Введение

Поле битвы будущего — это прежде всего информация.
Николай Огарков [14].

Четыре газеты смогут причинить больше зла, чем стотысячная армия.
Наполеон [11].

Информационное противоборство (ИП) как направление научных исследований и практической деятельности имеет давнюю историю. Оно возникло одновременно с появлением вооруженного противоборства как составная часть вооруженной борьбы в виде средств и способов информационно-психологического воздействия (ИПВ) как на противника для ослабления его боевой мощи, так и на свои войска для поднятия их боевого духа. С возникновением государств и благодаря появлению, массовому распространению и доступности новых, более эффективных носителей и средств доставки информации, на основе которых происходит принятие решений, ИП продолжило активно развиваться и стало составной частью взаимоотношений между странами [8; 9; 29; 44].

Вследствие продолжающейся научно-технической революции в области информационных технологий происходят глубокие качественные изменения в направлениях развития вооружения и военной техники. Одной из основных тенденций в этом процессе является ориентация на разработку различного рода средств информационного воздействия (СИВ). В первую очередь это постоянно совершенствуемые средства радиоэлектронной борьбы и психологических операций, средства проведения так называемых «кибернетических атак» в информационных сетях, а также средства информационно-психологического (СИПВ) и информационно-технического воздействия (ИТВ).

Сегодня правомерно утверждать, что в XXI в. в социальной сфере окончательно сформировалось новое явление, которое в различных источниках получило такие названия, как «информационное противоборство», «информационная борьба» (ИБ), «информационная война» (ИВ), «сетецентрическая война» (СВ), «психологическая война» (ПВ) [1–4; 8; 9], и что при прочих равных условиях достижение государством стратегических преимуществ будет зависеть от имеющихся у него информационных возможностей [18; 27; 32–34].

Особенностью ИП является то, что оно включает две составляющие: информационно-техническую и информационно-психологическую, ведется между государствами не только в военное, но и в мирное

время, ведется явно и скрытно в защиту собственных интересов, за зоны политического влияния, за рынки сбыта, за спорную территорию, за укрепление оборонной сферы. Оно постоянно ведется и внутри каждого государства за власть и деньги, за возможность управлять большими массами людей, за контроль над производством и за доходы от реализации продуктов производства. Вмешиваясь в регулирование потоков информации, воздействуя на ход ее обработки и управления, можно влиять на те или иные события и процессы. В этом-то и кроется одна из причин ожесточенной борьбы за контроль над средствами массовой информации (СМИ), а значит, и за контроль над сознанием населения страны.

В ходе информационного противоборства (борьбы) (ИП(б)) поражение информационного ресурса (ИР) (элементов ИР) реализуется многочисленными способами и средствами (средствами информационного воздействия (СИВ)). В зависимости от объектов воздействия различают средства информационно-технического воздействия (ИТВ) и средства информационно-психологического воздействия (ИПВ).

Возможные способы ИТВ на технические объекты (например, системы и средства управления войсками и оружием) включают радиоэлектронное подавление (РЭП) (радиоподавление и оптико-электронное подавление) и радиоэлектронное поражение (функциональное поражение и поражение специальным программно-аппаратным воздействием (СПАВ)).

В рамках информационно-психологического противоборства (ИПП), воздействуя средствами ИПВ на психику (сознание, подсознание) информационных объектов (народа, общественных групп, лиц, принимающих решение (ЛПР)) противостоящей стороны, решается задача по их когнитивному[1] подавлению и (или) подчинению, а применительно к информационным объектам своей стороны — по их информационно-психологической защите от средств ИПВ.

ИПВ — это особым образом организованные энергоинформационные потоки излучений физической природы, которые носят деструктивный характер и направлены на трансформацию индивидуального, группового и массового сознания, а также на изменение морально-политического и социально-психологического климата в коллективе и обществе.

В основе методологии ИПП лежат концептуальные положения философии войны (в том числе философии ИП), психологии воз-

[1] Когнитивный — связанный, соотносящийся по значению с существительным когниция или познание. Когниция — это совокупность ментальных процессов, служащих для обработки и трансформации информации. Включает постижение и оценивание собственной персоны в окружающей действительности.

действия, манипуляции общественного сознания, коммуникации. Сегодня англосаксонская цивилизация в рамках ИПП в России выбрала следующие основные мишени — властную вертикаль, Русскую православную церковь, внешнюю и внутреннюю политику руководства страны, русскую историю, ментальность и образ жизни русского народа, русский язык, русское искусство [29; 44].

