

ОСНОВЫ ФОРМИРОВАНИЯ, ПОДГОТОВКИ И ПРИМЕНЕНИЯ ШТУРМОВЫХ ПОДРАЗДЕЛЕНИЙ
Часть I

Предлагаемый материал является дополнением боевых уставов в части подготовки и применения штурмовых подразделений и призван восполнить пробелы и упростить понимание вопросов тактики применения штурмовых подразделений в современных боевых действиях.

Цикл предназначен для внимательного прочтения и изучения всеми командирами, подготовки и применения штурмовых подразделений, без ограничений по уровням: от командиров мотострелковых отделений до командующих армиями. Цикл имеет целью помочь понять необходимость формирования штурмовых подразделений и особенности их подготовки, восполнить пробелы и упростить понимание вопросов тактики применения штурмовых подразделений в современных боевых действиях. Детально рассматриваются этапы подготовки и проведения штурмовых действий с применением средств огневого поражения, охранения, контрбатарейной борьбы, разведки и радиоэлектронной борьбы, беспилотных систем и средств противодействия им, средств связи и автоматизированного управления, маскировки (в том числе путем имитации радиоэлектронной обстановки), медицинского, инженерного, геопространственного

обеспечения и психологической борьбы. Предлагаемый материал не является подменой или противопоставлением боевым уставам, а дополняет их.

1.1. Новая реальность штурмовых действий

Война - это «ментальность плюс технологии»!

Не отмахивайтесь от этого постулата, думая, что Вас это не касается, что война - это стратегия! Стратегия присутствует и обязана быть у всех - от солдата до главкома!

Стратегия начинается там, где начинается «тактика вышестоящего начальника». То есть для командира штурмовой группы стратегия - это цели штурмового отряда и варианты возможных действий в решении его командира. Для бойца на поле боя стратегия - это задача его штурмовой группы. Технологии - это не только «железо и программы». Технологии войны включают: вооружение, военную технику и различные технические средства, все (в том числе гражданские), влияющие на противника на поле боя, а также технологии принятия решений, ведения разведки, анализа, распределения, блокирования и искажения информации, технологии реализации способов ведения боевых действий и тактических приемов, технологии обучения и др.

ВАЖНО! Пощады от врага, если победит, не будет! Война от конфликта отличается главным образом тем, что войны ведутся не за ресурсы и территории, а за БУДУЩЕЕ, возможность строить жизнь по собственному пониманию миропорядка. Они ведутся до победы одной из сторон. Конфликты же заканчиваются договоренностями и имеют более приземленные цели – ресурсы, территории и др.

Типовыми функциями образцов вооружения и военной техники в современных боевых действиях являются:

1) огневое поражение, в том числе самонаводящимся на излучение оружием;
2) разведка (в доступных физических полях);
3) связь (цифровая, аналоговая, по проводам и без них);
4) автоматизированное управление;
5) радиоэлектронное подавление;
6) компьютерные атаки;
7) тактическая маскировка (маскировка и имитация боевой (в том числе радиоэлектронной) обстановки);
8) поражение мощным (когерентным и некогерентным) электромагнитным излучением;
9) психологическое воздействие;
10) нелетальное воздействие;
11) радиационное, химическое и биологическое воздействие.

Необходимо отметить высокую скорость изменения способов ведения боевых действий и тактических приемов под влиянием современных технологий (как военных, так и гражданских), и в первую очередь – «мобильного интернета» и современных цифровых средств связи. Это позволило сформировать **киберпространство поля боя**, а также нарастить применение всевозможных беспилотных систем (далее – Б п С): наземных (далее – Б Н С), авиационных(далее – БАС). Ведь сейчас мы наблюдаем переход войны людей в **войну роботов**.

На поле боя используется следующие основные стандарты связи:

- спутниковая связь с прямым доступом к сети Интернет преимущественно через космическую систему Starlink, а также систему Kuiper от Amazon и, в отдельных случаях, систему OneWeb. Терминалы свази этих систем пока еще достаточно громоздкие и могут размещаться только на крупногабаритных беспилотных авиационных системах. Однако в ближайшее время планируется ввести в эксплуатацию сеть спутниковой связи типа Direct-to-Cell (D2C). Ее терминалами будут обычные смартфоны. На орбите уже находятся более тысячи спутников, готовых к этой задаче. Оперативность ввода в эксплуатацию системы Starlink не дает оснований сомневаться, что эти планы могут быть реализованы в течение ближайшего времени. И тогда каждый беспилотник сможет быть оснащен системой управления и передачи данных с использованием терминалов типа D2C, что существенно затруднит его блокирование средствами радиоэлектронной борьбы;



Общая схема классификации автоматизированных систем управления НАТО

- сотовая связь поколений 2G…5G с использованием гражданских базовых станций в зоне ведения боевых действий;
- транковая связь стандарта Digital Mobile Radio (DMR), терминалы которого работают либо в режиме «трубка-трубка» (дальность связи около 5…10 км в зависимости от рельефа местности), либо в режиме «трубка-ретранслятор-трубка» (дальность связи до ретранслятора до 25…30км, зависит от трассы распространения радиосигналов). Эти терминалы используют стойкое шифрование и могут быть подключены в качестве модема к сети Интернет через специальные шлюзы, подключаемые к ретрансляторам, антенны которых размещаются на столбах, верхушках деревьев, крышах зданий и иных возвышенностях;
- классическая аналоговая радиосвязь;
- цифровая широкополосная радиосвязь в виде стационарных mesh-сетей и самоорганизующихся MANET- сетей, в основном регламентированных стандартами американского консорциума IEEE и реализованных в современных цифровых радиомодулях (например, семейства Falcon).

Также следует обратить внимание на планы по полномасштабному введению в эксплуатацию в ближайшие годы космической системы из нескольких тысач коммерческих низкоорбитальных малогабаритных искусственных спутников радиолокационной разведки, аналогичных космическим аппаратам системы Starlink.

Кроме того в основе действий сил и средств лежит фундаментальное понятие «боевого цикла» или «цикла боевого управления» Джона Бойда- «цикл Бойда» или OODA-цикл.

