# Памятка участнику СВО по противодействию техническим средствам разведки

ПРОЕКТ «АРХАНГЕЛ СПЕЦНАЗА»

В военное время важнейшую роль всегда играла разведка. Чем вооружен противник? Какова его численность? Что он намерен делать? В условиях современной войны одним из решающим фактором успеха является  успешное проведение мероприятий технической разведки. В силу высокого уровня технологического развития стран Запада в сфере информационных систем (вспомним Apple, Microsoft, Intel), противник оснащен самыми передовыми средствами технической разведки.

Данный материал содержит краткую выжимку сведений, необходимых для выживания и успешного выполнения боевых задач в условиях применения противником передовых средств технической разведки.

## В чем угроза?

Противник получает сведения о военнослужащих ВС РФ проводя комплекс мероприятий в рамках сразу нескольких разведывательных дисциплин:

GEOINT – метод сбора разведданных о человеческой деятельности на Земле, получаемых в результате анализа изображений и геопространственной информации, позволяющей осуществить географическую привязку человеческой деятельности на Земле

SIGINT - метод сбора разведданных путем перехвата сигналов различных видов, определения их источников и расшифровки передаваемой информации

HUMINT - метод сбора разведданных, получаемых посредством межличностного контакта с объектами интереса

MASINT - метод сбора разведданных на основе проведения измерений и анализа сигнатур. Данная дисциплина служит для обнаружения, отслеживания, идентификации или описания отличительных характеристик (сигнатур) статических или динамических источников целей. К ним часто относятся радиолокационная разведка, акустическая разведка, ядерная разведка, химическая и биологическая разведка.

Все описанные методы используются как совместно в рамках комплекса мер, применяя все доступные средства для получения разведданных о военнослужащих ВС РФ и других важных целях на территории СВО и не только. Противник не остановится ни перед какими моральными принципами, не будет себя ограничивать в применяемых средствах для добычи необходимой информации.

# Задача анализа разведданных

Обрывчатые сведения о войсках в руках опытных аналитиков позволяют после проведения анализа построить детальную картину текущей обстановки. Задача анализа разведданных: сбор фактов, толкование фактов, построение гипотезы и формирование вывода.

**Пример:** противник определил дату развертывания подразделения, его специализацию и вид транспорта на основе перехвата звонков, фотографий из соцсетей, свидетельств очевидцев. В ходе *сбора фактов* применяются описанные ранее дисциплины разведки. Исходя из анализа этих сведений противник может приблизительно определить типы применяемого подразделением вооружения, определить его задачу, возможности, место применения. К примеру зная тактико-технические характеристики техники определить предельно возможную численность войск, которые могут перевозится известным количеством техники. Данный этап называется *построением гипотезы.* Зачем противник выполняет переброску к линии фронта машин-понтоноукладчиков? Справедливо предположить что планируется форсирование крупной водной преграды. В качестве итога *формируется вывод* о планируемых действиях подразделения.

Успешным ли будет выполнение задачи, о которой противник знает все заранее? Однозначно нет. Противник сможет оказать желаемое влияние на ход проведения операций еще до её начала, усилить участок фронта или имитировать отступление, нанести превентивный удар, сорвать операцию диверсией или начать внезапное наступление на другом участке фронта.

К сожалению, такая информация часто доступна в социальных сетях, таких как VK, TikTok, Facebook. Раньше уходили недели прежде чем информация «утечет» в печатные СМИ, сейчас же видео проходящей колонны танков по мосту моментально разлетается по Интернету, попадает в руки разведслужбам противника и анализируется.

В современных реалиях разведслужбы обладают намного большими возможностями чем когда-либо в военной истории!

# Как не подставить себя и своих боевых товарищей?

Комплекс методов противодействия разведке называется OPSEC (Operation Security, англ. оперативная безопасность или безопасность операций). Данный метод применяется в армии США со времен войны во Вьетнаме. Он определяет меры по защите информации, критически важной для текущих операций дружественных сил, недопущения непреднамеренного предоставления такой информации противнику. Методы защиты строятся на определении и типизации угроз.

Основные угрозы можно поделить на категории, соответствующие дисциплине разведки:

- Несанкционированная фото/видеосъемка, публикация любых материалов о своей специализации, личности, задачах
- Использование в зоне СВО любых носимых устройств, электроприборов, девайсов, имеющих доступ в Интернет
- Передача информации по недоверенным и незащищенным каналам

- Передача чувствительной информации индивидуумам, не уполномоченным на работу с ней

Следует **запомнить ряд тезисов**, которые помогут обеспечить безопасность операций. От их соблюдения зависит **физическая безопасность и жизнь Вас и Ваших боевых товарищей**:

- **Любой фотоснимок или видеозапись в зоне СВО может содержать информацию, которая может быть проанализирована противником в целях сбора разведывательной информации!**
- Любое подключаемое к Интернету устройство может быть запеленговано или взломано, современный смартфон в авиарежиме и выключенном состоянии тоже. **Пока из смартфона не извлечена батарея и SIM карта он может осуществлять передачу данных в сотовой сети!**
- Если вы находитесь в тылу и вам нужен телефон для выполнения задач, **убедитесь что он**:
    - Ранее **не использовался в личных целях** (был куплен перед отправкой, распакован и подготовлен к работе на месте), **тем более с него не совершались звонки на территории РФ**
    - Не содержит **НИКАКОЙ личной информации** (Ваше имя, фамилия, дата рождения, номер машины, и т.п.)
    - В него ранее **не устанавливались SIM карты Российских операторов** (уникальный идентификатор устройства IMEI может быть связан с номером, итог: абонент идентифицирован).
    - Исходите из того что т**елефон в любой момент может быть потерян и его тут же обнаружит противник**
- **Любой неподконтрольный канал связи** по умолчанию **считается недоверенным**. Это в частности касается:
    - Мессенджеров, таких как WhatsApp, Viber, Вконтакте, Signal, Wiebo, Confide, Cloackman. На WikiLeaks опубликована документация о **Vault7, наборе инструментов, созданного АНБ США для взлома шифрования** указанных мессенджеров.
    - Каналов сотовой связи на территории противника
    - Любых сервисов электронной почты
    - Незащищенных каналов радиосвязи

