# Алгебра информационного противоборства

Расторгуев С.П.

*Среди многих факторов благополучного существования и просто существования любого общества, народа, любой цивилизации есть один из главенствующих — это поколение, которое придёт на смену поколению уходящему и останется носителем тех же базовых ценностей, которые были присущи отцам и дедам.*

*Издревне задачу по программированию, т.е. воспитанию себе подобных решала школа — семейная, дворовая, уличная, средняя, высшая и любая другая, способная дать человеку те знания, которые в дальнейшем определяли его жизненный путь и защищали от какой-то части самых примитивных ошибок типа "не суй пальцы в розетку".*

*Сегодня в список перечисленных школ добавились школа телевидения и школа самообуча на базе ПЭВМ. При этом эффективность перепрограммирования учеников в этих школах значительно превосходит возможности обучать и воспитывать нашего привычного и пока ещё живого учителя обычной средней школы.*

*Что такое хорошо, а что такое плохо телевизор объясняет быстрее и проще. Но эти "быстрее и проще" не значат правильнее. Ибо понятно, что "хорошо" владельцу телеканала, не всегда обернется благом для отдельно взятого послушного зрителя.*

*В борьбе за пульт системы программирования и перепрограммирования нашего будущего тактическое преимущество всегда у владельца более современных информационных технологий по обучению. По обучению "за кого голосовать", "что первично, а что вторично", "всему остальному", в том числе естественнонаучным дисциплинам. Понятно, что "всему остальному" приоритеты будут выданы в зависимости от того, кто и как нас с вами учит и чему научит по первым двум позициям.*

*Программист, стоящий за пультом программатора, может быть бездарен, и тогда мы будем совершать ошибку за ошибкой. Он может быть больным или мечтающим нас грабить, и тогда мы получим вместо полезных знаний отравленную информационную пилюлю, ибо знания способны не только спасать, но и убивать.*

*Эта статья о том, что такое информационные войны, о том, как убивают знаниями, ибо если враг научил свою жертву, что из пункта "А" надо следовать в пункт "В", то ему уже больше не надо никого контролировать. Когда же потребуется очередная порция дани, "В" вдруг, как бы по велению волшебной палочки, превратится в информационную бойню, на которую жертва сама же и пожалует.*

*Сегодня, чтобы познать народ или отдельно взятого человека, а затем управлять ими, проще и дешевле не изучать их, а интенсивно формировать требуемую модель мира, не ждать, пока субъект самостоятельно до чего-то дозреет (потом поди попробуй пойми, до чего он дозрел), а как можно быстрее вложить в него требуемые знания, которые изначально известны агрессору. И это главный принцип современных информационных войн.*

## Программа специализированного курса

### *Вводная часть*

*Исходные теоретико-методические предпосылки*

Рыночные отношения и конкуренция как способы социального взаимодействия неизбежно приводят современное общество к массовому использованию психологических манипуляций в политике, экономике, повседневной жизни людей.

Система методов, средств и приёмов манипулятивного воздействия, доведённая до идеологии и технологии межличностного взаимодействия в США и в значительной мере в Европе, активно и широкомасштабно внедряется в социальную практику российского общества.

Включённость в информационно-коммуникативные процессы манипулятивных технологий многократно увеличивает эффект воздействия и, таким образом, трансформирует их в основной фактор угрозы информационно-психологической безопасности социальных

субъектов различного уровня общности — от личности до населения страны в целом.

Умения выявлять акты манипулятивного воздействия и формировать защитные механизмы у человека в настоящее время — актуальная задача психологической науки и необходимый элемент профессиональной деятельности практических психологов, педагогов, государственных служащих, руководителей разных уровней управления и людей, участвующих в информационно-коммуникативных процессах современного общества.

Спецкурс представляет собой ряд циклов занятий, объединённых общей проблематикой и структурой. Логика и методика процесса обучения построены по модульному типу (включают как теоретические, так и прикладные или технологические модули).

Внутреннее единство спецкурса обеспечивается взаимосвязью содержания рассматриваемых тем и форм проведения занятий (лекций, семинаров, практических занятий, тренинговых и диагностических процедур, индивидуальной работы под руководством преподавателя и самостоятельной работы обучаемых).

В РАМКАХ СПЕЦКУРСА МОЖНО ВЫДЕЛИТЬ ТРИ ОСНОВНЫХ ЭТАПА:

***I этап***

На первом этапе осуществляется диагностика возможностей психологической самозащиты и формирование установки на обучение.

Используются: психологическое тестирование; интервьюирование; наблюдение; имитационно-ролевая игра. Основное отличие этой имитационно-ролевой игры от аналогичных игр второго этапа заключается в том, что с её помощью решаются задачи демонстрации и диагностики уровня психологической самозащиты обучаемых.

***II этап***

Теоретическое обучение: лекции, которые содержат необходимые сведения для формирования психологической самозащиты личности и семинары, закрепляющие получаемые знания.

Различные формы практических и тренинговых занятий, самостоятельной работы: анализ и моделирование конкретных ситуаций; анализ и разбор видеозаписей; самостоятельный анализ текстов и ТВ-программ; групповой тренинг в форме имитационно-ролевых игр (“Переговоры”, групповая дискуссия, “Пресс-конференция” и т.д., в том числе различные видоизменения “Палермо” — “Мафия”, в частности, “Деловой круиз”, с последующим анализом их видеозаписей); парный тренинг определения неискренности и скрытого получения информации (на первом этапе один “выведывает”, другой должен отрефлексировать скрываемые цели партнёра, затем смена; на втором этапе используется более сложная форма — встречное “выведывание” На обоих этапах производится групповой анализ их видеозаписей); самоотчёты (формирование умения отрефлексировать ситуации, собственное поведение, чувства и поведение участников); анализ обучаемыми проведения имитационно-ролевых игр, в том числе их видеозаписей (формирование умения отрефлексировать ситуацию, чувства и поведение участников).

***III этап***

На третьем этапе проводится: итоговая игра с разбором и оценками экспертов; подготовка курсовых и дипломных работ, рефератов; интервьюирование (после окончания курса обучения).

Результаты обучения в соответствии с программой спецкурса, проводимых по такой методике, показывают, что их участники приобретают своеобразный “социально-психологический иммунитет” к манипулятивному воздействию. У них повышается самоконтроль собственных эмоциональных состояний в процессе общения и коммуникативного воздействия (в том числе с использованием средств массовой коммуникации), формируется установка на критический содержательный анализ поступающей вербальной информации и используемых невербальных средств.

Приобретённый в процессе занятий коммуникативный опыт и знание наиболее характерных приёмов и уловок, используемых для оказания манипулятивного воздействия на людей, а также самостоятельная тренировка по специальной программе и соответствующей методике позволяют приобрести первичные навыки и умения по их выявлению и способствуют снижению степени подверженности личности психологическим манипуляциям.

Кроме этого, у обучаемых вырабатываются навыки логико-психологического и рефлексивного анализа, развивается индивидуальный стиль психологической самозащиты. Это способствует эффективной работе личности по самосовершенствованию психологической безопасности.

*Требования к уровню начальной подготовки. Направления формирования основного понятийного аппарата*

Предполагается, что слушатели владеют основами понятийного аппарата логики, политологии, психологии личности и социальной психологии (если не владеют, то эти вопросы включаются в соответствующие темы либо согласуются с программами других изучаемых дисциплин). В частности следующими понятиями: структура личности и её основные компоненты, субъективные отношения личности (субъективно-личностные отношения), ориентировочная основа действий, общение (структура, виды, функции), коммуникация (виды и функции), массовые информационные процессы (в том числе стихийные), средства массовой коммуникации (классификация, основные функции), психологическое воздействие, внушение, убеждение и т.д.

