К ВОПРОСУ РАЗРАБОТКИ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ ВОЙНЫ

Актаева А.У., Илипбаева Л.Б.

Аннотация **- Статья посвящена теории математической модели информационной войны. В статье собраны и проанализированы представленные и доступные для исследователей материалы по теории информационной войны, а также проблемы информатизации общества. Основное внимание уделено вопросам классификации модели «кибервойны» и обеспечению информационной безопасности и защиты.**

Ключевые слова **- Информатизация, математическое моделирование, информационная война, ИКТ, киберпространства, информационная безопасность и защита, глобальная информационная сеть**

I.Введение

В XXI веке современный этап развития общества характеризуется высокой степенью его информатизации и возрастающей ролью ИКТ, которые активно влияют на состояние политической, экономической, оборонной и других составляющих безопасности государства и их граждан. Для разрешения различных социальных и межгосударственных конфликтов все чаще используется информационная сфера, что порождает такое явление как «Информационная война», характеризующееся, с одной стороны, воздействием на информационную сферу противника, а с другой – принятием ряда мер по выявлению и защите своих элементов информационной инфраструктуры от деструктивного и управляющего воздействия. Применяемые при этом средства имеют своей целью, как правило, не только непосредственное физическое уничтожение противника, а управление информационным пространством его деятельности в целях изменения его в нужном направлении [1].

II.Основная часть

Предметом теории информационной войны являются модели, создаваемые информационными субъектами и служащие для управления этими субъектами (см. рис 1).

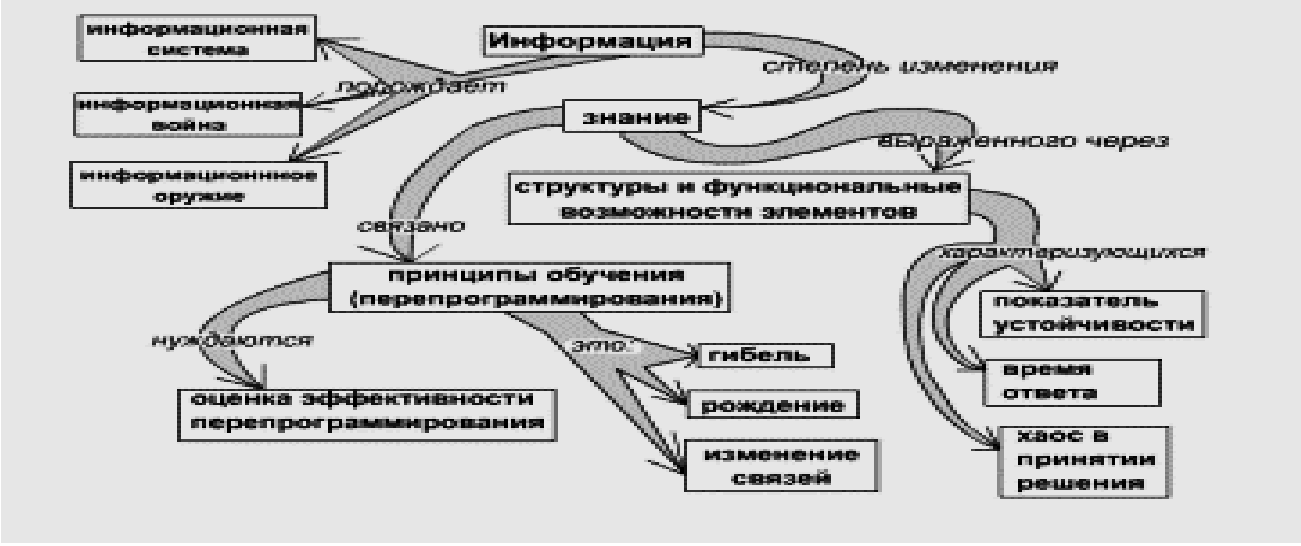

Рис.1- Классическая структура информационной войны [2]

А формальная теория информационной войны изучает возникновение, существование и гибель информационных систем как результат совокупного действия множества информационных систем по программированию и перепрограммированию путем передачи информации, понимаемой как степень изменения знания субъекта [2,4].

