СОЦИОЛОГИЯ ИНТЕРНЕТА: ФОРМАЛИЗАЦИЯ МОДЕЛЕЙ ИНФОРМАЦИОННОЙ ВОЙНЫ

А.У. Актаева
Доцент кафедры «Вычислительная техника и информационные системы»

Н.Г. Галиева
Исследователь кафедры «Вычислительная техника и информационные системы»

Г.Б. Байман
Исследователь кафедры «Вычислительная техника и информационные системы»

Казахская академия транспорта и коммуникаций им. М.Тынышпаева, Республика Казахстан

Abstract. This article is devoted to the theory of a formalization 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 the information society. Main attention is paid to the classification model the so-called "cyber -warfare", exams information security and protection. The emphasis is on the classical structure and classification of the information war, so the axioms proposed management information objects of information in social networks.

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, информационное противостояние, дезинформация, информационные конфликты» 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. Все большее число игроков, необходимых для решения транснациональных проблем, их противоречивые интересы – вот что усложнит процесс принятия решений [1, 2].

Повсеместное использование новых коммуникационных технологий стало для власти «палкой о двух концах». С одной стороны, социальные сети позволять гражданам объединяться и формировать вызовы власти. С другой стороны, такие технологии позволять правительствам, беспрецедентную возможность наблюдать за своими гражданами. Неясно, каким образом будет достигнуто равновесие между влиятельными представителями IT-индустрии, социальных сетей, и традиционными политическими структурами (рис. 1) [2].

Рис. 1. Классическая структура информационной войны [3]

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 [2].

Информационные технологии, позволяющие мгновенно реагировать на любые вызовы, организовывать массы вне географических границ, повышают возможность любого вмешательства в развитие глобальных событий. Доступные информационные технологии ввода больших данных, мощность процессов и большой объем хранения информации упрощают глобальное распространение киберуслуг и социальных медиа. По данным доклада Национального совета по разведке США «Глобальные тенденции до 2030 года», что информационные войны будут доминировать и в XXI веке. Определить, кто с тобой воюет, архисложная задача, когда их могут вести и отдельные лица, группы людей, страны. Это потребует не только расширения рынков информации, но и повышения уровня безопасности глобальных сетей, что в свою очередь поставит весьма серьезные задачи для государственных институтов и гражданского общества. *Кибер-оружие* может принимать различные формы (вирусы, черви трояны, атаки по типу «отказ в обслуживании», фишинг и т.др.). Сценарии кибер-войны включают скоординированные атаки, которые саботируют работу многочисленных инфраструктур одновременно. Угрозы безопасности становятся нарастающей проблемой: расширяются возможности доступа к смертоносным и разрушительным технологиям, что позволяет отдельным лицам и небольшим группам осуществлять акты насилия и диверсий в крупных масштабах [2, 3 ,5].

К 2030 году технологические направления, такие как технологии, в области хранения и обработки больших массивов данных, технологии социальных сетей, технологии «умные города» изменят наш образ жизни, порядок ведения дел и безопасность (таблица 1).

Таблица 1. Глобальные тенденции развития информационных технологии [6]

Направление	**Текущее состояние**	**Возможности к 2030 г.**	**Проблемы**	**Эффекты**
Технологии обработки данных	Применение масштабного сбора и анализа данных	Инновационные разработки в области программного и аппаратного обеспечения новые решения: сбор, анализ BIG DATA	Скорость обработки и эффективно безопасное използование технологии BIG DATA . Возражение клиентов против сбора персональных сведений	+ /- Сбор персональных сведений о клиентах частных компаний и государственных структур
Социальные сети	Безграничные возможности коммуникации между USER	Инновационные способы коммуникации и их применение пользователями	Внедрение успешных бизнес-моделей для поддержки роста провайдеров. Выбор между конфиденциальностью и функциональностью пользователями.	+ / - Стирание геополитических границ между пользователями
Технологии «умных городов»	IT-компоненты «умного города» сегодня слабо внедрены и не очень эффективны	Оснащение интегрированной IT-инфраструктурой, обеспечивающей бесчисленное множество услуг города	Масштаб, сложность и высокие издержки внедрения системы могут оказаться чрезмерными для большинства городов.	+Повышение качества жизни, усиления деловой активности и снижения уровня потребления ресурсов.