В процессе изучения этого спецкурса в понятийный аппарат слушателей интегрируются следующие основные понятия: информационно-психологическая безопасность личности, манипулятивное воздействие, психологические манипуляции, тайное принуждение личности и скрытое психологическое принуждение, манипулятивные технологии (в том числе техники и приёмы), психологическая защита (в том числе внутриличностная и межличностная), социально-психологическая защита, индивидуальная социально-психологическая защита, коммуникативные (информационно-коммуникативные) ситуации и их классификация, приёмы манипулятивного воздействия и т.д.

## *Часть 1. Введение в информационно-психологическую безопасность*

*Тема 1. Информационная среда общества как общий источник угроз информационно-психологической безопасности личности*

Понятие, сущность и характеристика информационной среды, основные подходы к её определению, взаимосвязь понятий информационной сферы и информационной среды.

Сущность информационного контакта личности и общества, диалепктика их информационной взаимосвязи. Понятие и характеристика основных групп коммуникативных ситуаций.

Средства массовой коммуникации, их общая характеристика и основные функции. Манипулятивные возможности масс-медиа.

Характеристика факторов, влияющих на действенность манипулятивного воздействия.

Оснвные факторы деформации информационной среды (субъективная и “иллюзорная” реальности), сущность информационно-психологических опасностей.

*Тема 2. Информационно-психологическая безопасность личности*

Понятие, сущность и характеристика информационно-психологического воздействия.

Понятие, сущность и характеристика информационно-психологической безопасности личности и других социальных субъектов, их взаимосвязь.

Междисциплинарный характер проблемы информационно-психологической безопасности личности, предпосылки актуализации проблемы.

Угрозы информационно-психологической безопасности личности и их основные источники.

*Тема 3. Психологические манипуляции как тайное принуждение личности и способ социального управления*

Понятие, сущность и характеристика информационно-психологического и манипулятивного воздействия психологических манипуляций. Социально-экономические и политические факторы, определяющие массовое распространение психологических манипуляций (исторический и современный аспекты).

Общественные изменения как источник повышения психической напряжённости.

Психологические манипуляции как элемент коммуникативных процессов современного общества.

Массовое использование психологических манипуляций как результат эволюции социального управления в условиях кардинальных общественных изменений.

Значение контроля за информационными потоками для социального уравления.

Социально-психологические особенности политической ситуации в российском обществе.

Массовое распространение психологии манипуляций как ведущая угроза информационно-психологической безопасности личности в экстремальных условиях развития российского общества. Психологические предпосылки усиления подверженности личности манипулятивному воздействию. Факторы повышения опасности психологических манипуляций.

## *Часть II. Сущность, организация, способы и технологии тайного принуждения личности*

Тема 4. Тайное принуждение личности как
социально-психологическое явление

Особенности анализа тайного принуждения личности.

Культурно-историческая эволюция тайного принуждения личности. Использование тайного принуждения личности в различных культурно-исторических условиях. Особенности использования тайного принуждения личности в различных сферах социального взаимодействия.

Эволюция представлений о тайном принуждении личности. Общая характеристика понятийного отображения проявлений тайного принуждения личности. Анализ, систематизация и уточнение основных понятий, отображающих проявления тайного принуждения личности.

Определение понятия “манипуляция” как научного отображения сущности тайного принуждения личности. Общая характеристика научного понятийного аппарата, отражающего проявления тайного принуждения личности. Средства описания процесса межличностных манипуляций. Анализ и обобщение подходов к определению понятия “манипуляция”. Уточнение содержания понятия “манипуляция” как научного отображения сущности тайного принуждения личности.

*Тема 5. Комплексные организационные технологии тайного принуждения личности*

Психологические операции как комплексные организационные технологии тайного принуждения личности. Активизация и основные сферы использования комплексных организационных технологий тайного принуждения личности. Сущнсть, содержание и общая характеристика психологических операций, используемых во внешнеполитической сфере и в военном противоборстве. Общие правила и требования к проведению информационно-пропагандистских акций в процессе осуществления психологических операций. Характеристика основных компонентов психологических операций, используемых во внешнеполитической сфере и военном противоборстве.

“Crisis management” и технологии тайного принуждения личности. Сущность и общая характеристика “Crisis management” и “кризисных” технологий. Иллюстрация кризисных технологий с использованием ситуационного моделирования. Основные составные компоненты crisis management'a и их общая характеристика.

Информационно-психологические операции как основные комплексные организационные технологии тайного принуждения личности в современных условиях в сфере внутриполитических отношений. Общая характеристика информационно-психологических операций, используемых в сфере внутриполитических отношений. Характеристика основных компонентов информационно-психологических операций, используемых в сфере внутриполитических отношений. Характеристика лоббирования как компонента структуры информационно-психологических операций. Комплексные организационные технологии тайного принуждения личности: уточнение и систематизация понятий. Анализ применения конкретной информационно-психологической операции в современной политической борьбе в России.

*Тема 6. Технологии тайного принуждения личности в массовых информационных процессах*

Информационно-психологическое воздействие в массовых информационных процессах и особенности его анализа. Позиции рассмотрения и особенности анализа психолоогических манипуляций в массовых информационных процессах. Основания для выделения различных групп приёмов манипулятивного воздействия в массовых информационных процессах. Особенности и задачи основных этапов информационно-психологического воздействия манипулятивного характера.

Технология тайного принуждения личности в массовых информационных процессах. Приёмы и техника манипулятивного воздействия в массовых информационных процессах. Техника формирования доверия и привязанности к коммуникатору. Манипулятивные техники в массовых информационных процессах. Основные приёмы оказания манипулятивного воздействия, используемые в средствах массовой информации (в том числе “семь приёмов” или “азбука пропаганды” и т.д.). Слухи и провокации как специфические техники информационно-психологического воздействия. Алгоритм анализа информационных сообщений в средствах массовой информации.

*Тема 7. Технологии тайного принуждения личности в межличностном взаимодействии*

Позиции рассмотрения и особенности анализа межличностных манипуляций. Характеристика коммуникативных ситуаций межличностного взаимодействия (групповая дискуссия, публичная полемика, обсуждение, переговоры, общение в диаде). Обсуждение как основной компонент межличностного взаимодействия.

Приёмы и техника психологических манипуляций в межличностном взаимодействии. Общая схема ориентировочной основы действий в межличностных коммуникативных ситуациях и используемые уловки, их классификация. Манипулятивные приёмы, используемые уловки, их классификация. Манипулятивные приёмы, используемые в ходе обсуждений и дискуссий. Характеристика основных организационно-процедурных, логико-психологических и личностных уловок. Психологические манипуляции, используемые в переговорах и личном общении.

Манипулятивные игры в межличностном взаимодействии (психологические игры как технологии манипулирования личностью). Межличностные манипулятивные игры. Соотношение понятий “игра”, “ритуал”, “времяпровождение” в межличностном взаимодействии. Примеры межличностных манипулятивных игр. Техники скрытого получения информации от партнёра по общению как межличностные манипулятивные игры. Манипулятивные игры в предпринимательской деятельности.

## *Часть III. Психологическая защита как основной способ обеспечения информационно-психологической безопасности личности*

Тема 8. Возможности человека и психологическая защита личности

Индивидуальные различия защитного личностного потенциала (индивидуальные различия в использовании личностью возможностей психологической защиты). Виды психологических защит. Понятие, сущность и характеристика психологической защищённости, психологической защиты, особенности механизмов межличностной и внутриличностной

психологической защиты. Психологическая защита как основной способ обеспечения информационно-психологической безопасности личности.

