

УДК: 004.35

ПРОСЛУШКА ТЕЛЕФОНА, ОПРЕДЕЛЕНИЕ ГЕОЛОКАЦИИ

Калпакова А.В, студент гр 21401, 4 курс Ковшенин П.С,
студент гр.21477, 4 курс

Научный руководитель: Субаева А.К., д. э. н/, доцент
Чистопольский филиал «Восток» Казанского национального исследовательского технического университета им. А.Н. Туполева-КАИ,
г. Чистополь

Вопросы, связанные с возможностью прослушивания при телефонных разговорах и отслеживания местоположения, вызывают серьезные опасения относительно сохранности личной информации и приватности.

К 2026 году смартфон превратился из простого средства связи в мощный инструмент слежения. Он обладает информацией, превосходящей знания самых близких людей: где находится человек, с кем общается, о чем говорит и даже как взаимодействует с экраном. Сегодня актуально не то, что могут ли за кем-то следить, а скорее, кто именно это делает и насколько законны его действия.

Технологии, позволяющие прослушивать и определять местоположение, развивались на протяжении десятилетий. То, что ранее было доступно лишь спецслужбам с громоздким оборудованием, теперь может быть использовано любым желающим, просто скачав соответствующее приложение из магазина. Более того, исследования показывают, что даже без установки шпионского ПО телефон может передавать информацию о местоположении без ведома[1].

Современные смартфоны оснащены двумя основными процессорами: процессор приложений (AP), отвечающий за работу пользовательских программ, и базовый процессор (BP), управляющий функциями сотовой связи. Эти процессоры функционируют независимо друг от друга. Именно базовый процессор обрабатывает сигналы от базовых станций мобильной связи, поступающие по служебным каналам, а не через интернет-соединение[1].

Разберём три ключевых аспекта проблемы: технический (как это работает), юридический (что разрешено законом) и бытовой (как обывателю распознать слежку и защититься).

Многие думают, что их местоположение в безопасности, если они выключили GPS и запретили приложениям использовать геолокацию на своих телефонах. Но это большое заблуждение.

Внутри современных смартфонов есть два "мозга": один для обычных программ (приложений) и другой, который управляет связью с мобильными вышками (базовый процессор). Они работают отдельно. Именно

этот второй "мозг" получает специальные сигналы от вышки, а не через интернет.

Ученые выяснили, что специальные программы (протоколы RRLP и LPP), которые создавались для экстренных служб (чтобы находить людей, звонящих в 112, даже без SIM-карты), имеют серьезные недостатки. Это значит, что спецслужбы или злоумышленники могут незаметно отправлять на телефон команды. Телефон, получив такую команду, ненадолго включает GPS, определяет точное местоположение (до сантиметра) и отправляет его обратно. При этом обычная программа на телефоне и человек об этом не узнают – значок GPS на экране не появится[1].

Геолокацию можно определить, не прибегая к GPS или Wi-Fi. Исследователи из Северо-Восточного университета (Northeastern University) продемонстрировали, что приложения для Android, даже не запрашивающие никаких специальных разрешений, способны использовать данные с акселерометра и гироскопа для определения как текущего, так и прошлого местоположения телефона.

Этот метод основан на анализе вибраций и изменений положения устройства. Движения автомобиля, поезда или даже обычная ходьба человека генерируют уникальные "вибрационные отпечатки", которые можно сопоставить с картографическими данными. Более того, анализ нажатий на сенсорный экран позволяет злоумышленникам восстанавливать введенные пароли и PIN-коды, изучая, как именно меняется положение смартфона при касании различных участков экрана.

Чтобы понять, прослушивается ли телефон или за человеком следят, нужно обратить внимание на следующие тревожные сигналы:

- странности в работе устройства (экран включается сам, приложения запускаются без участия человека, а индикаторы микрофона или камеры горят, когда их не используют);

- проблемы с производительностью (телефон сильно греется даже в режиме ожидания и быстро разряжается, что может указывать на фоновую активность шпионского ПО[2]);

- необъяснимый расход трафика (заметьте резкое увеличение фонового интернет-трафика в статистике или ночные сеансы передачи данных).