По данным доклада Национального совета по разведке США «Глобальные тенденции до 2015 года», что информационные войны будут доминировать и в XXI веке. Определить, кто с тобой воюет,

Актаева А.У.,доцент,dr PhD, КазНУ им. Аль –Фараби г.Алматы, aakhtaewa@bk.ru
Илипбаева Л.Б., АУЭС, доцент, к.т.н., г.Алматы, ilizat1011@mail.ru

архисложная задача, когда их могут вести и отдельные лица, группы людей, страны. Например, для проверки защищенности своих компьютеров Пентагон набирал и собрал команду из хакеров со всего мира и «развязал им руки». Результат их работы показал, что они взломали защиту у 88% из 8900 компьютеров военного ведомства «Пентагон» и только 4% атак были замечены. Оказалось, что компьютеры военного ведомства «Пентагон» способны без ведома их владельцев собирать и передавать информацию о содержании созданных баз данных, включая зарегистрированных пользователей по каналам Интернет их разработчикам [3].

Анализ существующего метода информационной войны показал, что информационная война развивается по следующим основным направлениям (см.рис.2), в рамках которых оно и применяется в военной разведке: проведение и планирование специальных информационных операций, и управление процессов их проведения и оценка результативности.

Рис. 2- Классификация информационного оружия информационной войны [3]

Условно можно выделить четыре общих класса математических моделей информационной войны (см.рис.3):
– описательные модели;
– имитационные модели;
– оптимизационные модели;
– модели принятия решений [4].

III. Обсуждение

Описание математическим аппаратом различных компонент информационной войны и его изучение уже входит в сферу интересов многих ученых. В этом направлении следует отметить, что использование математической теории передачи информации по классическим каналам связи для построения модели и оценок эффективности конкретных информационных воздействий. При помощи теории графов и игр составлены модели информационных сетей и войн, а для противоборствующих сторон найдены смешанные стратегии. Стратегии, в основном, рассчитаны на выведение из строя информационных инфраструктур противоборствующих сторон или их защиту посредством как физического, так и программного (вирусы, трояны, шпионские программы, кибератаки и др.) воздействия [3].

В последнее время становится актуальной разработка математических моделей информационной войны, т.е. информационных технологий, базирующихся на промышленном производстве, распространении и навязывании информации. Например, каждые 20 секунд в США имеет место преступление с использованием программных средств, в 80% преступлений атаки идут через Интернет. По данным Института компьютерной безопасности США компьютерная преступность растет темпом 16% в год [2,4].

