ПАМЯТКА

по угрозам информационной безопасности
при использовании мобильного телефона

Определение текущего местоположения – прямая угроза жизни военнослужащих!

Все телефоны (смартфоны и «кнопочные» телефоны в том числе) предоставляют возможность удаленного определения местонахождения абонента способом пеленгования (в том числе по базовым станциям) и/или перехвата данных с абонентского терминала, где содержится информация о местоположении в виде геокоординат (встроенная функция геолокации аппаратно не отключаема), что в условиях ведения боевых действий способствует наведению высокоточного оружия.

Выключенный телефон все равно остается на связи в сети оператора!

Прослушивание разговоров – прямая угроза жизни военнослужащих!

При выполнении специальных задач за пределами Российской Федерации мобильные телефоны используют базовые станции иностранных государств для передачи сигнала, что позволяет иностранным спецслужбам производить прослушивание телефонных разговоров военнослужащих. Полученная информация используется для выявления планов действий/маневров войск с целью нанесения огневых ударов.

Дешифрование информации, передаваемой с использованием мессенджеров – прямая угроза жизни военнослужащих!

Спецслужбы располагают ключами шифрования от мессенджеров (приложения, поддерживающие возможность обмена сообщениями), что позволяет:

получать информацию о планах действий/маневров войск с целью нанесения огневых ударов;

добывать личные данные и компрометирующие сведения о владельце телефона;

получение доступа к служебной информации;

запись голосов речи и их обработка с целью последующей имитации.

Дезинформация противником военнослужащих ВС РФ передачи ложной информации от имени владельца телефона с целью получения конфиденциальных данных, дезорганизации управления, обеспечения и взаимодействия.

Идентификация личности военнослужащего и его круга общения

Пользовательский номер абонента является уникальным идентификатором, по которому можно определить круг общения в различных мессенджерах, социальных сетях и т.д. Результатом является морально-психологическое воздействие на близких родственников владельца номера с целью шантажа и давления.

Внедрение программных агентов в абонентский терминал

Мобильные устройства на базе операционных систем Android, iOS предоставляют иностранным разведкам (противнику) возможность полностью контролировать внутренние цифровые модули, начиная с получения данных на встроенных носителях и заканчивая получением доступа к микрофону и встроенным камерам. Появляется возможность контроля абонентского терминала по расписанию или при необходимости.

ПАМЯТКА

по использованию терминала сотовой связи
(мобильного телефона)

Абонентский терминал сотовой связи –
техническое средство разведки иностранных государств

Любой без исключения телефон – источник информации о местоположении абонента, даже в выключенном состоянии!
В БОЕВЫХ УСЛОВИЯХ – ПРЯМАЯ УГРОЗА ЖИЗНИ!

Взял мобильный телефон с собой при выполнении специальных задач – поставил под огневой удар всё подразделение!

Позвонил командиру/сослуживцу/подчиненному – сорвал выполнение боевой задачи и предоставил противнику информацию для нанесения огневого удара!

Отправил информацию с использованием «защищенного» мессенджера – обеспечил противника разведданными!

Пользуешься мобильным телефоном как накопителем личной информации – предоставляешь самую полную информацию о себе и круге общения!

Позвонил родным с мобильного телефона с территории иностранного государства – раскрыл сведения о себе и своих близких!

Используешь мобильный телефон при выполнении специальных задач – предоставляешь иностранным разведкам всю информацию о своих действиях!

Мобильный телефон – источник получения самой полной информации, способной в руках иностранных спецслужб нанести ущерб не только владельцу, но и его подразделению, близким родственникам, а также дискредитировать деятельность Вооруженных Сил Российской Федерации.