*Тема 9. Механизмы внутриличностной психологической защиты*

Особенности рассмотрения механизмов внутриличностной психологической защиты. Характеристика базовых механизмов внутриличностной психологической защиты и особенности их проявлений в защитном поведении личности. Краткие рекомендации по учёту базовых механизмов внутриличностной психологической защиты при формировании психологической самозащиты личности.

*Тема 10. Система психологической защиты личности.*

Эволюция способов защиты. Определение понятия “психологическая защита личности”. Содержание и структура системы психологической защиты личности. Понятие, сущность, характеристика, уровни психологической защиты, основные направления и способы психологической защиты личности.

Соотношение и взаимосвязь психологической самозащиты, психологической и социально-психологической защиты личности.

Понятие, сущность, характеристика психологической самозащиты, структура и основные этапы её формирования.

*Тема 11. Алгоритмы психологической самозащиты личности*

Понятие алгоритма психологической самозащиты личности. Содержание и структура алгоритмов психологической самозащиты в межличностных ситуациях. Особенности алгоритмов психологической самозащиты в контакт-коммуникационных ситуациях. Особенности алгоритмов психологической самозащиты в масс-коммуникационных ситуациях.

*Тема 12. Методика формирование психологической самозащиты личности*

Разработка структурно-логической модели процесса подготовки. Выделение теоретического материала, который необходимо усвоить слушателям, последовательности его подачи, форм проведения занятий. Описание системы умений, которые должны сформироваться у обучаемых. Обоснование и выбор необходимых учебно-методических материалов, материально-технических и организационных условий. Системы оценки (диагностики) и коррекции.

Понятие индивидуального стиля психологической самозащиты, личностные факторы и социально-психологические условия, влияющие на его формирование. Методические рекомендации по формированию и совершенствованию индивидуального стиля психологической самозащиты личности.

> *Наверное, то же самое мы сейчас должны будем сказать о компьютерах, выступающих в роли искусственного интеллекта. Они должны будут не только освободить, но и покорить человека. Как машины встали между природой и человеком, так и компьютеры встанут между человеком и смыслами. И если нам сейчас приходится, хотя и тщетно, защищать природу, то не придется ли так же и, наверное, так же тщетно, защищать смыслы?*
>
> *В.В. Налимов*

Чтобы сформировать у слушателей навыки по созданию математических моделей в сфере информационного противоборства, необходимо: изучить основные определения и теоретические положения из сферы информационного противоборства; изучить существенные и разработать собственные модели для решения задач, которые в общем виде могут быть охарактеризованы следующим образом.

Исходные данные:

- два и более субъектов, осуществляющих борьбу друг с другом за ресурсы;
- поведение сражающихся субъектов определяется имеющимися у них моделями мира.

При этом модели мира претерпевают постоянные изменения под воздействием данных, поступающих на вход систем;

• борьба идёт исключительно путём целенаправленого информационного воздействия, т.е. благодаря созданию соответствующих последовательностей сообщений, направленных на искажение модели мира противников.

Результатом решения названных задач должны стать модели и стратегии поведения субъеков (информационных объектов*), разработанных слушателем.

*Здесь и далее под информационным объектом понимается объект — носитель знания.

**Основные термины и определения**

Чтобы эффективно использовать холодное оружие, его владельцу необходимы ловкость и сила.

Основу принципа функционирования огнестрельного оружия составляет химическая реакция, протекающая с выделением энергии. Физическая сила становится не нужной. Задача стреляющего только в том, чтобы точно направить оружие.

В основе принципа функционирования термоядерного оружия лежит реакция ядерного синтеза, протекающая с выделением энергии, которая и используется для уничтожения всего живого вокруг места падения снаряда или бомбы.

Основа принципа функционирования информационного оружия — запуск или генерация **программы самоустранения (самоуничтожения, самоограничения)**, присущей любой **сложной информационной системе***, способной к обучению. Задача противника состоит только в том, чтобы, манипулируя входными данными, активизировать в системе требуемые программы или процессы, приводящие к генерации подобных программ.

* Система — совокупность абстрактных или материальных объектов вместе с известными либо заданными связями и отношениями, образующих в известном либо заданном смысле единое целое". В данном случае это целое является носителем знания и при определённых отношениях может именоваться информационным объектом.

Здесь и далее под **информационной системой** понимается система, осуществляющая:

• получение входных данных;

• обработку этих данных и (или) изменение собственного внутреннего состояния (внутренних связей/отношений);

• выдачу результата либо изменение своего внешнего состояния (внешних связей/отношений).

Эмпирический объект*, способный к обучению с помощью абстрактных объектов, назовём **информационным самообучающимся** объектом.

* Эмпирический объект (по А.А. Зиновьеву) — объект, обладающий ограниенными пространственно-временными координатами.

Информационную систему, элементы которой функционируют в соответствии с правилами, порожденными одним и тем же взаимно непротиворечивым множеством аксиом, назовём **простой информационной системой**.

**Информационную систему,** которая содержит элементы, функционирующие в соответствии с правилами, порождёнными отличными друг от друга множествами аксиом, назовём **сложной информационной системой**. Допускается, что среди правил функционирования различных элементов могут быть взаимно противоречивые правила и цели. При этом нарушение защитных барьеров во взаимодействии элементов сложной системы друг с другом приводит к перепрограммированию этих элементов и (или) их уничтожению. В результате, с одной стороны, чем функционально разнообразнее элементы системы, тем больше потенциальных функциональных возможностей у самой системы, а с другой стороны, тем чаще постоянные изменения состояния системы, происходящие в основном под воздействием входных данных, могут приводить к взаимодействию внутри системы взаимоисключающих или "мешающих" друг другу элементов, что в определённых случаях становится причиной гибели системы или самогенерации опасных для нее программ.

Таким образом, **информационное оружие** представляет собой средства, направленные

на активизацию в информационной системе_процессов, в которых заинтересован субъект, применяющий оружие.

В информационное оружие не требуется “вкладывать энергию” для уничтожения противника. Изначально предполагается, что противник обладает всеми необходимыми средствами для собственного уничтожения.

В качестве информационного оружия могут выступать любые технические, биологические, социальные средства (системы) для целенаправленного производства, обработки, передачи, представления (отображения), блокировки данных и (или) процессов, работающих с данными.

Применение информационного оружия предполагает:

1) анализ способов и механизмов активизации у конкретной системы-противника, заложенных в неё программ самоуничтожения, самоподавления, самоограничения и т.п.;

2) разработка конкретного информационного оружия;

3) применение информационного оружия по заданному объекту в рамках разработанной **информационной операции**.

**Информационная операция** — это последовательность действий по применению конкретного информационного оружия в рамках разработанной тактики и стратегии ведения **информационной войны**.

**“Война”** в соответствии с используемыми в большинстве стран мира определениями* представляет собой “*наличие вооруженной борьбы между государствами*”. Таким образом, **информационная война** — это борьба между государствами с использованием исключительно информационного оружия.

*Подробный анализ таких понятий как “информационная война” и “война” приведён в работе И.В. Свиридова “Информационная война: определения, подходы, взгяды...”, опубликованной в журнале “Безопасность информационных технологий”, № 4, 1998.

В силу того, что создание алгоритма определения начала информационной войны в общем виде — алгоритмически неразрешимая проблема*, информационные сражения могут протекать и без применения каких-либо иных вооружений, т.е. в “мирное” время. Принципиальной разницы между терминами “**информационная война”** и **“информационное противоборство”** нет.

*Расторгуев С.П. Информационная война. М.: Радио и связь, 1998.

Информационные “сражения” протекают между любыми сложными информационными объектами, осуществляющими борьбу за общие ресурсы.