Уже становится очевидным, что будущее международных отношений, мировой политики и мировой экономики будут определять ИР и информационные услуги, поскольку первенство в развитии информационной сферы существенно скажется в наступившем столетии на расстановке сил на мировой арене. Эти обстоятельства предопределяют, с одной стороны, дальнейшую интенсификацию развития глобальной информационной сферы, а с другой, обостряют конкуренцию за мировое лидерство в этом процессе и делают информационную сферу все более привлекательным объектом противоборства. Отсюда следует, что обеспечение информационной безопасности (ИБз) приобретает все более весомое место в деятельности любого государства, и ИБз становится важнейшей составляющей национальной безопасности.

Руководство США, стремясь к удержанию глобального лидерства, еще в начале 1990-х гг. вплотную приступило к изучению и проработке проблем, связанных с противоборством в информационной сфере, или так называемой ИВ [21; 24]. Символической точкой отсчета революционных преобразований в области использования новых информационных технологий в военной сфере стал тщательный анализ американским военным руководством опыта по достижению информационного превосходства на поле боя, полученного в ходе операции «Буря в пустыне» (1991 г.), которая считается последней «классической» и первой крупной ИВ в современной военной истории США (приложение 1). Одним из фундаментальных выводов, полученных на основе материалов анализа, стало заключение о том, что содержание войны коренным образом изменилось. Та сторона, которая выиграет информационную кампанию, победит. Информация является ключом к современной войне в стратегическом, оперативном, тактическом и техническом отношении. Выводы и предложения, полученные в результате проведенного анализа, легли в основу ряда концепций: «Информационная война» (1992 г.), «Единая перспектива-2010», «Единая перспектива-2020», в которых определены основные направления ИВ (психологические операции, введение противника в заблуждение, противодействие разведке противника, радиоэлектронная борьба (РЭБ) и уничтожение (разрушение) пунктов управления противника и его систем связи), а также в основу концепции, полу-

чившей название сетецентрической войны (в англоязычных источниках — *Network Centric Warfare, NCW*), которая является системой взглядов на военно-техническое обеспечение и ведение военных (боевых) действий в условиях тотальной компьютеризации сил и средств ИБ [20; 24; 35; 36]. На основе утвержденных концепций США интенсивно проводят широкомасштабные исследования в области ИП, продолжают создавать и совершенствовать структуру органов управления, частей и подразделений, ведут подготовку соответствующих специалистов.

В соответствии со взглядами США на войну будущего основной составляющей кардинального повышения боевых возможностей вооруженных сил (ВС) является достижение информационного и технологического превосходства. Это превосходство преобразит современные понятия о маневре, ударах, защите и тыловом обеспечении и приведет к появлению новых оперативных концепций господствующего маневра, высокоточного сражения, целенаправленного обеспечения и всеобъемлющей защиты. Реализация этих концепций позволит Соединенным Штатам достичь «всеохватывающего господства». Доминирующими видами военных действий в новом военном измерении наряду с традиционными станут информационные операции (ИОп), проводимые как самостоятельно, так и совместно с другими видами военных действий на суше, в воздухе, на море и в космосе (приложение 2).

Успех в любой военной операции зависит от способности быстро и точно собрать и обобщить нужную информацию для принятия оптимального решения и воспретить проведение аналогичных действий противником. Однако следует, что ИОп являются не просто отдельным видом наступательных или оборонительных действий. Они также включают сбор и передачу информации командирам на поле боя. Маневр на информационном поле боя будет играть главенствующую роль по отношению к маневру на местности. Информационная защита дополняет традиционные представления о защите физической.

Противоборство в информационной сфере, кроме того, даст импульс к созданию качественно новых средств поражения информационных объектов противника с целью срыва его оперативных замыслов и разрушения его государственной инфраструктуры. Например, посредством ИВз можно нанести чрезвычайно эффективный урон торговым и финансовым операциям, совершаемым по компьютерным сетям.

Самостоятельные элементы ИОп могут включать нанесение скрытых ударов с помощью компьютерных вирусов. За этими ударами могут последовать открытые воздействия на объекты ИР с помощью средств ИП(б).

Самостоятельные ИОп могут использоваться для введения противника в заблуждение относительно состава, местонахождения и намерений своих сил, для временного или постоянного вывода из строя его датчиков и систем обработки информации, а также для нарушения коммуникации информационных сетей с помощью энергетического воздействия.