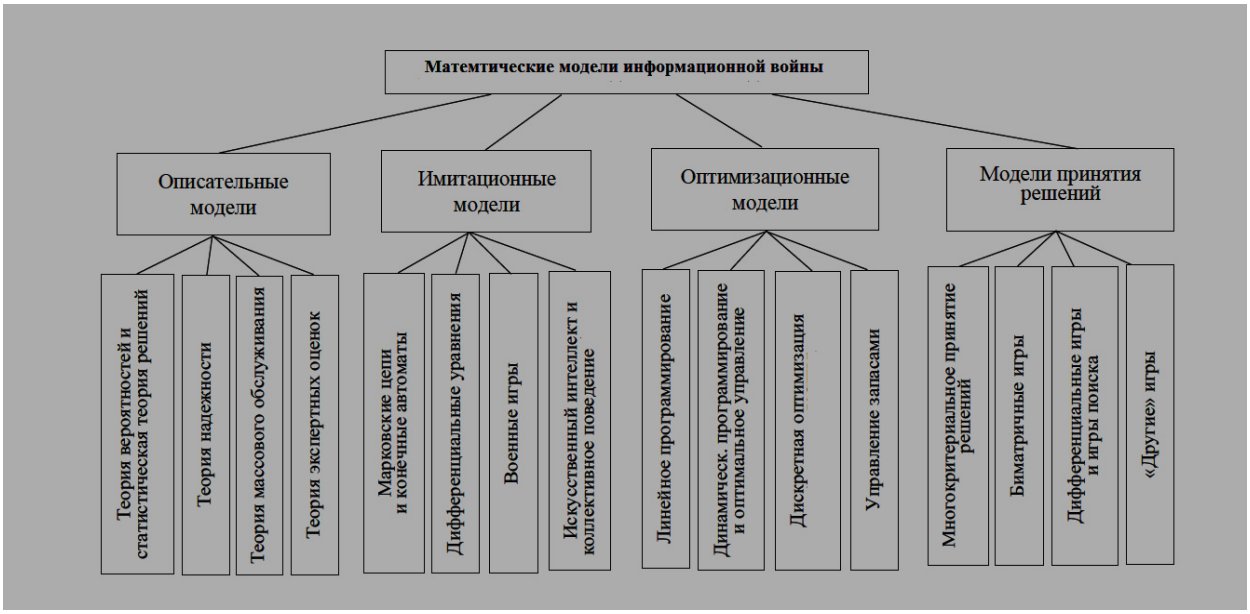

Рис. 3- Классификация математических моделей информационной войны

Любая информационная операция всегда направлена на изменение картины мира противника, на его перепрограммирование и это, в свою очередь, предполагает корректировку знания противника. Например, в октябре 2010 года была создано киберкомандование, 2-я армия США. Это ведомство объединило в себе подразделения киберзащиты Пентагона и вошло в состав АНБ (число сотрудников более 21 тыс. человек). По замыслу, киберкомандование «планирует, координирует, интегрирует, синхронизирует и управляет сетевыми операциями и защитой сетей» и будет работать в киберпространстве и будет обеспечивать в сети GIG (Global Information Grid) свободу действий силам США и союзников и лишать такой возможности противника [7].

Согласно анализу российских экспертов любое государство, располагающие АИСУ, вскоре окажутся беззащитными перед противоборствующими сторонами, если не будут располагать высокопрофессиональными специалистами и службами по информационной безопасности и защиты. Вместе с тем, «сплошная компьютеризация и информатизация», в том числе, и стратегических объектов породила новую проблему — они стали более «прозрачными» для противоборствующих сторон. Мы считаем, что корректировать знание, которое воплощается в структуре информационной системы и функциональных возможностях элементов структуры ИС, означает корректировать саму структуру, т.е.:

– принцип рождения;
– принцип гибели;
– принцип изменения связей [3,4].

IV.Заключение

Это значит, необходимо пересмотреть и корректировать методику преподавания учебных курсов в области ИКТ с учетом современной ситуацией в области информатизацией и компьютеризацией общества. Необходимо ввести инновационные курсы дисциплин, как «Теория информационной войны», «Основы кибервойн» будущим специалистам в области ИКТ, учитывая, что «Кто владеет информацией, тот и владеет миром». На основе изучения целей информационной войны существенное внимание уделять фундаментальным аспектам информационной войны таким, как математический характер законов информатики и ведения войн, принцип теории передачи информации. Также в курсе лекций «Теория информационной войны и Основы кибервойн» необходимо ответить на следующие вопросы как, теория передачи информации (методы, модели и технологии), связанные с инновационными технологиями современного мира. Также необходимо включать в план лекций курса методы ведения информационной войны, основанные на теории математического моделирования и их практические применения. На основе изучения целей информационной войны спроектировать лабораторные работы на стендах с помощью ИКТ по процедуре анализа и алгоритма определения стратегий информационного противоборства (в том числе провокаций, дезинформации, безопасности и др.). Обучить будущих специалистов по разработке процедуры планирования информационных операций (атак и вторжений, защита), алгоритма принятия решений в информационной войне и подходов к управлению информационным противоборством. Все эти рассматриваемые разделы курса должны быть использованы для анализа и проектирования комплексных систем управления противоборством в информационной войне разной природы и масштаба — от корпоративных и отраслевых до региональных и национальных, а также исследованы в условиях Глобализации и Интернетизации. Следует включить,

в программу курса изучения дисциплины тенденции интенсификации процессов передачи информации, этапы развития глобального информационного общества массовой коммуникации. А в практических занятиях должны приведены конкретные примеры ведения информационного противоборства в современном мире.

