**Защищенная телефония.**

 ***Специальный абонентский терминал (САТ), предназначенный для защиты переговоров от прослушивания оператором сотовой сети связи или недоброжелателями с использованием комплексов перехвата GSM.***

С появлением комплексов перехвата разговоров в системе GSM никто не может быть застрахован от прослушивания разговора третьими лицами.

∙          *Обнаружить такое вмешательство на стандартном или специальном телефоне без специальных мер защиты невозможно*

∙          *Решить проблему предупреждения и защиты от прослушивания можно с использованием разработанного нашей компанией специального абонентского терминала (САТ)*

**Основные источники угроз**

Существует множество способов, которыми злоумышленники могут получить информацию с вашего мобильного телефона:

* + Интернет;
	+ Ложные базовые станции
	+ SMS, ММS и электронная почта;
	+ приложения, устанавливаемые на мобильные телефоны из непроверенных источников;
	+ подключение к заражённому стационарному компьютеру;
	+ отключение пользователем встроенных механизмов безопасности телефона.

Во многих современных мобильных телефонах есть модули NFC (Near Field Communication — беспроводная высокочастотная связь малого радиуса действия). Для передачи данных с помощью NFC достаточно поднести два устройства на расстояние нескольких сантиметров друг к другу и отправить файл или ссылку. Соединение и авторизация проходят автоматически. Таким образом, для установки вредоносных программ на телефон с модулем связи NFC, достаточно послать на него с находящегося поблизости телефона файл с вирусом или ссылку, которая будет открыта автоматически.

**Программы-шпионы**

Программы-шпионы — программное обеспечение, собирающее и передающее кому-либо информацию о пользователе мобильного устройства без его согласия. Владелец телефона даже не подозревает о том, что на него установлена программа-шпион, поскольку программа работает в фоновом режиме и обнаружить ее в файловой системе или списке программ невозможно. Поскольку программа устанавливается во внутреннюю память телефона, она будет работать даже при смене SIM-карты. Для установки такой программы злоумышленнику достаточно иметь доступ к вашему телефону в течение 5 минут.

Шпионские программы для мобильного телефона способны следить и частично контролировать активность на мобильном устройстве, на которое они установлены. В результате злоумышленникам в любое время суток даже в противоположной точке земного шара будет доступна следующая информация:

* + SMS, MMS, электронная почта;
	+ любые данные, полученные или переданные через Интернет;
	+ координаты мобильного телефона с точностью до нескольких метров.
	+ входящие и исходящие вызовы вместе с продолжительностью звонка;
	+ прослушивание и запись всех разговоров с мобильного телефона;
	+ включение микрофона и прослушивание всех разговоров, ведущихся поблизости от телефона, даже когда он находится в режиме ожидания.

 **Дистанционное включение камеры и микрофона телефона**

С помощью программ, позволяющих дистанционно управлять мобильным телефоном, можно без ведома владельца включать видеокамеру или микрофон телефона. Включение микрофона возможно даже когда телефон находится в режиме ожидания. В результате становится возможным:

* + фотографирование окружающих лиц и предметов;
	+ видеосъемка;
	+ прослушивание разговоров в радиусе до 10 м от мобильного телефона;

**Ложные базовые станции**

Специальное устройство, называющееся ловушка IMSI (уникального идентификатора, прописанного в SIM-карте, IMSI — International Mobile Subscriber Identity), притворяется для находящихся поблизости мобильных телефонов настоящей базовой станцией сотовой телефонной сети. Такого рода трюк возможен потому, что в стандарте GSM мобильный телефон обязан аутентифицировать себя по запросу сети, а вот сама сеть (базовая станция) свою аутентичность подтверждать телефону не должна.

Как только мобильный телефон принимает ловушку IMSI в качестве своей базовой станции, этот аппарат-ретранслятор может деактивировать включённую абонентом функцию шифрования и работать с обычным открытым сигналом, передавая его дальше настоящей базовой станции.

С помощью ловушек IMSI на телефон могут посылаться ложные звонки или SMS, например, с информацией о новой услуге ложного оператора, в которых может содержаться код активации микрофона мобильного устройства. Определить, что у находящегося в режиме ожидания мобильного телефона включён микрофон очень сложно, и злоумышленник спокойно может слышать и записывать не только разговоры по телефону, но и разговоры в помещении, где находится мобильный телефон.

 **Фальсификация идентификации личности**

В последние годы все более популярным становится использование мобильного телефона как доказательства идентификации личности. Например, способом восстановления потерянного пароля учётной записи в Google является отправление SMS с подтверждением кода владельцу телефона. Некоторые банки используют похожую двухступенчатую аутентификацию, посылая коды на специальные мобильные номера для того, чтобы подтвердить личность клиента перед проведением транзакции. Были обнаружены мобильные версии троянов, которые могут перехватывать SMS сообщения с паролями, посланные банками, и разрушать двухступенчатую аутентификацию.

     *Комплексное устройство уникально сочетает базовую систему аппарата и инструменты для защиты от различных видов несанкционированного вмешательства.*

*Комплекс предлагает непревзойденную безопасность и конфиденциальность для всех, кто не желает уступать право собственности на личную жизнь.*

**Функции специального абонентского терминала:**

∙           Смена IMEI (идентификационного международного номера телефона)

∙           Защита от активных и пассивных комплексов

(перехват переговоров и дистанционное управление телефоном и другие атаки на аппарат со стороны оператора или мобильного комплекса GSM)

 ∙           Удаления информации о звонках из памяти телефона (удаленная информация хранится в специальных отсеках памяти и доступна специалистам)

 ∙           Невозможность локализации телефона и его владельца (а также определения номера основного телефона и связанных  с ним номеров других телефонов)