Следует обратить внимание и на выбор основной цели-выбивании личного состава. Поэтому усиливается работа по приоритетному выведению из строя личного состава, особенно специалистов беспилотных систем, разведки, радиоэлектронной борьбы, инженерных войск, медиков и др., а в основе стратегии по снижению военного и экономического потенциала лежит теория «пяти стратегических колец Уордена».

Линия боевого соприкосновения представляет собой смешанные участки почти сплошной линии обороны, а также участки с очаговой обороной, состоащие из укрепленных районов и опорных пунктов в населенных пунктах и вне их. Районы обороны и опорные пункты, созданные в населенных пунктах, могут оборудоваться как внутри их, так и на окраинах (особенно в промышленных зонах). Опорные пункты вне населенных пунктов, как правило, оборудуются с учетом использования местности (перепад высот, естественные преграды-реки, водоемы, овраги, леса, лесопосадки и др.).

Сегодна район боевых действий уже недостаточно воспринимать как «полосу наступлениа» или «полосу обороны», которые подразумевают территории, где воюют, и территории тыла, где готовятся воевать. Современный район боевых действий состоит из зон контроля – достаточно неоднородных и нечетко определенных зон, в разной степени подконтрольных воюющим сторонам, которые часто накладываются одна на другую или существуют одна внутри другой. Зона контроля – это производная двух составлающих контроля: 1) визуального контроля («видеть») и 2) огневого контроля (возможности нанести урон противнику). В этих зонах одновременно осуществлаются действия по усилению своего контроля (визуального и огневого) и противодействие (снижение или прекращение) контролю противника. Для простоты восприатия будем использовать цветовое обозначение зон контроля, как у светофора.

В глубину воюющих сторон от линии боевого соприкосновения располагается **красная тактическая зона**. Сегодня ее ширина около 15…20 км. Это зона сплошного контроля и высокой вероятности поражения противником, при входе в которую силы и средства каждой из сторон попадают в поле зрения разведки противостоащей стороны и по ним наносатся удары беспилотных систем, ракетных войск и артиллерии. Красная тактическая зона с каждой стороны трансформируется (перерастает) в **желтую тактическую зону**. Сегодня ширина желтой тактической зоны у каждой стороны составляет до 10…15км. Она характеризуется недостаточным контролем и существенно меньшей вероятностью поражения противником из-за удаления от линии боевого соприкосновения. Желтую тактическую зону обычно преодолевают рассредоточенным порядком пешком или с использованием высокоскоростных мобильных средств, в обоих случаях применяя беспилотные системы для разведки, огневой поддержки и снабжения. Размеры красной и желтой тактических зон по мере развития средств разведки и поражения постоянно увеличиваются. За желтой следует **зеленая тактическая зона** с основными силами и средствами сторон.

Нараду с этим в районе боевых действий формируются так называемые «серые зоны», появление которых обусловлено наличием хотя бы одного из нижеперечисленных факторов:

- нецелесообразностью полноценного использования данного участка местности (по совокупности причин);
- недостаточным контролем (визуальным и/или огневым) для захвата и удержания данного участка местности;

- несистемным присутствием тактических групп обеих сторон, что не позволяет осуществить закрепление на этой территории и контролировать ее.

В условиях вышеизложенного проводить штурмовые действия в вышеуказанных тактических зонах без реалистичного, детализированного планирования и тщательной подготовки нельзя! Но командиры старшего и среднего звеньев управления, к сожалению, до сих пор рассматривают штурм объектов шаблонно, чаще всего как «наскок пехоты». При постановке задач на штурм зачастую не проводится необходимая подготовка и доразведка района боевых действий, не выделается достаточного времени для проведения подготовительных этапов младшими командирами и подразделениями (доразведка, рекогносцировка, организация логистики, взаимодействие и т. д.), не реализуется должное боевое и всестороннее обеспечение.

Опыт боевых действий на Украине показал, что сами командиры подразделений часто плохо ориентируются в замысле старшего начальника, не видят общей картины боя и нередко получают указания типа: «иди туда – там никого нет» или «иди туда – там встретят». В случае потери связи это приводит к дезорганизации действий подчиненных подразделений, их деморализации и, как правило, к большим потерям и откату на исходные рубежи. Более того, такие действия командиров часто повторяются и по сути являются шаблонными. Недостаточно внимания уделяется организации введения противника в заблуждение (обмана) для сокрытия запланированных действий штурмовых подразделений.

Управление штурмом часто осуществлается из штаба высокого начальника и теряется с началом действий! Слабая всесторонняя подготовка штурмовых действий не позволяет, наблюдая и понимая картину боя целиком, своевременно реагировать на изменение обстановки, давать точные целеуказания и корректировку действий как штурмовым группам, так и артиллерии, и другим подразделениям боевого обеспечения.

Часто не организуются и не используются передовые подвижные пункты управления и временные/выносные пункты управления с распределением ответственности и возможностью дублирования функционала в случае возможной потери связи. Подразделения мало тренируются по действиям при потере связи. Недостаточно отрабатываются навыки действий при ведении боя в обороне, при закреплении на взятых позициях, в отрыве от основных сил и перекрытии логистических путей.

Недостаточное внимание на всех этапах боя уделается организации ключевого элемента успеха-**системного боевого обеспечения** (кратко-СБО).К СБО в современном бою относятся:

1) организация автоматизированной, сквозной («сверху-вниз», до окопа) системы поддержки принятия решения, обеспечивающей для всех применяемых сил и средств сбор, хранение, обработку (в том числе анализ) и использование всей имеющейся условно-постоянной и оперативной информации дла прогнозирования, планирования, координации и контроля предполагаемых и ситуативных действий (не путать с организацией управления в целом!);

2) комплексное (в том числе и в первую очередь с применением беспилотных систем) огневое поражение, подавление пунктов и средств управления, сил и средст введения воздушной и наземной разведки, сил и средств беспилотных систем, живой силы, техники, огневых средств, средств разведки и радиоэлектронной борьбы, систем связи и навигации противника в районе ведения боевых действий, уничтожение или нейтрализация его минно-взрывных заграждений и инженерных средств;

3) разведка и охранение, в том числе с применением разведывательно-сигнализационных приборов в доступных физических полях;

4) контрбатарейная борьба;
5) радиоэлектронная борьба;
6) противодействие беспилотным системам:
   - огневое поражение (так называемая противовоздушная оборона «нижнего и среднего неба»);
   - кинетическое воздействие (то есть перехват посредством соударения быстродвижущимся беспилотником-перехватчиком);
   - радиоэлектронное противодействие (как элемент радиоэлектронной борьбы);
7) связь (проводная и беспроводная, в том числе с использованием беспилотных систем) и автоматизированное управление;
8) тактическая маскировка (маскировка и имитация боевой (в том числе радиоэлектронной) обстановки);
9) медицинское обеспечение;
10) радиационная,химическая и биологическая защита;
11) инженерное обеспечение;
12) геопространственное обеспечение;
13) психологическая борьба (в том числе социальные технологии в Интернете);
14) метеорологическое обеспечение.