В человеческом обществе как сложной информационной системе, информационное противоборство велось на протяжении всей его истории. Однако ранее информационное оружие по критерию эффективность/стоимость значительно уступало любым другим средствам вооружения*. Величина данного параметра (эффективность/стоимость) в свою очередь зависела от природно-климатических условий, развития науки, промышленного производства, уровня развития соответствующих технологий. Для широкого применения информационного оружия, как и любого другого, требуется, чтобы оно:

• максимально быстро по сравнению с другим видом вооружения могло быть применено по объекту воздействия;

причинило объекту воздействия требуемый ущерб в заданный временной интервал;

• было достаточно простым и дешёвым в изготовлении по сравнению с другим видом оружия такого же класса воздействия.

*Использование в человеческом обществе того или иного вида оружия всегда определяется в отношением эффективности применения для достижения поставленных целей к стоимости создания и применения. Кроме того, важную роль в выборе оружия играет время на его создание и применение.

В последние десятилетия возникли условия, которые позволили говорить об информационном оружии, как о наиболее значимом оружии современной эпохи. К ним относятся:

• резкое удешевление производства данных благодаря средствам вычислительной техники. Производство информации поставлено на конвейер;

• резкое удешевление и сокращение времени на доставку сообщений практически в лю-

бую точку планеты благодаря развитию телекоммуникационных средств;

• резкое повышение эффективности информационного воздействия благодаря появлению развитых теорий в области перепрограммирования информационных самообучающихся систем: теория программирования для ЭВМ и NLP-программирования для социальных систем, включая большое количество методов и приёмов информационно-психологического воздействия.

Конечным объектом действия информационного оружия являются **знания** конкретной информационной системы, путём целенаправленного изменения которых вносятся искажения в модель мира противника. Для того чтобы в дальнейшем стало возможным использовать термин "знание" для описания результатов информационного воздействия, его требуется формально определить.

Под **знанием информационной системы** понимается совокупность сведений, выраженная через структуру системы и функциональные возможности её элементов.

Так как знание понимается через структурную и функциональную сложность системы, то представляется разумным определить "**информационную ёмкость"** пропорционально количеству элементов в структуре и числу связей между ними

$$E = s + n \quad ,$$

где s — общее число связей между элементами;

n — количество элементов в системе.

Тогда под термином **информация** будем понимать *изменение параметра наблюдателя, вызванное взаимодействием наблюдателя с объектом**, оцениваемое через величину изменения информационной ёмкости системы-наблюдателя

$$I = E(t_1) - E(t_2) \quad ,$$

где $E(t_1)$ информационная ёмкость системы в момент времени $t_1$,

$E(t_2)$ информационная ёмкость системы в момент времени $t_2$,

*Эта часть определения предложена В.И. Шаповаловым в работе "Энтропийный мир". Волгоград: Перемена, 1995.

Процесс целенаправленного изменения знания информационной системы под воздействием входных данных назовём **обучением** системы*. Изменения могут включать в себя:

• изменение связей между элементами системы;

• изменение количества элементов;

• изменение функциональных возможностей элементов**.

*Если воспользоваться введёнными определениями, то, образно говоря, информационную войну можно трактовать как столкновение различных знаний, в ходе которого определяется истина.

**Для оценки полученной информации изменение функциональных возможностей элементов всегда может быть представлено через изменение количества элементов, для этого достаточно закрепить за каждым элементом не более одной функции.

Из сказанного выше следует, что при столкновении двух и более носителей знания в информационном противоборстве побеждает тот:

1) кто смог в максимально короткие сроки сгенерировать и применить опасное для противника обучающее воздействия или последовательность воздействий;

2) чья структура* наиболее устойчива к информационному воздействию противника.

*В первую очередь здесь речь идёт о структуре управления, как о структуре наиболее подтверждённой информационному воздействию.

В дальнейшем общий план ведения информационной войны, включающий разработку последовательности информационных операций и мер по защите собственной структуры, назовём **информационной стратегией** или **стратегией информационной войны**.

Для систем, обучающихся на принципах гибели и рождения собственных элементов, не существует типовой всегда побеждающей стратегии*. Каждый противник заслуживает индивидуального подхода, максимально учитывающего его особенности по восприятию

информации. Для социальных систем требуется знание истории народов, культуры, обычаев, но в первую очередь принципов и самых подробных нюансов по функционированию и формированию системы управления. Для технических систем способы информационного воздействия, язык, особенности архитектуры, “люки” в системе защиты и, конечно, алгоритмы работы системы управления.

Расторгуев С.П. Информационная война. М.: Радио и связь, 1998.

Что же касается вопроса создания структуры, максимально устойчивой по отношению к внешнему знанию, к **входной обучающей выборке**, сгенерированной противником, то здесь именно требование “выжить” должно формировать под себя и динамически модифицировать структуру системы управления*. На сегодняшний день проблема проектирования устойчивых к внешним физическим воздействиям объектов частично изучается такой дисциплиной как “Сопротивление материалов”, что же касается социальных структур, устойчивых к информационным воздействиям, то подобные исследования были начаты в начале XX века в рамках социальной психологии. Одними из первых задач стали задачи по моделированию конфликтных ситуаций в коллективах. Формулировались они примерно так:

Дано:

1) социальная система из n человек, для которых известны их отношения предпочтения** друг к другу в виде: “+” положительно, “-” отрицательно, “0” нейтрально;

2) правило изменения предпочтений;

3) функциональные возможности всех элементов системы;

4) взаимоотношения между элементами, возникающие в процессе выполнения системой своих функциональных предназначений.

Требуется: определить структуру коллектива, имеющего минимально возможное предрасположение к возникновению в нём конфликтных ситуаций***.

*Это один из многих фактов, который не был учтён руководством Советского Союза в ходе глобального информационного противоборства.

**В данном случае предполагается, что отношения предпочтения формируются в ходе именно информационного взаимодействия.

***В данном случае под конфликтной понимается ситуация, приводящая к сокращению функциональных возможностей системы в целом.

### *Оценка эффективности информационного противоборства*

Как было отмечено выше, нарушение защитных барьеров во взаимодействии элементов сложной системы друг с другом приводит к перепрограммированию этих элементов и (или) их уничтожению. **Информационным “полем боя”** являются в первую очередь протоколы информационно-логического сопряжения элементов сложной системы, средства и технологии их практической реализации.

Протокол информационно-логического взаимодействия для элементов социального пространства нашёл свое воплощение в естественном языке каждого народа. Использование того или иного языкового подмножества языка во многом определяет информационные возможности различных групп населения.

Основными средствами корректировки протоколов информационно-логического взаимодействия для социального пространства сегодня стали СМИ.

Протокол информационно-логического взаимодействия для элементов кибернетического пространства отражён во множестве языков программирования, в сетевых протоколах. Основными средствами несанкционированной корректировки этих протоколов являются программные закладки, компьютерные вирусы и т.п. средства и технологии воздействия на каналы телекоммуникаций.

В зависимости от того, какие происходят изменения во внутреннем состоянии информационных систем, предлагается осуществить следующую классификацию:

**класс А —** системы с неизменным внутренним состоянием после отработки входного сообщения;

**класс В** — системы с изменяющимся внутренним состоянием.

В свою очередь в классе В можно выделить следующие подклассы:

**подкласс 1** — системы с неизменным алгоритмом обработки, но с изменяющимися данными (базы данных, отдельные массивы и т.п.), которые используются в процессе обработки входной информации;

**подкласс 2** — системы с адаптивным алгоритмом обработки, т.е. алгоритм настраивается на условия применения; настройка осуществляется путём либо изменения управляющих коэффициентов, либо автоматического выбора алгоритма из множества равносильных алгоритмов;

**подкласс 3** — системы с самомодифицирующейся целью и соответственно с полностью самомодифицирующимся алгоритмом, выходящим за пределы множества равносильных алгоритмов.