Среди сторонних угроз стоит упомянуть риск того, что противник завладеет Вашим мобильным телефоном при Вашем попадании в плен или гибели. В первую очередь военнослужащие противника проверят фотогалерею с целью определить Вашу причастность к тем или иным операциям или событиям в зоне СВО. Затем они начнут звонить Вашим родственникам, издеваться над ними и шантажировать. Еще худший сценарий – если в телефоне записаны телефоны сослуживцев, их могут заманить в засаду. Хранить номера следует в зашифрованном виде, очищать журнал вызовов после звонка. Например: прибавить произвольное число к каждому второй цифре номера. Вы можете проявить изобретательность и придумать свой способ шифрования, или запомнить номера наизусть.

На Ozon/Yandex.Market можно купить экранирующий излучения чехол для смартфона, обладающий физическими свойствами Клетки Фарадея: можно найти по запросу «чехол для смартфона клетка фарадея». **Это средство защиты испытано в ходе боевых действий!**

# Примеры реализации угроз

Ниже приведены примеры существующих угроз и их реализации в соответствии с применяемой дисциплиной разведки. Все приведенные примеры основаны на реальных сценариях:

1. **С помощью OSINT и GEOINT противник может получать данные из открытых источников, анализировать их и получать таким образом местонахождение интересующего субъекта.**

Дано: Солдат ВС РФ публикует фотографию редкой модификации боевой машины. Номерные знаки на технике, опознавательные знаки на форме бойцов замазаны. В момент съемки боец с помощью приложения для редактирования изображений замазывает опознавательные знаки и выкладывает фотографию в социальную сеть.

Найти: местность на снимке, точное местонахождение боевой машины.

Решение: Противник регулярно мониторит с помощью автоматизированных средств публикации в интересующих его каналах, на страницах интересующих людей – процесс поиска информации о противнике в открытых источниках (социальных сетях) включен в разведывательную дисциплину OSINT, разведку по открытым источникам. Полученная фотография из соцсетей передается аналитикам GEOINT. По различным косвенным признакам они определяют местность на фото. Угол падения теней, время публикации, специфические архитектурные сооружения, уникальные для того или иного города позволяют точно определить место съемки с точностью до улицы. После выполнения геопривязки по месту съемки наносится ракетный удар.

2. **С помощью SIGINT противник может перехватывать любые сигналы, определять их источники, получать доступ к передаваемой информации**

Дано: Солдат ВС РФ раздобыл в зоне СВО сотовый телефон и приобрел местную SIM карту. Боец был осведомлен о рисках публикации фотографий, поэтому использовал телефон лишь для связи с близкими родственниками.

Найти: местонахождение абонента с предположением его пребывания в месте скопления войск РФ с целью нанести точечный удар.

Решение: Вследствие проведения комплекса технических мер оперативно-разыскных мероприятий в сетях сотовой связи выявляются абоненты, осуществляющими вызовы на телефоны в нумерации РФ (+7). Спецслужбы имеют полный контроль над сотовыми линиями связи на территории своей страны. Осуществляется перехват звонка, исходя из контекста диалога определяется принадлежность абонента к ВС РФ. После этого осуществляется триангуляция сотового телефона (дисциплина SIGINT). Определение местоположения источника радиоизлучения (сотовый телефон) методом радиотриангуляции является лишь одним из нескольких методов пеленгации (определения местонахождения источника радиосигнала). По точке наносится удар.

# Практические рекомендации

1) **Не берите на задачи мобильные телефоны, любую носимую электронику (часы Amazfit, Apple, Garmin, Mifit)**. Если дома Вас никто не ждет – хотя-бы ставьте телефон в авиарежим для минимизации обнаружения детекторами сотовых излучений.
2) Не сообщайте по телефону, в мессенджерах свои геоданные, координаты. **Не давайте описаний местности**.
3) **Не контактируйте с мирными** жителями на неподконтрольных территориях.
4) Если снимаете материал, делайте это на action-камеры без функции выхода в Интернет!
5) **Не выкладывайте фото или видеоматериалы в Интернет**, выждите минимум 3-4 дня между съемкой и публикацией, выполните перед публикацией смену дислокации. **Публикуемая информация не должна быть актуальной для противника**!

**Пренебрежительное отношение к описанным в данном материале рекомендациям может привести к серьезным проблемам со здоровьем, инвалидности и смерти.**

Устройство **можно считать доверенным только после детального исследования** его внутреннего устройства специалистами. Это подразумевает в первую очередь анализ прошивки, поиск бекдоров в исходном коде и незадекларированных изготовителем возможностей. **Устройства вроде умных часов не сертифицированы** Федеральной службой по техническому и экспортному контролю как военное снаряжение, т.к соответствующие исследования на государственном уровне не проводились! **Эти устройства могут быть осуществлять негласное отслеживание вашей геолокации или совершать отправку текста PUSH-уведомлений с привязанного к часам смартфона на сторонние сервера!**