Системное боевое обеспечение ввиду бурного развития цифровых информационных технологий в современных условиях требует большего внимания и постоянного совершенствования. Чего стоит одно только то, что недостаточно продумываются вопросы организации надежной связи на различных этапах действий, особенно варианты действий при ее потере…

ВАЖНО! Разведка (во всех доступных физических полях), радиоэлектронная и психологическая борьба, применение беспилотных систем и противодействие им сегодня ведутся уже не только на уровнях бригады и выше, как это регламентировалось ранее руководящими документами, а начиная с уровня взвода (штурмовой группы)!

Опыт ведения боевых действий показал слабую обученность военнослужащих ориентированию и действиям в составе малых тактических групп на различных дистанциях огневого контакта, а так же при потере прямой видимости между подгруппами, действиям в отрыве от основных сил, во взаимодействии с бронетехникой (хотя ее использование становится редким) и особенно с различными беспилотными системами, при боях в городских условиях, лесистой местности, при действиях в окопах на опорных пунктах, а также недостаточное умение применять различные образцы вооружения и военной техники (штатные и трофейные).

Таким образом, боевые действия (способы и тактические приемы) стремительно менаются. Технологические прорывы в массированном применении беспилотных систем (воздушных, наземных), повышение тактической осведомленности, введение современных тактических и специализированных автоматизированных систем управления (для беспилотных систем, разведки, радиоэлектронной борьбы), внедрение систем искусственного интеллекта в штабах, в вооружении и военной технике привели к повышению оперативности принятия решения по действиям войск и нанесения комплексного поражения противнику.

В связи с этим **первоочередными задачами при планировании, проведении боевой подготовки и ведении боевых действий** являются:

- организация мониторинга и разведки района боевых действий на всю его глубину (способность «видеть»);

- повышение оперативности обработки массивов поступающей информации на основе устойчивых, скоростных сетей связи и автоматизированных систем управления, ее анализа, оценки, предоставления итоговых прогнозов и вариантов действий, приоритетности поражения целей, целеуказаний и расчетов;

- действия по выявлению и уничтожению пунктов управления подразделениями и частями противника;

- выявление и уничтожение/поражение/подавление пунктов управления, приемо-передающих систем (ретрансляторов), линий связи, а также средств, комплексов и систем разведки и радиоэлектронной борьбы;

- выявление и уничтожение пунктов управления, расчетов беспилотных систем;

- комплексное, многоуровневое применение всех средств нанесения урона противнику;

- постоанное системное боевое обеспечение и общее обеспечение боевых действий на всех этапах боя **цикла «Контроль – Захват – Закрепление - Контроль»**;

- организация бесперебойной логистики в районах ведения боевых действий;

- организация и обучение штабов и подразделений введению в бой без сосредоточения больших масс и средств в зонах досягаемости оружия противника – поэтапный ввод в бой с подхода, а также использование скоростного ввода в бой на специальных средствах (багги, квадроциклы, мотоциклы, беспилотные наземные системы большой грузоподъемности);

- организация обеспеченного подхода штурмового подразделения к объектам штурма, а также подвоза и эвакуации;

- организация подготовки специалистов беспилотных систем, операторов АСУ и цифровых систем, радиоинженеров, исходя из необходимости достаточного кадрового насыщения с формированием кадрового резерва!

При проведении современных наступательных действий в условиях сложного построения района боевых действий и влияния технологичного вооружения особую роль играют **штурмовые отряды**. Штурмовой отряд является ударной силой, способной взламывать оборону противника, обеспечивая дальнейшее наступление части или соединения.

ВАЖНО! Штурмовой отряд всегда находится в одном из двух состояний – штурм и подготовка к штурму!

Следует обратить особое внимание на то, что полноценное восстановление личного состава, вооружения и техники после выполнения боевой задачи является началом подготовки к следующим действиям.

Оптимизация алгоритма принятия решений командирами применительно к штурмовым действиям повышает эффективность действий подразделений и минимизирует потери. Значительно повысить эффективность работы командиров штурмовых отрядов можно, впервую очередь, за счет:

- вовлечения в процесс принятия решения младших командиров подразделений-командиров штурмовых групп и смежников (приданных и поддерживающих штурм подразделений);

- организации боя младшими командирами подразделений и принятия ими решения «снизу», т. е. на основе вариантов действий и решения командира основной штурмовой группы с целесообразной поддержкой силами и средствами СБО и средствами старшего начальника;

- введения вариативности выполнения боевой задачи.

1.2 Боевые принципы

Необходимо помнить и понимать, что каждый бой имеет четко сформулированную цель (или несколько целей)! При простоте этого тезиса его часто или забывают, или не могут сформулировать саму цель. «Пойдем и захватим», «Нужно взять/захватить»-не является целью и не будет понятно ни солдату, ни командиру. Цели в основном заложены в боевых приказах и распоряжениях старших командиров и должны соответствовать тактическим планам старшего начальника, а также быть четко взаимосвязанными с предыдущими и последующими действиями на данном участке.

При том, что бой не имеет ограничивающих законов (мораль боя зачастую определяется желанием выжить в бою!), а обстановка и действия никогда полностью не повторяются, целесообразно рассматривать подготовку и ведение боевых действий на основе боевых принципов.