На рис.1. приведены примеры информационных систем из различных классов. Однако воспринимать изображённое на нём желательно с определённой долей условности. В частности, старинный классический телеграфный аппарат является в большей мере механической системой, осуществляющей обработку входных данных и возвращающейся в исходное состояние по окончании обработки (класс А), но будучи оснащён процессором с памятью и алгоритмом для восстановления искаженных данных, поддерживающим несколько уровней протоколов информационно-логического взаимодействия, он вместе с подобными же аппаратами уже переходит в разряд систем передачи данных (класс В).

То же можно сказать и про автоматизированные информационно-поисковые системы; в зависимости от реализации они могут быть отнесены к системам как первого подкласса, так и второго. Системы управления также различаются не только по своим функциональным и потенциальным возможностям, но и по способам реализации.

Основная идея рис.1 в том, чтобы показать ступени развития информационных систем. Любопытно, что та ниша, которую в своей эволюции перескочила Природа — подкласс 2, заполнена с помощью человека.

**Информационное оружие** имеет прямое отношение к алгоритмам. Поэтому о любой системе, способной по входным данным отрабатывать тот или иной алгоритм, можно говорить как об информационной системе — объекте информационной войны.

Ещё раз вернёмся к понятию войны информационных систем и, опираясь на него, продолжим терминологическое оснащение основ данной теории. Под **войной информационных систем** будем понимать их **действия**, направленные на получение материального преимущества, путём нанесения противнику **ущерба** с помощью соответствующего **информационного воздействия**.

В данном случае предполагается, что пока противник устраняет полученный ущерб, т.е. занят только собой, противная сторона имеет преимущество во внешнем мире. Понятно, что подобная война имеет смысл лишь для систем, потребляющих в своей жизнедеятельности общие ограниченные материальные ресурсы.

При этом для систем из класса В действия, направленные на нанесение ущерба, представляют собой процесс обучения, в основе которого лежит целенаправленное манипулирование входными данными и результатом.

Перейдём к определению **понятия** ущерб, так как именно через причинённый ущерб противнику можно оценить **эффективность** собственного информационного оружия. Для этого рассмотрим весь цикл обработки входных данных информационной системой.

Обработка подразумевает процесс, включающий в себя получение (ввод) данных, обработку и выдачу результата.

**Процесс ввода** данных характеризуется:

1) исходными данными $F_i$ ($0<i<n_п$);

2) объёмом данных $n_п$;

3) временем получения и ввода данных $t_п$.

**Процесс обработки:**

1) исходными данными $F_i$ ($0<i<n_п$);

2) объёмом исходных данных $n_п$;

3) данными, используемыми при обработке — база знаний $B_j$ ($0<j<n_д$);

4) алгоритмами, используемыми при обработке, $A_j$ ($0<j<n_a$);

5) временем обработки $t_o$.

**Процесс выдачи результата:**

1) результатом $R_k$ ($0<k<n_p$)

2) объёмом результата $n_p$;

3) временем представления результата $t_p$.

Перечисленные характеристики во многом определяются следующими **показателями состояния информационной системы.**

Количеством элементов, ответственных за сбор входных данных, и эффективностью их функционирования. В данном случае под эффективностью функционирования элемента предлагается понимать такие количественные характеристики: объём добываемых данных, "новизна" данных, достоверность данных.

Количеством элементов, ответственных за доставку данных, и эффективностью их функционирования. В данном случае под эффективностью функционирования элемента предлагается понимать: время доставки данных, объём искажённых данных.

Количеством элементов, ответственных за обработку данных, и эффективностью их функционирования, которая в общем случае оценивается временем обработки данных, временем выработки решения и, возможно, мощностью потенциального пространства решений.

Количеством элементов, ответственных за представление результата, и эффективностью их функционирования. Здесь эффективность функционирования можно попытаться оценить через степень искажения принятого решения при его реализации.

Количеством и качеством связей между элементами.

Защищённостью ("жизненной силой") перечисленных выше элементов и связей между ними. При этом надо иметь в виду, что понятие "информационная защищённость элемента" подразумевает защиту этого элемента от информационных воздействий. В том случае, если защищаемый элемент принадлежит системе принятия решения, то наличие подобной защищённости резко понижает эффективность его работы в силу сокращения допущенных до него системой обеспечения безопасности данных, которые могут оказаться необходимыми системе для выработки команд адекватной реакции.

Считаем, что нанести системе **ущерб** — это значит:

а) **исказить результат** работы системы таким образом, чтобы получить преимущество в материальной сфере,

или

б) привести её в такое состояние, в котором она не способна выдавать никакого результата.

В случае, если ущерб заключается **в искажении результата** работы систем, назовём такой ущерб *локальным*.

Под **искажением** результата понимается:

1) искажение результата $R_k$ ($0<k<n_p$);

2) искажение объёма результата np, что приводит к уничтожению части данных и (или) добавлению новых;

3) изменению времени получения результата $t_p+t_o+t_п$.

Нанести *фатальный* ущерб — это значит привести систему в такое состояние, в котором она не способна выдавать никакого результата. При этом система самостоятельно не может выйти из этого состояния.

Теперь представим себе, что две или более информационные системы функционируют в условиях общего ресурса. Тогда в борьбе за ресурс системы класса А, безусловно, будут уступать любым системам из класса В. Любая информационная война между ними закон-

чится в пользу системы из класса В. Доказательство данного утверждения очевидно.

Сложнее обстоят дела, когда между собой сталкиваются системы из класса В. Но и в этом случае победитель, как правило, может быть назван заранее — это информационные системы из подкласса 3.

Что же касается информационного столкновения между собой систем из третьего подкласса, то определение победителя для них — это непростая проблема, не имеющая типового алгоритма.

Признаки информационного поражения надо начинать искать исходя из того, что информационное оружие в первую очередь действует на систему управления, не столько уничтожая, сколько подчиняя себе систему управления поражённого объекта в силу того, что именно система управления наиболее чутко реагирует на входные сообщения. Именно так воздействуют наиболее опасные биологические, социальные, психические и компьютерные вирусы.

При этом управление поражённой системой осуществляется с помощью скрытого и явного информационного воздействия на систему как извне, так и изнутри.

Цель этого воздействия — целенаправленно изменить поведение системы. Это значит, что главным признаком информационного поражения и будут изменения в поведении поражённой системы.

Поражённая информационным оружием система в своём поведении руководствуется уже не столько собственными интересами, сколько чужими командами. И чем больше ориентация в поведении на чужие команды, тем глубже информационное поражение. При этом команды могут быть скрытыми или явными.

Давать оценку степени информационного поражения имеет смысл исключительно по событиям, происходящим в материальном мире. Именно этот вектор предпочтения и есть та стрелка компаса, которая позволяет понять, в чьих интересах работает система управления.

Предлагается **степень поражения информационным оружием** оценивать через информационную ёмкость той части структуры поражённой системы, которая либо погибла, либо работает на цели, чуждые для собственной системы.

Что означает данное определение на практике?

Для вычислительной однопроцессорной системы степень ущерба можно оценить через процент потерянного полезного времени (иногда — через число репликаций компьютерного вируса), т.е. через долю процессорного времени, в течение которого инфекция управляет всей системой для достижения запрограммированных в ней целей плюс объём погубленных программ и данных, имеющих отношение к дальнейшему существованию этой системы, к поддержанию её потребительских свойств.

Для государства, по аналогии, — это доля паразитирующих государственных структур или структур, работающих в этом государстве в интересах других государств.