Наряду с военными специалистами США многие аналитические центры в мире (приложение 3) ведут проработку возможных типовых сценариев ведения ИВ, строя свои стратегии по обеспечению глобального информационного доминирования своих государств, а именно:

1) первый сценарий. Государство (потенциальный инициатор ИВ) располагает подавляющим превосходством в СИВ и способно преодолеть соответствующие оборонительные системы любой другой страны. В этом случае оно может выделить часть имеющихся у него средств ведения ИВ своим союзникам, взяв на себя задачи координации совместных действий, а также идентификацию информационных угроз и их источники. При этом, однако, должна быть обеспечена гарантия того, что само это государство не будет разоблачено в качестве «информационного агрессора»;
2) второй сценарий. В этом сценарии допускается наличие некоторого ограниченного числа государств, обладающих достаточным количеством СИВ для проведения самостоятельных ИОп. Однако все же одно государство (государство-агрессор) сохраняет свое превосходство в указанной области. Это обстоятельство должно сыграть роль фактора устрашения и удержать остальные страны от использования информационного оружия (ИО) против доминирующего государства и обеспечить его «исключительность» и в дальнейшем;
3) третий сценарий. В этом сценарии военными специалистами центров делается акцент на создание в стране информационного доминирования неуязвимой системы защиты от любых СИВ. По их мнению, это вынудит большинство стран мира отказаться от разработки и создания наступательных СИВ, чтобы не спровоцировать информационные атаки против себя, поскольку они не смогут противостоять им, так как не обладают адекватными защитными технологиями. В такой ситуации страна информационного доминирования может навязать другим странам систему принудительного контроля над информационным оружием, подобно тому, как это было сделано США в отношении программ создания оружия массового поражения (ОМП) в Ираке. В результате возможность развязывания ИВ против страны информационного доминирования будет сведена до минимума, а средства ее ведения у потенциальных

противников будут изъяты и уничтожены. Для придания легитимности таким шагам в условиях сформировавшегося абсолютного превосходства одной страны международному сообществу может быть навязано принятие соответствующих международных документов.

Доминирование в информационной сфере реально означает не абстрактную возможность влиять на мировую информационную сферу, а обладание вполне конкретными возможностями, позволяющими диктовать свою волю, т.е. обеспечить глобальное доминирование и в других сферах деятельности.

Президент России В.В. Путин на заседании Совета безопасности, в ходе которого рассматривался проект «Основ государственной политики в области международной безопасности», отметил[1], что доминирование в цифровой сфере является одним из основных стратегических вызовов современности, который может привести к масштабной конфронтации, поскольку:

1) цифровое пространство сегодня содержит много потенциальных угроз для глобальной безопасности, а также для суверенитета и национальных интересов отдельных стран;
2) «новые технологические решения порождают и новые риски: мы видим, что глобальное цифровое пространство нередко становится площадкой для жесткого информационного противоборства, для качественно нечестной конкуренции и кибератак. Все это качественно меняет ситуацию на международной арене»;
3) «цифровую среду используют международные террористы, организованная преступность, здесь много потенциальных угроз для общей глобальной безопасности, но и для отдельных стран, их суверенитета и национальных интересов»;
4) «кардинальную трансформацию проходят традиционные сферы деятельности государства, общества, бизнеса, создаются принципиально новые возможности для экономики и рынка труда, для повышения качества жизни людей».

В настоящее время достаточно широко известна крылатая фраза: «Тот, кто владеет информацией, тот владеет миром». Сегодня в этом посыле проявляется цель и сущность ИП(б).

Следует отметить, что в последние годы в РФ произошли определенные позитивные изменения в решении проблем информационного противоборства, которое в военном деле выливается в ИБ. Так, выступая 22 февраля 2017 г. в Госдуме, министр обороны РФ Сергей Шойгу заявил о создании в составе ВС РФ войск ИОп. А в современ-

[1] 26 марта 2021 года, Московская область, Ново-Огарево.

ных концептуальных и законодательных документах РФ (Стратегии национальной безопасности РФ [50], Военной доктрине РФ [7], Концепции внешней политики РФ [25], Основах государственной политики Российской Федерации в области ядерного сдерживания [40], Федеральном законе о безопасности критической информационной инфраструктуры РФ [55] и др.) определены основные цели, задачи, мероприятия и действия специальных сил и подразделений ИП(б).

Материал книги позволяет выбрать (обосновать) направление эффективного развития как отдельных государственных структур, так и государства в целом, которое в условиях современной международной обстановки при постоянном ИПВ на человека в современном мире обеспечит ИБз государства, общества и личности.

А уважаемый читатель, прочитавший книгу, несколько по-другому будет смотреть на события, происходящие в мире.