Боевые принципы являются сокращенной и удобной формулировкой тактических принципов, прописанных в боевых уставах, а также основой для принятия целесообразных и необходимых решений командира/бойца, как плановых, так и вновь возникающих на поле боя, в боевой подготовке. То есть работают от бойца и выше. При этом всегда следует помнить: **«НА ВОЙНЕ ЛЕНЬ И ПАНИКА УБИВАЮТ ЕЩЕ ДО ПУЛИ!».**

Для достижения цели в бою необходимо руководствоваться следующими боевыми принципами.

Выживать - комплекс мероприятий для сохранения бойца/подразделения как активной боевой единицы. Включает как подготовку к боевым действиям, так и системное применение тактико-огневой, тактической, инженерной, физической и ресурсной подготовок, подготовки по применению устойчивых средств автоматизации управления и связи, разведки, управления, радиоэлектронной борьбы, беспилотных систем и средств противодействия им, медицинскую и другие виды подготовки и обеспечения.

Поражать - целенаправленные, системные, ресурсно - обеспеченные действия ВСЕМИ доступными средствами, наносящими урон противнику (без ограничения сфер применения и воздействия)при выполнении огневых и тактических задач.

Данные действия взаимосвязаны и не должны рассматриваться друг без друга. Чтобы выживать - нужно поражать, чтобы поражать - нужно выживать! Чтобы выживать и поражать – необходимо иметь способность «видеть» поле боя.

Видеть — способность знать и понимать обстановку на поле боя за счет его охвата всеми средствами наблюдения и разведки на всю возможную глубину, постоянного анализа местности и прогноза возможных действий противника, оперативного контроля его действий и действий своих сил по всему фронту и на всю возможную глубину. Основная задача командиров до боя и во время боевых действий - создавать целесообразные и эффективные цепочки непрерывного управления на основании способности «видеть».

Управление — это циклическая система непрерывных и целенаправленных действий, которая обеспечивает возможность:

– понимать обстановку (на основе способности «видеть»);

– прогнозировать варианты развития обстановки (способность «предвидеть»);

– планировать задачи на основе наиболее вероятных вариантов развития обстановки;

– координировать (организация взаимодействия, в том числе со смежными, приданными и поддерживающими подразделениями, до и в ходе боя!);

– контролировать выполнение задач плана;

– реагировать на все изменения обстановки, используя способность «видеть» и гибко «на лету» корректируя свои действия.

При этом имеет место следующая иерархия(снизу вверх).

Реагировать

Контролировать-Координировать

Понимать -Прогнозировать -Планировать

На основании способности «видеть» необходимо думать за противника, оценивать и прогнозировать его вероятные действия. Это означает предвидеть действия противника, учитывать и готовиться к возможному развитию ситуации. При этом следует мысленно не подыгрывать своему плану, а, наоборот, планировать свои действия на случай самого негативного варианта развития ситуации.

На основании способности видеть и предвидения действий противника необходимо создавать условия для совершения противником ошибок (втягивать его на путь ошибок и вести по этому пути) и использовать их в своих целях. На данный момент это делать все труднее, так как противник массированно использует многоэшелонированные системы разведки, связи и автоматизации управления, которые значительно ускоряют работу с огромными массивами различной информации, а также выдачу готовых решений для средств поражения и вариантов реагирования на тактическом уровне и выше.

Если вы считаете, что противник глуп, то вы глупее!

«Видя» поле боя и предвидя противника, необходимо, исходя из цели и ситуации, наращивать готовность к действиям. Это принцип для подразделения, бойца и вооружения. При любых действиях стремитесь расширять фронт.

Это касается наблюдения (способность «видеть»), позиции, огня, маневра, связи, возможностей. Мышление и наблюдение должны быть шире и глубже. Постоянно улучшите позицию!

Расширение фронта и способности «видеть» позволяет выявлять «дырки» (уязвимости), т. е. слабые места у себя и противника с учетом изменяемой обстановки, а также «собирать кулак» – сосредотачивать усилия. Выявленные «дырки» – это потенциальные направления сосредоточения усилий. Этот принцип касается всех ресурсов.

Слабое место/звено у себя следует закрывать, а у противника – использовать.

Не воспринимайте бой как полигон. Исходите из того, что противник Вас постоянно видит, а у него могут быть скрытые ресурсы! Всегда учитывайте возможность внезапного появления и воздействия противника.

Проявляйте гибкость. Любые изменения не должны ставить ступор командира и подразделение. Необходимо подстраиваться под изменяющуюся обстановку. Надежный план учитывает все изменения обстановки и имеет варианты решения.

Решения, действия и обеспечение должны быть максимально надежны и не запутаны. В боевой подготовке исключаются ненадежные действия и «навыки-фокусы».

Огневая инициатива – своевременное, комплексное использование всех огневых и других средств поражения – обеспечивает выживаемость вашего подразделения, поражение/подавление противника на всех дистанциях и невозможность его дальнейшего сопротивления!

Маневрирование подразделения, бойца и огня обеспечивает выживаемость и достижение задач боя.

Важно отметить, что перечисленные боевые принципы во многом детализируют применительно к современному бою.

1.3 Борьба за информацию

Суть современной революции в военном деле. Сегодня много говорится о важности современных цифровых информационных технологий на поле боя. Ведь именно они стали основной причиной происходящей сейчас революции в военном деле. Однако информация это основа любой деятельности. В бою информация была важна всегда. Суть же современной революции в военном деле состоит в том, что новые цифровые информационные технологии лишь добавили еще больше информации, намного больше... и усовершенствовали все процессы по ее сбору, хранению, обработке, передаче и использованию. В результате стало очевидно, что имеет *огромное* преимущество та сторона, которая лучше работает с информацией (своей и противника), в том числе быстрее (то есть быстрее ее боевые циклы/циклы боевого управления).

По сути, сейчас революционный скачок, связанный с ситуацией с информацией на поле боя, аналогичен тому, как если бы вы раньше играли в классические шахматы, где правила просты и привычны, а теперь от двухмерной шахматной доски вынуждены перейти к трехмерному шахматному пространству, где к двум измерениям добавилось третье, характеризующее информацию во взаимно пересекающихся боевых циклах не только отдельных бойцов, средств и подразделений, но и противоборствующих сторон в целом. В такие «шахматы» всему миру еще только предстоит научиться играть.