А также необходимо провести серьезные исследования, позволяющие научно обосновать основные принципы методики проведения информационной войны. В силу объективных и субъективных причин значительная часть НИИ постсоветского пространства уже не располагает конкурентоспособными коллективами, способными на высоком научно-техническом уровне выполнить необходимые исследования и конкурировать с Западными НИИ, но тем не менее, необходимо формирование коллектива специалистов среднего поколения и высококвалифицированных специалистов из нынешнего поколения молодежи. И способствовать финансированию НИР и НИРС, связанных с теорией информационной войны и компьютерными науками для формирования научных основ.

Библиография

[1] Информационные войны http://infwar.ru
[2] Расторгуев С.П. Информационная война. Проблемы и модели. - М.:Гелиос АРВ, 2006
[3] Маревцева Н.А. Простейшие математические модели информационного противоборства. Математическое моделирование социальных процессов.- М.:МАКС Пресс, 2010
[4] Расторгуев С.П. Математические модели в информационном противоборстве. Экзистенциальная математика.- М.: 2014
[5] Михайлов А.П., Клюсов Н.В. О свойствах простейшей математической модели распространения информационной угрозы. Математическое моделирование социальных процессов.- М.: МАКС Пресс, 2002, с.115-123.
[6] Гриняев С. Взгляды военных экспертов США на ведение информационного противоборства. // Зарубежное военное обозрение. № 8, 2001
[7] Шнепс-Шнеппе М.А., Намиот Д.Е, Цикунов Ю.В. Телекоммуникации для военных нужд: сеть GIG-3 по требованиям кибервойны//International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 10. – С. 3-13.
[8] Р. Броуди. Психические вирусы. Как программируют ваше сознание.- М.:Поколение. 2006, 304 с.
[9] Прокофьев В.Ф. Тайное оружие информационной войны. 2 изд.- М.: СИНТЕГ, 2003
[10] Расторгуев С.П. Теория информационной войны. - М.: 2002
[11] Расторгуев С.П. Информационная война. — М.: Радио и связь, 1999
[12] Почепцов Г.Г. Информационные войны. Основы военно-коммуникативных исследований. - М.: Рефл-бук, 2000
[13] Этьен Кассе Третья мировая психотронная война. Санкг-Пб.:Изд.Вектор, 2007
[14] Гриняев С.Н. Информационная война: история, день сегодняшний и перспектива. – СПб.: Арлит, 2000
[15] Бухарин С.Н. Методы и технологии информационных войн.- М.: Академический проспект, 2007. - 384 с.
[16] Панарин И.Н. СМИ, пропаганда и информационные войн.- М.: Поколение, 2012, 411 с.
[17] Jason Andress, Steve Winterfeld Cyber Warfare Techniques, Tactics and Tools for Security Practitioners.- www.elsevier.org
[18] Петухов А.Ю. Моделирование социальных и политических процессов в условиях информационных войн.- http://cyberleninka.ru
[19] Чхартишвили А.Г. Модели информационного влияния и информационного управления в социальных сетях //Проблемы управления,2009, № 5.

CONTEXT DEVELOP A MATHEMATICAL MODELING OF INFORMATION WARFARE

Aktayeva A.U., Ilipbayeva L.B.

Abstract **- This article is devoted to the theory of a mathematical model of information warfare. The paper collected and analyzed the presented available materials for researchers on the theory of information warfare, as well as problems of information society. Main attention is paid to the classification model the so-called "cyber-warfare", information security and protection.**

Keywords **- Informatization, mathematical modeling, information warfare, ICT, cyberspace, information security and protection, global information network**