УДК 519.816

АКТУАЛЬНОСТЬ ЗАДАЧИ ОЦЕНКИ ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ КОНФЛИКТУЮЩИХ СТОРОН

д.т.н., проф. В.М. Бильчук, Н.А. Александрикова, И.С. Николаева

Рассматривается актуальность задачи информационного противодействия сторон, преследующих конечные противоположные цели.

Весь период после Второй мировой войны обычно характеризуется как история противостояния Востока и Запада. Мир, разделенный на два враждебных лагеря, застыл в ожидании развязки необузданной гонки вооружений, требовавшей неимоверного напряжения всех ресурсов. На последнем отрезке этого периода (70-е – 80-е годы) становилось ясно, что восточному блоку в этом соревновании не устоять. Развал Варшавского договора, объединение Германии, распад СССР – эти события знаменовали собой завершение данного этапа мировой истории.

Стоило ослабнуть глобальной конфронтации, присущей эпохе холодной войны, как многие страны бывшего восточного блока были объяты беспрецедентными по своей жестокости и кровавости локальными конфликтами (Карабах, Абхазия, Чечня, Таджикистан). Югославский кризис полностью дестабилизировал Балканы.

Современные военные конфликты высветили новые черты локальных войн:

– центр тяжести вооруженной борьбы перенесен в воздушно-космическую сферу;

– возросла роль межконтинентальных переброс войск;

– произошла информатизация вооруженной борьбы;

– высокий уровень задействованности стратегического и технического обеспечения.

Операция "Буря в пустыне" продемонстрировала уязвимость перед новым оружием – информационным. Информационное воздействие – эффективный инструмент достижения быстрой и бескровной победы в военном, экономическом и политическом конфликте. Известны примеры "внезапного" заражения программного обеспечения противника "логическими бомбами" и "вирусами".

Завоевание информационно-технического и информационно-психологического превосходства в мирное время и угрожающий период; информационная поддержка и информационное сопровождение военных действий во время и после их окончания – это задачи, входящие в список

стратегических задач достижения успеха в локальной войне [1].

Тенденция сегодняшнего дня такова, что на данном этапе информационная война рассматривается развитыми странами, как наиболее эффективный способ достижения и обеспечения своих целей и интересов во всех жизненно-важных сферах (политической, экономической, социальной, военной и т.д.).

Предварительная классификация информационного оружия показала чрезвычайную опасность и разнохарактерность его видов, так опасность и разнохарактерность его каналов влияния – от средств массовой информации до программирования (зомбирования) поведения людей на подсознательном уровне.

В информационной войне особое внимание уделяется информационным системам, которые используются в военной сфере.

В настоящее время в Вооруженных Силах Украины, в управлении экономикой Украины, используются информационные и информационно-управляющие системы, не имеющие достаточный уровень защиты, так как базовое системное, большое количество прикладного программного и аппаратного обеспечения является импортным (операционные системы, аппаратные платы и т.д.). Информационные и информационно-управляющие системы являются наиболее привлекательными объектами для информационного воздействия противника, он может целенаправленно навязать противоборствующей стороне, для своей выгоды, свои информационные технологии. Поэтому в настоящее время актуальна задача разработки средств и методов информационного противоборства.

Преимущество в информационной борьбе является одним из существенных факторов позитивного результата применения Вооруженных Сил Украины в операциях. Полная автоматизация способов информационной борьбы на базе повышения уровня "интеллектуализации" процессов анализа обстановки и уменьшения времени принятия решения с оценкой текущей ситуации обеспечит в значительной мере преимущество в информационной войне.

Характерной особенностью информационной войны является то, что она может вестись как в военное, так и в мирное время, как на государственном (дипломатические, экономические, информационные, специальные и другие силы и способы), так и на военном уровне (силами и способами борьбы с системами боевого управления).

По установившемуся пониманию, информационное оружие представляет собой совокупность специально организованной информации, информационных технологий, которые позволяют целенаправленно изменять (портить, искажать), копировать, блокировать информацию, вскрывать системы защиты информации, ограничивать допуск законных пользователей, разрушать носители информации, совершать дезинформацию, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей [2].

Переход информации в разряд наиважнейших ресурсов и возникновение стремления владения этим ресурсом, ведет к переосмысливанию методологических основ оценки противостояния сторон с противоположными конечными целями. Информационное преимущество будет основой составляющей стратегии поведения оперирующей стороны.

По нашему мнению решение задачи оценки информационного противодействия сторон, преследующих противоположные конечные цели, связано с постановкой и решением следующего перечня частных задач:

– выявление содержания пакета информации, обеспечивающей выполнение задач управления перспективной группировкой вооружений;

– выявление закона распределения случайной величины объёма принимаемого пакета информации;

– определение минимального (необходимого) объёма принимаемого пакета информации, при котором обеспечивается доведение команд управлением вооружением;

– выявление значимости (важности) отдельных символов пакета информации (в четкой или нечеткой постановке);

– выявление закона распределения случайной величины времени передачи пакета информации;

– разработка показателей достоверности и полноты пакета информации;

– разработка модели и метода оценки информационного противодействия сторон;

– разработка модели противодействия сторон с учетом информационного противодействия и на её основе выработка рекомендаций к составу перспективной группировки вооружений.

Решение этих задач может позволить выявить наиболее целесообразные стратегии информационного образа действий оперирующей стороны в различные временные интервалы противодействия сторон.

ЛИТЕРАТУРА

1. *Костин Н.А. Общие основы теории информационной борьбы // Военная мысль. – 1997. – № 3. – С. 44-50.*
2. *Прокофьев В.Ф. Опасно! Объект атаки психики и сознания человека. mvd-expo.ru Untitled Document.*

Поступила 16.07.2002

***БИЛЬЧУК Виктор Михайлович**, доктор техн. наук, профессор, заведующий кафедрой ХВУ. В 1956 г. окончил ХВАИВУ, в 1967 г. – ХГУ. Область научных интересов – системный анализ эффективности функционирования сложных систем и операций.*

***АЛЕКСАНДРИКОВА Наталья Анатольевна**, инженер-программист ХВУ. В 1978 году окончила ХИРЭ. Область научных интересов – системный анализ эффективности функционирования сложных систем и операций.*

***НИКОЛАЕВА Ирина Сергеевна**, магистр-экономист. В 2000 г. окончила ХАОП. Область научных интересов – экономико-математическое моделирование.*