Поскольку технологии социальных сетей становятся сутью виртуального существования, они могут стать важным инструментом обеспечения корпораций и правительств ценной информацией об отдельных людях и группах, позволяя разрабатывать надежные модели прогнозирования поведения информационного объекта в информационном пространстве, спектр применения которых может варьироваться от адресной рекламы до противодействия терроризму. Социальные сети способны вытеснять функции, обеспечиваемые в настоящее время корпорациями и государственными структурами, заменяя их новыми категориями услуг, которые невосприимчивы к централизованному контролю и управления.

Технологии обработки данных включают ряд новых решений, позволяющих собирать, хранить и извлекать информацию из «BIG DATA», то есть из таких, чрезвычайно обширных, массивов данных, которыми трудно управлять с помощью обычных инструментов. Новые решения в области хранения и обработки данных помогут пользователям решать сложные экономические и управленческие проблемы, повысят доступность и удобства в использовании знаний, а также значительно увеличат точность прогнозных

моделей и передовые разработки в операциях с данными могут стать каналом информационной перегрузки и инструментом репрессий, настоящим бременем, которое потребует больших ресурсов на обслуживание. Однако эти разработки нужны для общей инфраструктуры, а также как поле многополярных информационных войн.

Стратегии информационной войны заключается в выборе такой последовательности, которая дешевле реализуется и позволяет максимально быстро «загнать» противника в требуемое состояние. В данной работе рассматриваться технические и гуманитарные информационные объекты на более высоком уровне абстракции, т.е. на уровне информационного пространства, способных к обучению или программированию и перепрограммированию.

Управляемость информационного объекта приводит к поиску соответствующих алгоритмов целенаправленного воздействия (перепрограммирования – формализм машины Тьюринга). Существует три типа управляемости информационного объекта: тотальная, частичная и скрытная (рис 2).

Рис. 2. Типы управляемости информационного объекта

Поведение *тотально управляемого* информационного объекта полностью прогнозируемое на интервале времени $[t_0,t_1]$, если известен алгоритм информационного воздействия, позволяющий привести объект в любой момент времени $t \in [t_0,t_1]$ к требуемому от него результату x.

Информационный объект *частично управляемый,* а поведение его *частично прогнозируемым*, на интервале времени $[t_0,t_1]$, если известен алгоритм информационного воздействия, позволяющий привести объект *в некоторый момент* времени $t \in [t_0,t_1]$ к требуемому от него результату x.

Скрытное управление информационным объектом, в гуманитарной сфере, предполагает сокрытие управляющего алгоритма в потоке событий, а в технической – сокрытие управляющего алгоритма в последовательности исполняемых команд и активизируемых программ.

Тогда *точность управления прогнозирования* поведения информационного объекта эта величина временного интервала между планируемым временем получения требуемого от объекта результата и действительным. Осуществление

управления информационным объектом – это применение информационного оружия.

Управление информационным объектом опирается на контроль за ним. Существует два типа контроля информационного объекта: полный и частичный (рис. 3).

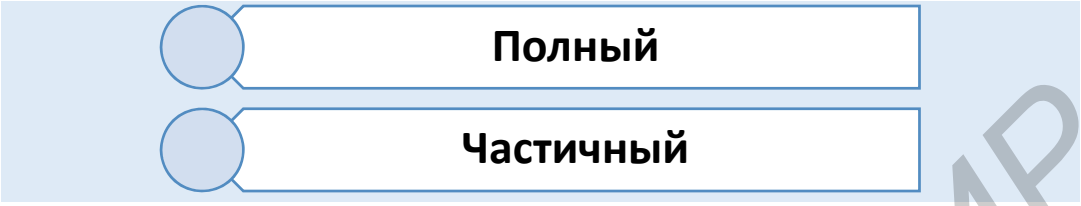

Рис. 3. Типа контроля информационного объекта

Информационный объект полностью контролируемый на интервале времени $[t_0,t_1]$, если известен алгоритм, позволяющий на основании анализа текущего состояния информационного объекта в момент времени t_1 определить доминирующее информационное воздействие, направленное на него в любой момент времени $t \in [t_0,t_1]$.

Информационный объект частично контролируемый на интервале времени [t0,t1], если известен алгоритм, позволяющий на основании анализа текущего состояния объекта в момент времени t1, определить отдельные информационные воздействия на интервале времени $[t_0,t_1]$ к требуемому от него результату x.