Разведка и маскировка. Начинается работа с информацией на поле боя с разведки. То есть разведка является первым этапом любого боевого цикла. Разведка – это система мероприятий и действий, проводимых в целях добывания сведений о противнике, местности и погоде, необходимых для подготовки и ведения боя. Она дает способность «видеть».

Задачи разведки:

– выявление (поиск и обнаружение), вскрытие (распознавание, классификация, понимание структуры обнаруженного) и отслеживание;

– характеристик местности в районе боевых действий, которые во многом определяют и помогают предположить возможности, тактику действий обеих противоборствующих сторон. Местность играет ключевую роль, являясь одновременно объектом изучения, фоном и условием, влияющим на действия противника и наших сил и средств, а также на возможности и способы ведения разведки;

– состава, состояния и вероятного характера действий противника в зоне ответственности;

- изменений в составе, состоянии и положении подразделений противника, действующих в зоне ответственности с учетом наращивания резервами с других направлений;

- маршрутов ротаций и эвакуации, подвоза боеприпасов и материальных средств на передовые позиции;

- районов действий диверсионно-разведывательных групп противника;

- применения противником беспилотных систем, их каналов управления, передачи данных, навигации и взаимодействия с вышестоящими органами управления;

- местоположения и функционирования командных пунктов и пунктов управления противника;

- местоположения и деятельности сил и средств разведкии радиоэлектронной борьбы противника;

- порядка развертывания и изменений в составе, построении и функционировании АСУ, связи и других видов боевого обеспечения противника;

- состава и боеспособности резервов противника, порядка, сроков и маршрутов их переброски;

- изменений в составе поддерживающих противника сил и средств;

- изменений в системе материально-технического обеспечения противника, в том числе переброски резервов.

Разведчик ищет различные сведения (информацию), добывая их, вычленяя и объединяя в разведпризнаки объектов, действий, определенных свойств (например, местности) или замыслов противника.

Разведка ведется в отношении заметных для нее объектов во всех известных физических полях.

Заметность объекта – это совокупность его отражательных и излучательных свойств, определяющих возможность его обнаружения и/или распознавания и/или наведения на него оружия на различных фонах наблюдения.

Виды разведки в тактическом звене:

- по сферам действий - наземная, воздушная и космическая (морская здесь не рассматривается);

- по применаемым техническим средствам:

1) **оптоэлектронная разведка** (без электроники называется оптической) – прием и анализ *электромагнитных волн* ультрафиолетового, видимого и инфракрасного диапазонов, которые создаются или переотражаются объектами разведки. Включает:

а) телевизионную разведку;

б) инфракрасную или тепловизионную разведку (не путать с радиотепловой разведкой!);

в) лазерную разведку;

2) **радиотепловая разведка**- обнаружение и определение местоположения объектов по их тепловому излучению в радиодиапазоне электромагнитных волн (не путать с инфракрасной разведкой!);

3) **радиоэлектронная разведка** (в радиоволновом диапазоне электромагнитных волн). Включает:

а) радиоразведку- поиск, обнаружения, идентификация, пеленгование, перехват и анализ излучений радиоэлектронных средств связи (радиостанций);

б) радиотехническую разведку - поиск, обнаруяения, идентификация, пеленгование и анализ излучений радиоэлектронных средств, не используемых для связи;

в) радиолокационную разведку- добывание сведений о параметрах (координатах, направлении движения и т.д.) целей (называется параметрической разведкой) и получение радиолокационных карт местности- аналогов фотографий (называется видовой разведкой);

4) **магнитометрическая** или магнитная **разведка** – определение местоположения объектов на основе измерения создаваемых ими возмущений магнитного поля Земли для разминирования и поиска замаскированных объектов;

5) **акустическая** или звуковая (звукометрическая) **разведка** (в т.ч. гидроакустическая) – определение местоположения источников механических волн (не путать с электромагнитными волнами!) в воздухе и воде (например, стреляющих орудий,

минометов, пусковых установок, мест разрывов снарядов, работающих беспилотников);

6) **сейсмическая разведка** – определение местоположения источников механических волн на поверхности Земли и внутри нее;

7) **компьютерная разведка**–добывание, сбор, доставка и анализ цифровых данных в компьютерных сетах: проводных и беспроводных (не путать с радиоразведкой!);

8) **метеорологическая разведка**–добывание и анализ информации для определения текущего состоания и/или прогнозирования будущего состояния атмосферы в конкретном месте и в конкретный момент времени;

9) **радиационная, химическая, биологическая разведка**.

Различные виды разведки объединаются, обеспечивая, например, артиллерийскую, инженерную разведку.

ВАЖНО! Разведка противника ищет вас всегда, используя для этого все физические поля!

Спутниковая оптическая и радиолокационная разведка ведется непрерывно с периодом обзора, равным 4…6 часам, с передачей целеуказания на тактические средства поражения через 10…15 минут после обзора района. Качество, с которым ведется со спутника, не хуже, чем качество карты в приложении Google Maps.

Возможности оптического наблюдения критически зависят от метеоусловий. Но этого недостатка лишена видовая радиолокационная разведка. Качество радиолокационных снимков сегодня близко к качеству фотографий.

Если вас не увидели спутники противника, то это может сделать его воздушная разведка (например, на БАС типа «Mavic 3» и аналогичных). Площадь, которую одновременно может осматривать оператор БАС типа «Mavic 3» без увеличения (без «зума»), составляет около 400×400 м. При максимальном увеличении эта площадь составляет около 25×25 м. Поэтому скорость перемещения в районе, в котором ведется воздушная разведка, должна исключать возможность явного обнаружения объекта без увеличения. Обычно это достигается переползанием со скоростью около 10 м за 1 минуту.

Также используется системы разведки наземных движущихся целей –это сеть из многих сенсоров (в основном оптических, сейсмических и акустических), разнесенных в пространстве и предназначенных для наблюдения за большими по площади участками местности, позициями, районами сосредоточения, путями движения войск, водными преградами и переправами в реальном масштабе времени, обеспечивая при этом возможность не только обнаруживать, но и распознавать цели (гусеничную и колесную технику, личный состав), а также фиксировать время, направление, скорость движения и определять длину колонн военной техники. Также эти системы могут прикрывать минные поля и другие заграждения, забрасываться в предполагаемые или заранее намеченные районы (рубежи) дистанционного минирования либо в иные запланированные районы. Датчики движения реагируют на появление людей и техники на дальности до 3 км. Дальность обнаружения человека и автомобиля видеокамерой и тепловизором может составлять до 20 км, танка – до 40 км.