Для быстрой проверки переадресации звонков и сообщений нужно набрать *#21#. Если она включена, данные могут перехватываться. Отключить все виды переадресации можно командой ##002#[3].

Если подозрения подтвердились, самый надежный способ – это полный сброс телефона до заводских настроек. Рассмотрим в таблице 1 технологии слежки:

Таблица 1 – Технологии слежки

Метод слежки	Принцип действия	Точность	Сложность обнаружения
Уязвимости LPP/RRLP	Скрытый запрос к модему через сотовую вышку	До 1 метра	Очень высокая (пользователь не видит индикации)
IMSI-ловушка (Paging)	Перехват сигналов поискового вызова в GSM	До 1 км ²	Высокая (требует спецоборудования)
Атака через сенсоры	Анализ данных акселерометра/гироскопа	Средняя	Средняя (приложения не требуют GPS-прав)
Ультразвуковой трекинг	Активация микрофона звуком 20 кГц	Высокая	Очень высокая (человек не слышит звук)
Приложения слежки	Доступ к микрофону и данным геолокации	Абсолютная	Низкая (видно в списке приложений и разрешений)

Проблемы конфиденциальности в мобильных сетях достигли критического уровня, став одной из главных забот современного общества. Новые технологии, такие как 5G, интернет вещей (IoT) и продвинутая геолокация, дают правоохранительным органам и спецслужбам мощные средства для борьбы с преступностью и угрозами. Однако эти же технологии открывают возможности для массовой слежки, позволяя собирать и анализировать огромные объемы личных данных, включая перемещения, привычки, связи и биометрические показатели. Существующее законодательство, разработанное до повсеместного распространения цифровых технологий, не успевает за этими изменениями и не может эффективно регулировать новую реальность.

В современном цифровом мире идут жаркие споры о балансе между безопасностью и свободой. Вопросы о предустановленном ПО, раскрытии личности пользователей мессенджеров и сборе их данных вызывают острые разногласия между теми, кто ставит во главу угла безопасность, и теми, кто отстаивает гражданские права. Найти золотую середину между защитой личной и государственной безопасности и правом на конфиденциальность – главная задача нашей эпохи. Для этого нужны не только новые законы, встроенная в системы приватность и повышение

цифровой грамотности, но и постоянное обсуждение допустимых пределов контроля. В такой ситуации пользователи мобильных устройств должны быть особенно осторожны: внимательно проверять, какие разрешения запрашивают приложения, использовать шифрование, менеджеры паролей, VPN и другие инструменты для защиты своей информации. Важно понимать, что полная анонимность в нашем мире практически невозможна, а цифровая гигиена становится не просто технической мерой, а необходимым условием сохранения личной свободы в условиях повсеместной цифровизации [4].

Список литературы :

1. В смартфонах найдена древняя технология слежки. Ей десятки лет, она работает сверхточно, и отключить ее нельзя [Электронный ресурс] URL: https://safe.cnews.ru/news/top/2026-02-04_v_smartfonah_najdena_drevnyaya (дата обращения: 09.02.2026)
2. Телефон на «прослушке»: как понять, что за вами шпионят [Электронный ресурс] URL: <https://news.rambler.ru/tech/55461909-telefon-na-proslushke-kak-ponyat-cto-za-vami-shpionyat/> (дата обращения: 17.02.2026)
3. Вы не один на линии: озвучены главные признаки «прослушки» телефона [Электронный ресурс] URL: <https://deita.ru/article/570098> (дата обращения: 17.02.2026)
4. Эксперт Бедеров: прослушка в смартфоне может быть активирована через ультразвук [Электронный ресурс] URL: <https://technosovet.ru/novosti/bezopasnost/ekspert-bederov-proslushka-v-smartfone-mozhet-byt-aktivirovana-cherez-ultrazvuk/> (дата обращения: 17.02.2026)