# Пояснительная записка.

При проведении специальной военной операции (СВО) в Украине наши бойцы сталкиваются с новыми демаскирующими факторами и противодействием иностранных технических разведок (сокращённо - ИТР). Современные ИТР с широким спектром возможностей в настоящее время теоретически имеют только 3 стороны: ОДКБ с центром в лице России, Китай и НАТО с центром в лице США. Но никогда ранее эти стороны открыто не передавали разведданные, добытые с помощью ИТР, третьим странам, не входящими в ОДКБ и/или НАТО. Допускался только обмен этими данными между собой при пересечении взаимных интересов и/или выполнении обязательств по международным договорам (Договор по открытому небу, Договор об обычных вооружённых силах в Европе, и др.).

С началом проведения СВО группа стран во главе с США начали демонстративно передавать Украине данные технической разведки НАТО, в том числе по геолокации (месторасположению) скоплениям наших войск, полученных с активных сотовых телефонов наших бойцов (при наличии «немодулированного» процессора в телефоне определяются даже выключенные аппараты). Есть множество методов накопления этих данных (спутниковые системы для определения местонахождения, поиск по беспроводным сетям: Cell of Origin, Time of Arrival, Observed Time Difference, Assisted Global Positioning System и многие другие). Массивы этих данных анализируются в суперкомпьютерах США (один такой суперкомпьютер может достигать вычислительной мощности в сотни петафлопс: 1 петафлопс = 1 тыс. трлн вычислений в секунду), по количеству и мощности суперкомпьютеров США на втором месте после Китая, а если суммарно по военным блокам, то НАТО на первом месте (Россия в этой таблице стран мира на седьмом месте, по ОДКБ данные закрыты, Украина в таблице отсутствует).

В результате полученного анализа массива данных США имеет стратегические и тактические карты местонахождения наших бойцов в режиме реального времени (on-line), которые может передавать в центры принятия решений Украины, в том числе для последующего нанесения ударов по скоплениям наших бойцов и/или маневрирования от окружения и ухода от контрударов. Также эти передаваемые данные могут загружаться в передаваемые Украине американские реактивные системы залпового огня (РСЗО) для дальнейших ударов по нашим позициям (все аппаратные и программные части техники по заявлениям НАТО унифицированы) или по старинке использоваться для нанесения ударов по выявленным координатам (ракетные и/или артиллерийские).

Склады боеприпасов (по «следам» логистики), штабы войск РФ на территории Донбасса, приезд командного состава войск РФ на позиции СВО, мобилизованные отслеживаются особо тщательно, что уже приводило к их обстрелу.

Проведенный нами анализ выявил, что способ противодействия может применяется только в форме технической блокировки сигналов сотовых телефонов и/или использовании закрытых систем связи. Это также актуально для войск РФ на всей территории России в повседневной деятельности (построения подразделений, войсковые учения, передвижения по войсковым частям, кораблям или по служебным маршрутам, особенно в составе подразделений и т.д.).

К сожалению, не все бойцы соблюдают «режим тишины», часто имеет место желание быть на связи с близкими («человеческий фактор»), много случаев включения телефонов для использования подсветки в темное время суток (при отсутствии фонарика) и т.д., что может приводить к раскрытию местоположения бойцов или всего подразделения. Поэтому мы учли все демаскирующие факторы.

Данные изделия скрывают местонахождения и передвижения личных мобильных устройств военнослужащих и гражданских работников во время службы (работы), предотвращая удары беспилотных летательных аппаратов (БПЛА) и ракетных обстрелов врага по месторасположению их скоплений, определяемые иностранной технической разведкой (ИТР), тем самым сохраняя жизни работников и обеспечивая безопасность военных объектов и объектов критической инфраструктуры.