ВАЖНО! Защита от разведки — это **МАСКИРОВКА.** Маскировка в радио-, радиолокационном, оптическом и акустическом физических полях - это основа выживания. Малейшая оплошность в маскировке - и Вас обнаружили. Далее вопрос времени - как противник использует разведанную информацию. Но помните, что он ее обязательно использует.

В движении и при нахождении на месте необходимо продумывать применение средств

тепломаскировки. Опыт показал, что от обнаружения тепловизором защищает:

- наличие преграды;

- плотный изоляционный кусок материи, натянутый на дистанции не менее полуметра от источника тепла (чем сильнее источник тепла, тем на большей дистанции должен быть натянут экран);

- элемент сооружения или конструкции, не способный нагреться на всю свою глубину от воздействия источника тепла;

- использование специальных костюмов, пончо, накидок и элементов обмундирования, скрывающих тепловое излучение тела (заранее проверенных в условиях, приближенных к боевым). Помните: при использовании пончо необходимо учитывать его маскирующие свойства с местностью, погодой и временем суток! Края защитных накидок и пончо обладают демаскирующими тепловыми контурами;

- использование природных (трухлявые пни, нагреваемые в солнечную погоду поверхности) или иных источников тепла (лесной или городской пожар, плотная дымовая завеса) для маскировки (уменьшения яркости, размывания, изменения формы) своего теплового следа;

- рассеивание (уменьшение заметности) исходящего горячего воздуха от работы двигателей и печей при помощи наложения большого количества веток в местах выхода теплого воздуха из труб (систем вентиляции).

Для маскировки позиций техники не следует пренебрегать использованием участков и зон затемнения от крупных объектов (домов, стен, сооружений, деревьев и специально созданных валов, курганов). Участки затемнения ослабляют эффективность обнаружения объектов в них.

НИКОГДА не следует использовать личные устройства связи для выхода в Интернет и обмена информацией по обычным сотовым сетям, находясь в зоне боевых действий. Наличие средств мобильной связи и выхода в Интернет в зоне военного конфликта, а также средств их пеленгации и кражи конфиденциальной информации вносит множество особенностей в ход ведения боевых действий. Это одна из сфер современной войны, и противник использует ее эффективно. Для любого использования открытых сетей (мобильных сетей и Интернета) необходимо иметь не связанный информационно с человеком аппарат («чистый» телефон, смартфон, планшет и др.) и использовать заранее обговоренную систему шифрования передаваемой информации (известную всем абонентам). Используя устройства связи, надо учитывать высокую вероятность перехвата переданных сообщений и вычисления месторасположения абонентов. Использование таких каналов связи оправдано только в ситуациях, когда важность оперативной передачи данных больше, чем ущерб от передачи противнику своего местоположения и факта совершения каких-либо действий.

ПОМНИТЕ! Личный мобильный телефон подключился к сотовой сети - через 15 мин всю группу накроют.

Главный принцип разведки–скрытность! Поэтому даже если вы полагаете, что в непосредственной близости на поле боя противника нет, то нужно помнить, что любое средство радиосвязи может прослушиваться специалистами разведки противника, находящимися в десятках километрах от вас.

Любые переговоры по средствам радиосвязи должны вестись по переговорным таблицам, которые нужно менять по возможности как можно чаще.

Смартфон в бою - друг, помощник и **враг (!)**, если не подготовлен специалистами для выполнения боевой задачи. При этом следует помнить, что не каждый, кто себя называет специалистом, действительно является таковым. **Доверяй, но проверяй!** При подключении к любой сети, имеющей доступ в Интернет (даже если вы лично не знаете, что такой доступ есть), неподготовленный смартфон связывается с удаленными серверами той страны, которая произвела его операционную систему. То есть, по сути, ваша информация попадет в руки противнику. А **все, что попало в Интернет, будет там ждать своего часа вечно!**

После добывания информации ее необходимо сохранять и обрабатывать для прогнозирования и планирования действий своих сил и средств не только в виде огня, ударов и маневра, но и для ведения борьбы за информацию, то есть информационно – технических и

информационно - психологических воздействий на противника и защиты от таких воздействий с его стороны.

1.4 Информационно-техническая борьба

Информационно – техническая борьба - это техническая составляющая борьбы за информацию на поле боя, включающая наступательные и оборонительные действия сторон с использованием информационно – технических средств во всех физических полях и в киберпространстве.

То есть информационно-техническая борьба — это не только радиоэлектронная борьба, а радиоэлектронная борьба - это не только ставшее уже привычным на поле боя радиоэлектронное противодействие БпС противника.

Воздействия в радиоэлектронной борьбе (здесь и далее подразумеваем информационно – техническую борьбу) разделяются на поражение и подавление.

Подавленное состояние объекта воздействия - это когда он не работоспособен в течение воздействия, но работоспособность восстанавливается по завершении этого воздействия. Пораженное состояние объекта воздействия - это когда его работоспособность не восстанавливается даже после завершения воздействия.

Базовы принципы РЭБ состоят в следующем.

РЭБ предполагает не только блокирование работы систем противника и противодействие аналогичному воздействию с его стороны, но и активные мероприятия по дезинформации средств разведки противника, в том числе путем создания ложной обстановки. РЭБ также включает разведку (в первую очередь-РЭР), нарушающую конфиденциальность информации противника.

Радиоэлектронная борьба всегда начинается с разведки. Ведение радиоэлектронной борьбы без средств разведки, как это нередко бывает при эксплуатации средств радиоэлектронного блокирования беспилотных систем, -это бой вслепую! Только разведка дает информацию о том, какие средства радиоэлектронной борьбы актуальны в текущий момент времени. Через час, а тем более день все может измениться.

Средства разведки принимают сигналы или излучают зондирующие сигналы (например, радиолокационные станции или РЛС). Средства РЭБ может включать (а может и не включать!) подсистему разведки. Но его обязательным элементом является подсистема подавления / поражения, которая только излучает сигналы или меняет условия распространения волн в различных физических средах.

