проблемы обеспечения бесперебойной связи. В процессе исследования были описаны частотные диапазоны мобильной связи в России, основные технологии блокировки мобильной связи и интернета, изучены альтернативные способы связи. Найдены возможные альтернативные способы связи, включая МАХ, которые могут помочь обеспечить связь при полном отключении мобильной связи и интернета.*

***Ключевые слова:** бесперебойная связь, диапазоны частот, мобильная связь, технологии блокировки, альтернативные способы связи, МАХ.*

***Annotation:** The article discusses the problems of ensuring uninterrupted communication. The study describes the frequency ranges of mobile communication in Russia, the main technologies for blocking mobile communication and the Internet, and explores alternative methods of communication. The article identifies possible alternative methods of communication, including MAX, which can help ensure communication in the event of a complete shutdown of mobile communication and the Internet.*

Key words: *uninterrupted communication, frequency bands, mobile communication, blocking technologies, alternative communication methods, MAX.*

В эпоху цифровизации скоростной интернет и стабильная мобильная связь для обычных пользователей стали общепринятыми явлениями. Но на сегодняшний день для нашего государства актуальной проблемой стала безопасность определённых объектов, предприятий и простых граждан.

В условиях 2025 года вопросы обеспечения безопасности критической информационной инфраструктуры, включая сети связи, вышли на первый план. Это потребовало от государства и телеком-компаний найти баланс между внедрением необходимых защитных механизмов и сохранением стабильного, бесперебойного доступа к услугам связи для населения и экономики.

Таблица 1.

Частотные диапазоны мобильной связи в России

Устройство / Система	Диапазоны частот	Ключевые особенности и примеры
Мобильная связь (Россия)	0.7 ГГц, 0.8 ГГц, 1.8 ГГц, 2.6 ГГц, др. (4G/LTE)	"Золотой диапазон" 3.4-3.8 ГГц занят силовыми структурами и не доступен для 5G.

Подавление связи (глушение) — ключевой метод. В России эту задачу выполняют подразделения радиоэлектронной борьбы (РЭБ) и, согласно законодательным инициативам, ФСБ может запрашивать отключения интернета у операторов.

Устройства подавления (глушилки) работают по принципу создания мощных помех в определенных диапазонах частот. Они могут быть нацелены на конкретные стандарты связи, такие как GSM, 3G, 4G (LTE), Wi-Fi и GPS/ГЛОНАСС, делая невозможным установление соединения для выхода в интернет. Важно отметить, что современные подавители способны работать в широком спектре частот, заглушая все основные диапазоны сотовой связи,

что приводит к полной недоступности мобильной сети на локальной территории.

С весны 2025 года в России резко возросло число временных отключений мобильного интернета, которые власти объясняют необходимостью [1]. По данным на конец ноября 2025 года, из 85 российских регионов 55 подвергаются постоянной блокировке мобильного интернета. В некоторых случаях, как это было в Белгородской области и Москве, отключения носят массовый характер и затрагивают целые регионы. Власти некоторых областей, например, Ульяновской, уже заявили о блокировке мобильного интернета «до окончания СВО на Украине».

Таким образом, противостояние в эфире развивается по принципу «щита и меча». С одной стороны, разработчики внедряют все более изощрённые средства связи, включая защищённые протоколы и альтернативные каналы управления (например, через спутники). С другой — системы РЭБ и организационные меры по отключению связи становятся мощнее и масштабнее, неизбежно затрагивая гражданское население.

Основные технологии блокировки представлены на рисунке 1.



Рисунок 1. Технологии блокировки [2]

Решения о применении этих мер принимаются силовыми ведомствами. федерального уровня для обеспечения безопасности [3] возле объектов особого назначения.

В ситуации, когда мобильная связь и интернет недоступны, пользователи вынуждены искать обходные пути. Таким образом альтернативой связи в условиях блокировок могут быть:

– Проводная телефонная связь - это одна из немногих технологий, которая может оставаться рабочей при подавлении сотового сигнала. Однако она обеспечивает только голосовую связь, недоступна для всех (требует наличия стационарного аппарата) и, как показывает практика, в некоторых случаях может отключаться вместе с мобильным интернетом.

– Спутниковый интернет [4] и Mesh-сети (децентрализованные беспроводные сети) как способ обхода блокировок.

Ещё одним возможным вариантом является новый российский мессенджер МАХ. В условиях нестабильной связи многие обращаются к российскому мессенджеру МАХ.

"Белые списки". При отключении интернета пользователям остается доступен ограниченный перечень сайтов. В него входят социально значимые сервисы, такие как "Госуслуги", сайты правительства, навигаторы, сервисы такси, маркетплейсы и личные кабинеты операторов. Но несмотря на заявления Минцифры о едином стандарте, операторы связи жалуются на хаос и отсутствие согласованных правил формирования этих списков у разных компаний. Это снижает эффективность мер и усложняет жизнь пользователям.