Для народа степень ущерба можно оценить через процент, на который ежегодно происходит уменьшение его численности плюс погибшие культурные ценности и научно-производственные центры.

### Устойчивость знания

Понятие устойчивости — одно из ключевых при исследовании информационных самообучающихся систем. В силу того, что структура, образно говоря, олицетворяет собой **знание**, словосочетание “устойчивость структуры” означает “**устойчивость знания**”

Ответить на вопрос: какое знание наиболее устойчиво? — означает найти структуру, соответствующую этому знанию.

В качестве исходной предпосылки предположим, что система **устойчива к внешним информационным воздействиям**, если количество её элементов не испытывает “резких” колебаний от этих воздействий.

Если взять введённое определение устойчивости в качестве базового, то надо понять,

какой структурой должна обладать система, чтобы количество её элементов не испытывало так называемых резких колебаний, и определиться с тем, что понимается под резкими колебаниями?

Первое, что напрашивается в качестве примера, это структура, в которой есть несколько групп элементов, тесно связанных друг с другом, но при этом связи между группами очень неустойчивы, например:

A:{ 1(2,3,4),2(1,3,4),3(1,2,4),4(1,2,3,5),5(4,6,7), 6(5,7),7(5,6)} .

В приведённой структуре (рис. 2) А достаточно уничтожить элемент с номером 4, как сразу количество элементов системы уменьшится в два раза. Интуитивно понятно, что эта структура не является устойчивой в смысле данного выше определения, т.е. неустойчивой является любая структура, в которой имеют место одиночные элементы, осуществляющие связку групп элементов.

И наоборот, **максимально устойчивой системой** можно считать систему, структура которой обладает максимальным количеством связей — каждый соединён с каждым.

Попробуем формализовать сказанное.

Обозначим через $U_i$ — количество элементов структуры, которые будут потеряны для системы, в случае уничтожения i элемента. А через n — количество элементов.

Тогда под первой степенью устойчивости той или иной структуры будем понимать следующую величину:

$$V = \frac{n}{\left(\sum_i U_i\right)}$$

.

Название “первая степень устойчивости” выбрано с предположением, что одновременно из структуры вырывается только один элемент. Если же речь идёт об одновременном изъятии из структуры двух и более элементов, то здесь уже надо говорить о соответствующем показателе степени устойчивости к внешним воздействиям.

В том случае, если первая и вторая степени устойчивости совпадают, будем считать, что структура обладает глубинной устойчивостью.

Например, такие структуры как круг (круглая форма) и решётка (клеточная форма) имеют первую степень устойчивости. Однако их исследование на уровне второй и третьей степени устойчивости показывает, что в отличие от решётки круг не обладает глубинной степенью устойчивости.

Звёздообразная форма структуры не имеет даже первой степени устойчивости. Достаточно выбить центровой элемент, чтобы система погибла. Однако данная форма структуры способствует минимальной “мере хаоса в принятии решения”*, т.е. система раньше других способна “почувствовать” опасность и принять соответствующие меры. Устойчивость систем, в основе которых лежит звёздообразная структура, к внешним воздействиям определяется исключительно “жизненной силой” центральных элементов и их защищённостью. Если в процессе функционирования центральные элементы вырождаются или поражаются, как в случае СССР, то система распадается.

*Предполагается, что избыток связей создаёт хаос в принятии решения, увеличивая тем самым время реакции системы, т.е. снижая её способность к сопротивлению от угроз, требующих быстрой реакции.

**Структура является абсолютно устойчивой**, если все её степени устойчивости стремятся или равны 1.

Удаление любого из элементов отражается только на этом элементе и в меньшей степени на структуре, т.е. оставшаяся структура “страдает” от потери только одного этого элемента.

Степень устойчивости всегда меньше либо равна 1.

Система максимально устойчива тогда, когда V=1.

Степень устойчивости минимальна, если изъятие любого из элементов приводит к пол-

ному разрушению системы. Наиболее близкий пример подобной структуры — звёздообразная форма. Уничтожение центрального элемента приводит к гибели всей системы.

Степень устойчивости структуры, имеющей звёздообразную форму, стремится к 1/2.

Аналогичный в смысле определений подход по оценке устойчивости структур можно найти в существующих исследованиях математических моделей в экологии, в частности Ю.М. Свирежев*, анализируя устойчивость как меру флуктуаций численности видов в сообществе, отмечает: *"Сообщество максимально устойчиво в том случае, когда число трофических связей в нём равно максимально возможному и интенсивность взаимодействий между различными видами одинакова. Другими словами, максимально устойчивым является сообщество без иерархической структуры"*

*Свирежев Ю.М. Вито Вольтерра и современная математическая экология//Вольтера В. Математическая теория борьбы за существование. М.: Наука, 1976.

**Проблема понимания друг друга информационными противниками**

Прежде чем перейти непосредственно к математическим основам теории рефлексивных процессов отметим, что в сложных технических системах с элементами самообучения, биологических или социальных объектах, нас в первую очередь интересует присущая им информационная общность, безотносительно их природы. Так, если в приведённой ниже цитате основоположников NLP-программирования заменить слово "людьми" на "информационными самообучающимися системами", то смысл практически не пострадает. Ибо с возрастанием сложности даже в области технических систем мы имеем всё более выраженную информационную индивидуальность, объясняемую не столько конструкторскими решениями, сколько результатами конкретных столкновений системы с входными данными, изменяющими её:

*"В мире нет и двух человек, опыт которых полностью совпадал бы между собой. Модель, создаваемая нами для ориентировки в мире, основывается отчасти на нашем опыте. Поэтому каждый из нас создаёт отличную от других модель общего для нас мира и живёт, таким образом, в несколько иной реальности.*

*Будучи людьми, мы не имеем дела непосредственно с миром. Каждый из нас создаёт некоторую репрезентацию мира, в котором мы все живём. То есть все мы создаём для себя карту или модель, которой пользуемся для порождения собственного поведения. В значительной степени именно наша репрезентация мира задаёт наш будущий опыт в этом мире: то, как именно мы воспринимаем этот мир, с какими выборами сталкиваемся в своей жизни".**

*Гриндер Д.,Бэндлер Р. Структура магии. СПб.: Белый кролик, 1996.

Понятно, что чем дальше в пространстве смыслов отстоят друг друга информационные системы, тем чаще их столкновение друг с другом будет приводить к возникновению ситуаций, приводящих к резкому изменению знания, носителями которого они являются, а значит и к конфликту структур.

Этот параграф посвящен проблеме сравнения информационных самообучающихся систем одного типа друг с другом. В силу того, что их структура постоянно изменяется, а кроме того, является внутренней сущностью системы, недоступной для внешнего наблюдателя, опираться на неё, как на сравнительную характеристику, не всегда удобно. Хотелось бы, чтобы сравнительная характеристика была наблюдаема. В частности, для этой цели предлагается воспользоваться некоторой оценкой входа/выхода системы, т.е. оценкой множества входных сообщений и соответствующих им выходных.

Считаем, что одна информационная система "понимает" другую, если их языки связи с внешним миром и, естественно, друг с другом частично или полностью совпадают*.

*Расторгуев С.П. Инфицирование как способ защиты жизни. М.: Агентства Яхтсмен, 1996.

Определим язык i-й информационной системы в виде множества пар:

$$S_i = \left\{ \left( a_{i,k}, b_{i,k} \right) \right\} \quad ,$$

где

$0 \le k \le n$ ;

n — количество различных возможных сообщений в языке системы i;

$a_{i,k}$ — сообщение, поступающее на вход системы i;

$b_{i,k}$ — сообщение, выдаваемое на выходе системы i в ответ на сообщение ai,k.