1.5. Информационно-психологическая борьба

Ключевое значение на поле боя имеет борьба «за умы», она же информационно-психологическая борьба (как составная часть борьбы за информацию) или, кратко, психологическая борьба. Потенциально ее эффективность не меньше, чем эффективность всех остальных средств вооруженного противоборства вместе взятых! Ведь только она может достичь выполнения боевой задачи без последствий для здоровья противника.

В информационно-психологической борьбе используются те же свойства безопасности информации, что и в информационно-технической борьбе: конфиденциальность, целостность и доступность. Однако способы воздействия на человека, естественно, специфичны. В основном сначала нарушается конфиденциальность информации субъекта воздействия (то

есть человека или группы лиц), а за тем на основе полученной информации нарушается целостность его информации (дезинформация) и/или ее доступность. Но нередко нарушается исключительно доступность субъекта воздействия.

Цели информационно-психологических воздействий:

1) выведывание важных сведений (нарушение конфиденциальности информации);

2) вывод из строя субъекта воздействия (нарушение доступности носителя информации);

3) снижение эффективности работы субъекта воздействия (нарушение доступности носителя информации);

4) вброс деструктивной информации в долгосрочных целях (нарушение целостности информации);

5) достижение управляемости субъектом воздействия (нарушение целостности информации).

Информационно-психологические воздействия в боевых условиях осуществляются:

- на **центральную нервную систему (ЦНС)** субъекта воздействия путем его физического и психологического подавления / поражения или изматывания из-за нахождения в постоянном напряжении;

- **сознание**. В боевых условиях работа с сознанием ведется по принципу: «добрым словом и оружием можно добиться гораздо большего, чем одним только добрым словом».

ВАЖНО! Способом защиты от изматывания центральной нервной системы является отдых. Эффективный отдых достигается сном (даже в течение 15…20 минут) или полным намеренным расслаблением всех мышц тела, в первую очередь – лица, остановкой внутреннего диалога с собой и намеренным отключением мыслительной деятельности.

Для подавления/поражения ЦНС могут применяться средства не летального воздействия:

- формирующие чувство страха (например, использующие акустические волны ниже или выше слышимого диапазона);

- ограничивающие функции (например, ослепление, оглушение).

В основе работы с сознанием лежит не контролируемая способность головного мозга запоминать события информировать знания об окружающей действительности с использованием собственного интеллекта.

Воздействие на сознание осуществляется передачей человеку **мемов.** Мем (англ. meme) – это единица значимой для культуры информации, то есть идей, символов, манер, ситуаций или образа действий. Мемы содержатся в речи, письме, видео, ритуалах, жестах и т. д. Мемы настраивают сознание человека, как регулировщик скрипку. Мемы могут быть для человека полезными и деструктивными. Но в любом случае они подобны «вирусам» (как собирательному образу болезнетворных микроорганизмов) в человеческом теле и компьютерных системах. Человек, в сознание которого попал мем, может передавать его всем, кто с ним взаимодействует. Мемы ориентируются на группу людей, выделенную по некоторому множеству признаков. Они действуют вероятностно предопределенно, то есть на большинство представителей группы, а не на каждого.

Воздействие противника мемами на сознание основывается:

1) на вплетении в ложную информацию правды, подаваемой как глубокая мысль, с которой невозможно не согласиться, в целях размягчения критического восприятия для последующей манипуляции;

2) дискредитации командования и военно-политического руководства страны,

формировании из них образа врага;

3) запугивании;

4) имитации смысла;

5) инсценировках порочащих нас действий;

6) использовании только тех фактов, которые подтверждают навязываемую точку зрения, и игнорировании всех противоречащих;

7) компрометации лиц, принимающих решения;

8) критике не аргументов, а самого человека;

9) манипуляции фактами, в том числе формированием мозаичного восприятия информации, когда она разделяется на фрагменты, отдельные события и факты и предъявляется по нескольким информационным направлениям так, чтобы объект не смог соединить их и осмыслить в целом;

10) многократном повторении одного и того же утверждения, которое рано или поздно заставляет людей воспринимать его как правдивое («вода камень точит»);

11) навешивании «ярлыков» для создания упрощенного и крайне негативного образа, чтобы сплотить «своих» и оправдать любые действия против «чужих»;

12) отвлечении внимания от реальных фактов:

- путем сознательного смещения акцента на деструктивную информацию;

- переориентации внимания, когда деструктивная информация подается на фоне эмоционально или ярко выраженных правдивых сообщений;

- формирования «информационного шума» для наступления «информационного насыщения», когда человек неспособен распознать действительно важную информацию в общем потоке сообщений;

эмоционального окраса, частично замещающего смысловое содержание информации и навязывающего деструктивное восприятие фактов;

13) подмене тезисов, первоочередных проблем вымышленными (малозначительными), в том числе передачей «сакральных знаний»;

14) призыве «Все так делают!», демонстрации «очевидцев» и «лидеров мнений»;

15) приписывании нам противником его собственных негативных качеств или мотивов;

16) провокациях;

17) систематическом внушении человеку, что он неверно воспринимает реальность;

18) нарушении логики или убеждении, что одно небольшое событие неминуемо приведет к катастрофическим последствиям без доказательств причинно-следственной связи;

19) формировании ложной дилеммы (только два крайних варианта, игнорируя не только варианты за пределами биполярного отрезка, но и промежуточные варианты);

20) склонности человека воспринимать информацию как достоверную, если она не противоречит информации, поступившей ранее и т. д.

В основе воздействия на сознание лежит **принцип «чистого листа»**, согласно которому первое услышанное человеком правдоподобное мнение о чем-либо становится его собственным. Поэтому деструктивные информационные воздействия противника легче упреждать, чем исправлять их последствия. Если упредить информационно- психологические воздействия на сознание не удалось, то нужно помнить, что они навязывают:

1) страх-оказывает наибольшее влияние;

2) вину, несправедливость;

3) стыд;

4) эгоизм;

5) ложность подаваемой руководством информации;

6) иллюзии, тщеславие, ложную уверенность в своем превосходстве;

7) привязку к материальным благам.