Проблема «глушения» и «белых списков» заключается в следующем: при подавлении сигнала РЭБ воздействует на физический уровень связи — радиоканал. Это нарушает работу любого устройства или приложения, использующего этот канал. Когда оператор по требованию властей полностью отключает мобильный интернет или переходит на режим «белых списков», пользователи лишаются доступа ко всем незарегистрированным ресурсам. Таким образом, даже внесенные в «белые списки» «Госуслуги» могут работать нестабильно, что парализует запись к врачу и получение других важных государственных услуг, а также привычных сервисов для граждан, таких как вызов такси, вход в мобильный банк, в мессенджеры и других.

МАХ [5], как и любое другое приложение, зависит от наличия базового интернет-соединения (через мобильную сеть или Wi-Fi). Однако ключевым его отличием и преимуществом в современных российских реалиях является способность работать при крайне нестабильном и слабом сигнале. Это достигается за счёт специальных алгоритмов, которые оптимизируют

передачу данных, сжимают трафик и могут использовать промежуточные узлы для повышения надёжности доставки сообщений. Таким образом, в условиях, когда обычные приложения и мессенджеры уже не функционируют, МАХ может сохранять частичную работоспособность, позволяя пользователям обмениваться текстовыми сообщениями.

Тем не менее, это преимущество действует только до тех пор, пока существует минимальный физический канал связи. Если же каналы связи полностью подавлены системой РЭБ (радиоэлектронной борьбы) или отключены оператором по требованию силовых структур, мессенджер, как и любое другое приложение, не сможет установить соединение. Глушение и отключения воздействуют на физический уровень связи — радиосигнал на определенных частотах.

Сегодняшние реалии привели к созданию в России сложной системы контроля над радиоканалом, включающей как точечное глушение, так и массовые отключения мобильного интернета. Эти меры, хотя и оправдываются соображениями безопасности, имеют серьезные социальные и экономические последствия, нарушая работу систем жизнеобеспечения, коммерции и здравоохранения. Национальный мессенджер МАХ может помочь пользователям обеспечить более стабильный сигнал при глушении и ограничении связи и мобильного интернета. Проводная телефония остаётся ограниченной альтернативой, а спутниковые технологии и Mesh-сети пока не стали массовым решением. Государство оказывается перед сложным выбором между безопасностью и цифровым суверенитетом, с одной стороны, и потребностями общества и экономики в стабильной связи — с другой.

Список использованных источников:

1. Путин объяснил ограничения мобильной связи угрозой атак беспилотников [Электронный ресурс] // Ведомости. 2025. 19 дек. URL:

<https://www.vedomosti.ru/politics/news/2025/12/19/1164781-putin-obyasnil> (дата обращения: 20.12.2025).

2. Ли И. Глушилки, геозоны, перезваниватели: как в России точно блокируют мобильный интернет [Электронный ресурс] // Новые Известия. 2025. 14 нояб. URL: https://newizv.ru/news/2025-11-14/glushilkiUQAqJ3KzD116VDGbaijIcsSeOss0FSBZggu_gmpy2kcvzuIEblokiryut-mobilnyu-internet-438238?utm_source=m.ok.ru&utm_medium=referral&utm_campaign=m.ok.ru&utm_referrer=m.ok.ru (дата обращения: 30.11.2025)

3. Операторы связи усилили меры безопасности для борьбы с БПЛА [Электронный ресурс] // Объясняем.рф: офиц. информ. портал. 2025. 10 нояб. URL: https://объясняем.рф/articles/news/UQAqJ3KzD116VDGbaijIcsSeOss0FSBZggu_gmpy2kcvzuIEborby-s-bpla/ (дата обращения: 20.12.2025).

4. Корелина А. Россияне побежали устанавливать дорогой спутниковый интернет из-за отключений мобильного. Как он работает и стоит ли того [Электронный ресурс] // Secretmag. 2025. 1 авг. URL: https://secretmag.ru/technologies/rossiyane-pobezhaliUQAqJ3KzD116VDGbaijIcsSeOss0FSBZggu_gmpy2kcvzuIEUQAqJ3KzD116VDGbaijIcsSeOss0FSBZggu_gmpy2kcvzuIEli-togo.htm (дата обращения: 30.11.2025).

5. Дубровская А. Пользователи Мах массово пожаловались на проблемы с доступом [Электронный ресурс] // Газета.Ru. 2025. 8 дек. URL: https://www.gazeta.ru/tech/news/2025/12/08/27358243.shtml?utm_source=ixbtcom&utm_auth=false (дата обращения: 20.12.2025).