Понятие “сообщение” в нашем случае включает в себя все присущие ему атрибуты: форму, содержание, время передачи, паузы и т.д. Для простоты будем рассматривать сообщение в виде следующей тройки:

$$a_{i,k} = d_{i,k}, f_{i,k}, t_{i,k} \quad ,$$

где

$d_{i,k}$ — само сообщение;

$f_{i,k}$ — интенсивность передачи сообщения (сила);

$t_{i,k}$ — время ответа.

Считаем, что сообщение

, 1, если

$a_{i,k} = a_j$

$d_{i,k} - d_{j,l} < \Delta d$ ,

$f_{i,k} - f_{j,l} < \Delta f$ ,

$t_{i,k} - t_{j,l} < \Delta d$ .

Обозначим

$s_{i,k} = (a_{i,k} , b_{i,k})$,

$A_i = \{ a_{i,k}\}$ ,

$B_i = \{ b_{i,k}\}$ ,

μ ()— функция подсчёта количества элементов множества.

Тогда уровень “взаимопонимания” систем i и j определим следующим образом:

$$M_{i,j} = \mu(S_i \cap S_j) / \max(\mu(S_i), \mu(S_j)) \quad (1)$$

уровень понимания системой i системы j

$$m_{i,j} = \mu(S_i \cap S_j) / \mu(S_i) \quad . \quad (2)$$

Эти определения отражают то интуитивное ощущение, что чем больше общих понятий, в частности одинаковых слов в двух языках, тем носители этих языков лучше понимают друг друга.

Однако вполне возможна ситуация, когда за одинаковыми словами скрывается разный смысл, т.е. система i на сообщение $a_{i,1}$ всегда отвечает сообщением $b_{i,1}$, а система j на то же самое сообщение отвечает сообщением $b_{j,1}$, при этом

$$b_{i,1} \neq b_{j,1} \quad .$$

Для того чтобы описать подобную ситуацию, введём понятие “похожесть” систем и будем оценивать уровень “похожести” системы i на систему j по следующей формуле:

$$p_{i,j} = \mu(A_i > A_j) / \mu(A_j) \quad . \quad (3)$$

Тогда, опять же интуитивно, понятно, что чем меньше взаимопонимание систем, но чем больше “похожесть” их друг на друга, тем более сильным может быть взаимное разрушение при их взаимодействии.

Простой пример. Собака, когда настроена доброжелательно, поднимает хвост. Кошка

поступает прямо противоположно. Взаимообратные языковые системы приводят к тому, что кошка с собакой и “живут как кошка с собакой”.

Попробуем ввести численную оценку уровня “агрессивности” систем по отношению друг к другу, которую обозначим через $U_{i,j}$.

Для того чтобы определить, что такое уровень агрессивности, введём ряд ограничений и требований к этой величине:

1) в том случае, если уровень “похожести” системы i на систему j равен 0, то $U_{i,j} = 0$;

2) $U_{i,j}$ прямо пропорционально количеству несовпадающих ответов (выходных сообщений) i и j систем на совпадающие вопросы (входные сообщения).

Тогда относительное количество несовпадающих выходов по совпадающим входам можно определить по формуле

$$U_{\mathrm{i,j}}=\Big(\sum_{k=0}^{k=n} \mu \quad (a_{\mathrm{i,k}} \cap A_j)\big(1-\mu(s_{\mathrm{i,k}} \cap S_j)\big)\Big)/n \tag{4}$$

Формула (4) удовлетворяет условию 1 и условию 2.

Таким образом, можно констатировать, что для выполнения совместных функций в каждой системе по отношению к соседней в процессе функционирования возникает “понимание”, которое можно оценить по формуле (2), и “агрессивность”, которую можно оценить по формуле (4).

**Алгебра рефлексивных процессов***

Историю становления проблематики рефлексивных процессов можно найти в работе В.Е. Лепского “Вехи становления проблематики рефлексивных процессов” // Прикладная эргономика. №1. 1994. (Специальный выпуск “Рефлексивные процессы”. М.: Ассоциация прикладной эргономики).

Одним из первых авторов, занимавшимся исследованием конфликтов между информационными самообучающимися системами был кандидат психологических наук Владимир Александрович Лефевр*. Важнейший для теоретических построений постулат, выдвинутый им, заключался в необходимости учёта при планировании информационных операций не только моделей мира, созданных противниками, но и моделей моделей... Им же была предложена достаточно наглядная форма описания процесса осознания мира рефлексивными системами**.

*Лефевр В.А. Конфликтующие структуры. М.: Сов. радио, 1973.

**Под рефлексивной системой В.А, Лефевр понимал систему зеркал, многократно отражающих друг друга. Рефлексия — способность встать в позицию исследователя по отношению к другому “персонажу”, его действиям и мыслям.

Здесь мы опишем формальные конструкции, ориентированные на формализацию стратегии информационного противоборства, частью фундамента для которых стала предложенная В.А. Лефевром “Алгебра рефлексивных процессов”, но с определённой модификацией, вызванной желанием приблизить предложенный им формализм к языкам программирования для ЭВМ, понимая, что дальнейшее развитие данной теории во многом связано с увязкой её с теорией программирования. Кроме того, опыт применение данного аппарата в практике формулирования информационных стратегий привёл к необходимости включения дополнительных операций преобразования мира.

Итак, введём следующие обозначения:

x,y,z — информационные объекты (противники);

A,B,C,D... — конкретные информационные объекты, имеющие имена собственные;

T, $W_1$,$W_2$,$W_i$ — миры, в которых функционируют информационные системы. Например: T = x+y+z;

$X_1$,$X_2$,...$X_i$, $Y_1$,$Y_2$,...$Y_i$ — модели мира, создаваемые соответственно объектами $x_1$,$x_2$,...$x_i$, $y_1$,$y_2$,...$y_i$

“•” операция осознание, результатом которой является возникновение внутри информационной системы картины мира. Внешний мир с определённой долей искажения перено-

сится внутрь информационной системы. Результат операции осознания будем записывать следующим образом: x•T или • (xT), или xT. Применение операции осознания к внешнему миру предполагает создание его модели. Повторное применение операции осознания предполагает создание модели модели мира — xxT или x•x•T, или $x^2T$. Операция возведения в степень используется исключительно для удобства записи неоднократного применения операции осознания;

“+” операция расширения мира, результатом этой операции является появление объекта в мире;

“-” операция исключения объекта из мира;

“-” операция отрицания, означает, что информационный объект, перед идентификатором которого стоит этот знак, в этом мире отсутствует;

“()” — скобки используются аналогично скобкам при выполнении операций умножить, сложить, вычесть;

“[]” — квадратные скобки используются для выделения отдельных объектов, присущих тому миру, перед которым они поставлены. Например, запись W[A,B,-C] означает, что для мира W характерно нахождение в нём объектов A, B и отсутствие объекта C.

Используя предложенный формализм, факт нахождения в мире двух объектов, имеющих модели этого мира, может быть записан следующим образом:

W = T + xT + yT.

При этом X = xT, Y = yT.

Введём следующие правила применения операций:

1) Расширение мира n раз за счёт одного и того же объекта не изменяет мир:

T + xT = T + xT + xT.

2) Исключение из мира n раз одного и того же объекта не изменяет этот мир:

T — xT — xT = T — xT.

3) Исключённым из мира может быть только объект, находящийся в мире:

T + xT — xT = T.

4) Осознание независимых объектов порождает независимые модели:

x(T + yT) = xT + xyT.

5) Операция осознания не обладает свойством коммутативности:

xT № Tx.