Если у военнослужащего появилась деструктивная для его мотивации информация (видеоролики, продукты средств массовой информации, репортажи, утверждения противника или лиц, действующих в его интересах), то ее надо не запрещать, а показывать ее несостоятельность (ложность, постановочность) на примере других сведений. Задача всех командиров – найти в условиях использования сети Интернет опровергающие или смещающие акценты материалы и показать их усомнившимся военнослужащим с подробными разъяснениями предполагаемого значения. Нельзя запретить людям думать, но можно дать пищу для ума, которая приведет его к правильным выводам.

В условиях недостаточного патриотического и политического воспитания многие военнослужащие не понимают причин своего участия в боевых действиях. В реалиях современной войны (при наличии у личного состава большого количества источников информации различной достоверности, а зачастую и целенаправленно ложных) устоявшиеся способы ведения военно-политической работы (например, в виде боевых листков и стенгазет) устарели.

Достижение эффекта от деструктивных информационно – психологических воздействий, убеждающих в чем-то, может быть растянуто во времени. В течение этого времени человеку необходимо получить контрубеждение, то есть убеждение в обратном. Дла этого требуется:

- развивать критическое мышления;
- контролировать свои эмоции;
- искать первоисточники и проверять информацию;
- иметь возможность обсудить ставшую вам известной неоднозначную информацию со здравомыслящими сослуживцами или командирами;
- знать правду о своих сильных и слабых местах и помнить: **ошибаться можно–врать нельзя!**

Боевой стресс для профессионалов – это нормальная естественная среда, но при его длительном воздействии и для неподготовленных может негативно «выстрелить»:

- агрессия. Признаки: оскорбления, импульсивность, направленность прямой агрессии «на кого-то, что-то», восприятие окружающих как угрозы. Что делать? Спокойно заговорить, избегать обвинений и угроз, переключить внимание (на задачу или последствия его действий). Если возможно, то нарубить дров, прокричаться;

- истерика. Признаки: слезы, паника, вычурность, театральность, стремление обратить внимание. Что делать? Замкнуть внимание (громкий звук, неожиданный жест), развернуть спиной к окружающим, говорить твердо, четко и ясно, скомандовать: «Успокойся!», «Стоп!», «Замолчи!», «Возьми себя в руки!», дать воды или «леща»;

- ступор. Признаки: неподвижность или заторможенность, молчание или замедленность речи, отсутствие реакции на обращение. Что делать? Обеспечить безопасность (убрать с линии огня), говорить четко, обращаться по имени или позывному, интенсивно растереть ладони, уши;

–дрожь. Признаки: частое судорожное сокращение мышц, мелкие неконтролируемые движения, заикание, прерывистость речи. Что делать? Успокоить, объяснить причину реакции, взять за плечи, заставить сжать кулаки, задержать дыхание на 5…7секунд и с

выдохом расслабиться, напоить сладким чаем.

Техника «заземления». При панике нужно переключить внимание: покрутить патрон в ладонях, проверить турникет (жгут), прочитать надпись на жетоне, заглотить леденец и т. п.

После «замеса» всегда идет «откат». Это не использованная энергия, которая мешает заснуть, вызывает дрожь в руках и невозможность усидеть на месте. Для «спуска пара» нужна взрывная физическая нагрузка (например, «burpee (бёрпи)»).

Универсальные средства от стресса: «физуха», еда, сон, чтение книги, шутка, музыкальный «трек» в голове и аварийные – молитва, мат.

Страх – основа выживания. Он мобилизует тело и психику, чтобы максимально быстро действовать и спасаться. Иногда страх может стать неконтролируемым, мешать критически мыслить и адекватно действовать, перерастает в панику. Понимаешь, что паника атакует и теряешь контроль, сядь на колено, дыши и осмотрись. Мысленно задавай себе вопросы: «Кто ты?», «Где ты?», «Где товарищи и оружие?», «Какая задача?». Ну и, конечно же, следует говорить себе все сильное «НАДО!» Если страшно, то нужно лечь, осмотреться и задать себе те же вопросы, завершив их тем же «НАДО!». Страхом можно и нужно управлять, обуздать его и использовать в своих интересах. Задача состоит не в том, чтобы «уничтожить» страх, а в том, чтобы превратить в ресурс боевой деятельности.

Страх – это еще и «бей», а не только «беги» или «замри». Вместо того, чтобы говорить себе: «Успокойся», лучше сказать: «Вот это заряжает меня по полной!». Смерть слепа, но издалека чувствует панику. Помни пословицу: «Кто ссыт – тот гибнет!»

При встрече с противником не паникуйте, держитесь спокойно, действуйте нагло и дерзко. Умение быстро и агрессивно использовать свое оружие в критической ситуации существенно увеличивает шансы выйти «из воды сухим».

Наиболее распространенные способы информационно- психологического воздействия:

- первый-«матюгальник» (звуковещательная станцианя машине или дрон с колонкой), курсирующий и орущий вдоль ЛБС;
- листовки;
- «радио». Выход в эфир по открытым каналам радиосвязи;
- «СМС-рассылка»;
- пропаганда в Интернете;
- распространение дезинформации через «фейковые» аккаунты рейтинговых средств массовой информации;
- создание «фейковых» волонтерских проектов для получения персональных данных («Нужны дроны? Заполните форму: ФИО, звание, должность, воинская часть, телефон»);
- «медия ловушка».Цель – знакомство с военнослужащим в социальных сетях через подставные аккаунты для получения необходимой информации или проведение мероприятия по его «заманиванию» и захвату;
- «звонок родственникам». Цель -запугивание, манипуляции, мошенничество.

Плен, если это случилось… Все происходит быстро и на стрессе, как правило, по этапам: захват-первичный, допрос-конвоирование-содержание. Наиболее жесткие-первые три. На допросах: в глаза не смотреть, «играть Васю», номера телефонов родственников не передавать. Не проявлять активности, не говорить первым, не говорить много и громко. Нейтральный холодный диалог, без агрессии, без заинтересованности.

Побеждают того, кто решил сдаться!

Принять необратимость произошедшего, сохранить волю, не верить противнику, не соглашаться на интервью, поддерживать других словами и действиями. Боевая триада

плена: Борись и выживай! – Беги! – Умри героем!

Источник: https://publishing.intelgr.com/index.php/izdannye-raboty?id=1106