Информационный объект частично управляемый, а поведение его частично прогнозируемый, на интервале времени $[t_0,t_1]$, если известен алгоритм информационного воздействия, позволяющий привести объект в некоторый момент времени $t \in [t_0,t_1]]$ к требуемому от него результату x.

В зависимости от роли моделей информационного объекта в информационном пространстве (социальные сети, Интернет) их можно классифицировать на: невидимые, тривиальные и опасные.

Невидимая модель – модель информационного объекта , у которой в отличие от остальных моделей данного информационного пространства не выработано никакого отношения (+-).

Тривиальная модель – модель информационного объекта, которая фактом своего включения в информационное пространство не активизирует в данном пространстве выполнение операций исключения из пространстве ранее существовавших моделей или включения ранее отсутствующих моделей пространства.

Опасная модель – модель информационного объекта, которая, будучи осознанной информационным пространством, приведет к частичному или полному уничтожению этого пространства.

Изложенные выше основы позволяют сформулировать основные аксиомы, решением задач в рамках которых и занимается формальная теория информационных войн:

Первая аксиома – проблема выявления факта начала информационной войны, которая, как известно, в общем виде является алгоритмически неразрешимой. Пути исследования данной проблемы лежат в направлении выявления характеристик события, связанного с фактом появления опасных моделей в информационном пространстве.

Вторая аксиома – проблема разработки типовой побеждающей стратегии ведения информационной войны, которая в общем виде является алгоритмически неразрешимой.

Третья аксиома – проблема «невидимости»:

– можно ли для каждой модели информационного объекта предложить такую стратегию обучения (программирования), которая переведет абсолютно невидимый для него факт в разряд тривиальных или опасных;

– можно ли по каждому тривиальному или опасному факту (модели), известному в информационном пространстве, предложить такую стратегию обучения (программирования), которая сделает этот факт (модели информационного объекта) невидимым;

– при каких исходных условиях существует такая стратегия обучения (программирования), в ходе которой поступившее на вход информационного пространства информация (факт осознания модели) уничтожит всю ранее существовавшую информацию (модели информационного объекта) и/или правила ее обработки.

Четвертая аксиома – проблема разработки стратегии поведения информационного объекта, позволяющего избегать появления в его информационном пространстве наиболее опасных моделей. Данная проблема только лишь на первый взгляд перекликается с проблемой выявления опасных моделей информационного объекта. Суть здесь в выборе таких решений для информационного пространства, применение которых позволяет заблокировать или уничтожать опасные модели информационного объекта.

Пятая аксиома – проблема наблюдения и управления информационного объекта, способного к обучению, в частности, теоретическая и практическая оценка качества наблюдения и управления информационным пространством отношений моделей информационного объекта.

Вышеперечисленые аксиомы не полностью отражают формальную теорию информационной войны. Но решение выделенного класса задач, используя математическое моделирование и образует целостную теорию информационной войны.

По данным Института компьютерной безопасности США компьютерная преступность растет темпом 16% в год. Каждые 20 секунд в США имеет место преступление с использованием программных средств, в 80% преступлений атаки идут через Интернет [2,4].

В последнее время становится актуальной разработка математических моделей и информационные технологии информационных войн и противостояний, а также распространение и навязывание информации,

производителями которых являются крупные мировые IT – компании, поддерживаемые спецслужбами на государственном уровне.

Литература

[1]. Информационные войны - http://infwar.ru

[2]. Development of a mathematical model of information warfare .- International Journal of Open Information Technologies.- vol. 2, №11, 2014, 28-33 pp., ISSN 2307-8162, www.injoit.org http://elibrary.ru/ https://doaj.org/toc/2307-8162

[3]. Расторгуев С.П. Информационная война.Проблемы и модели. - М.:Гелиос АРВ, 2006

[4]. Маревцева Н.А. Простейшие математические модели информационного противоборства. Математическое моделирование социальных процессов.- М.:МАКС Пресс, 2010

[5]. Расторгуев С.П. Математические модели в информационном противоборстве. Экзистенциальная математика.-М.:2014

[6]. Global Trends 2030: Alternative Worlds – пятый выпуск докладов Национального Совета по разведке - www.nkibrics.ru