6) Операции расширения мира *и исключения из мира обладают свойством коммутативности:*

*xT + yT = yT + xT.*

Представим ситуацию, когда у объектов, находящихся в мире, поочередно наступает процесс осознания мира:

1) $W_1 = T$;

2) $W_2 = T + xT$;

3) $W_3 = T + xT + y(T+xT)$.

Попытаемся описать динамику изменения мира, используя **операторы преобразования** мира*, которые включают в себя:

оператор осознания;

оператор расширения мира;

оператор исключения из мира.

*В работах В.А. Лефевра был введён лишь один оператор, который он назвал оператором сознания.

Очевидно, для того чтобы были возможны представленные чуть выше поочередно наступающие изменения мира, достаточно дважды применить операцию осознания в виде:

• переход от мира №1 к миру №2 — $W_2 = (1+x)W_1$,

• от мира №2 к миру №3 — $W_3 = (1+y)W_2$.

В дальнейшем при формировании стратегии информационного противоборства факт применения объектом x к миру $W_1$ оператора преобразования мира w в момент времени $t_1$ с затратой ресурсов в размере $r_1$ будем записывать в виде:

$x, t_1, r_1 \Rightarrow W_1: W_2 = wW_1$.

Появление в мире нового информационного объекта, нового сообщения будем фиксировать в виде:

$x, t_1, r_1 \Rightarrow W_1: W_2 = W_1 + w$.

Исключение объекта из мира:

$x, t_1, r_1 \Rightarrow W_1: W_2 = W_1 - w$.

Подобный формализм легко может быть спроецирован практически на любой язык программирования. Для этого достаточно поставить в соответствие введённым операторам имена функций и определить для них формальные параметры.

Опираясь на введённый формализм, возможно провести классификацию информационных систем в зависимости от частоты применения ими различных операторов преобразования мира (ОПМ).

Так, В.А. Лефевр выделяет следующие классы “замкнутых” информационных объектов в зависимости от предпочтения тем или иным операторам осознания:

1) информационные объекты, предпочитающие использовать оператор $1+x+xy$ “обречены исповедовать принцип максимина”, т.е. их внутренний мир устроен таким образом, что они считают, будто бы любая модель, в том числе и модель самого себя имеется и у противника. Поэтому, для того чтобы ввести в заблуждение противника, требуется при выборе поступка использовать случайный механизм типа бросания костей. Лефевр показал, что применение данного оператора оставляет мир практически неизменным, что оператор $1+x+xy$ порождает “особое **рефлексивное замыкание**” При этом процесс изменения мира может развёртываться через операторы преобразования мира без какой бы то ни было информации, поступающей извне*.

*В.А. Лефевр считает, что подобного типа оператор преобразования мира лежит в основе некоторых типов религиозного мышления. Например, Бог (y) является субъектом, контролирующим любую мысль субъекта x. “Это может приводить к парадоксальным и тяжёлым для верующего состояниям, когда он полагает себя неверующим, но это полагание в силу автоматической работы оператора мажорируется. Бог продолжает присутствовать во внутреннем мире”.

2) информационные объекты, отдающие предпочтение оператору $1+x_2$, обречены вступать в отношения с реальностью как с элементом своего внутреннего мира.

3) информационные объекты, предпочитающие оператор $1+xy$, опираются в своём поведении на мир, лежащий внутри другого персонажа.

Оператор w порождает **рефлексивное замыкание**, если в ходе его применения структура исходного выражения W, описывающего мир, не меняется. Например, пусть:

$w=1 + x + xy$;

$W = T + x(W_1 + yW_1)$.

Тогда:

$(1+x+xy)\ W = T + xW_1 + xyW_1 + xW + xyW = T + x\ ((W_1+W) + y(W_1+W)) = T + x(W_3 + yW_3)$.

Было показано, что, применяя к описанию мира W последовательность операторов преобразования мира, можно перевести этот мир в определённое состояние. В общем виде задача информационного агрессора именно в этом и заключается: перевести мир $W_1$ в такое состояние $W_2$, которое полностью устраивает агрессора.

Поэтому цель применения данного формализма заключается в решении задач, типа:

$W_1$ исходный мир;

$W_2$ заданный (конечный) мир;

$w_1, w_2, \ldots w_n$ операторы преобразования мира.

Требуется определить $w_1, w_2, \ldots w_n$ для решения задачи:

$W_2 = w_n\ w_{n-1}\ w_{n-2}, \ldots\ w_1\ W_1$.

При этом операторы преобразования мира должны располагаться в строгой временной последовательности. В начале $w_1$, затем $w_2$, а в заключение $w_n$.

Понятно, что в общем виде такую задачу не решить, а её решение, как правило, обладает неоднозначностью, т.е. всегда существует несколько различных последовательностей

операторов преобразования мира, позволяющих получить требуемый результат. Если каждую последовательность действий рассматривать в качестве алгоритма (информационной стратегии), то всё множество последовательностей по сути своей образует множество эквивалентных алгоритмов. Задача разработчика стратегии информационной войны заключается в выборе такой последовательности, которая дешевле реализуется и позволяет максимально быстро "загнать" противника в требуемое состояние. При этом применение операторов изменения мира должно быть настолько динамичным, чтобы противник не успевал за отпущенное ему время изменить состояние мира, т.е. не мог помешать применению следующего оператора из последовательности, принадлежащей разработанной стратегии. Информационные сражения в чём-то близки шахматным поединкам, там тоже есть набор состояний, после попадания в которые дальнейшая игра между равноправными противниками превращается в игру "в одни ворота"

***Источники данных для модели информационного объекта***

Построение модели, способной прогнозировать поведение информационной самообучающейся системы, являющейся противником, предполагает применение собственного оператора осознания (х) к противнику (у) хуТ, к модели мира и к модели себя, созданной противником хухТ + хухуТ и т.д.

Начало этого процесса лежит в организации сбора данных о противнике. Данные, собранные с помощью спецслужб и любых других источников, проверяются на достоверность и в качестве "строительного материала" идут на создание модели противника. На рис. 3, этот канал сбора данных обозначен как "канал №1"

Однако в силу того, что противник является информационной самообучающейся системой, он сам заинтересован в сборе данных. Поэтому любая информация, которая будет сообщена противнику, безо всякой проверки на достоверность может быть использована для создания его модели ("канал №2"). В процессе проектирования модели не так важно, о чём эта информация, важно лишь, что после акта передачи информации игрок, сделавший это, становится обладателем информации о своём партнёре*, т.е. информационные противники самостоятельно формируют друг у друга желательные модели мира, в том числе модели самих себя.

*Лефевр В.А. Конфликтующие структуры. М.: Сов. радио, 1973.

В современных условиях, когда применение информационного оружия стало наиболее эффективным средством воздействия на противника, именно "канал №2" начинает играть определяющую роль при построении прогнозной модели. Вести техническую и агентурную разведку (канал №1) дорого и опасно, в то время как производство и распространение информации (канал №2) дёшево, а при желании еще и анонимно.

В сказанном отчётливо проявляется наступательный характер информационных войн, ведущихся в мире. Отсюда следует, что объём информации, целенаправленно передаваемый от одного противника к другому, вполне можно рассматривать и оценивать как меру информационной агрессивности. При этом не важно, какой характер имеет передаваемая информация, важно, что потребитель чем больше потребляет, тем всё более и более осознаётся (моделируется), а значит и управляется своим информационным противником.

К осмыслению подобного утверждения надо подходить с иными, непривычными мерками и исходить из того, что в эпоху информационных технологий, когда социальная среда перенасыщена информацией, безопасность системы начинает определяться уже не только теми знаниями, которые данная система получает о противнике, но и, может быть, даже в первую очередь теми знаниями, от восприятия которых ей удалось уклониться*.

*Расторгуев С.П. Информационная война. М.: Радио и связь, 1998.