УНИВЕРСИТЕТ ИТМО

А.А. Воробьева, В.М. Коржук

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЕДУЩИХ ЗАРУБЕЖНЫХ СТРАНАХ

Часть 1

Учебно-методическое пособие

Санкт-Петербург
2019

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.А. Воробьева, В.М. Коржук

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЕДУЩИХ ЗАРУБЕЖНЫХ СТРАНАХ

Часть 1

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки 10.03.01 Информационная безопасность
в качестве учебно-методического пособия для реализации основных профессиональных образовательных программ высшего образования бакалавриата

Санкт-Петербург
2019

Воробьева А.А., Коржук В.М. **Системы защиты информации в ведущих зарубежных странах**. **Часть 1.** Учебно-методическое пособие.– СПб: Университет ИТМО, 2019.– 36 с.

Рецензент: Созинова Екатерина Николаевна, кандидат технических наук, доцент факультета безопасности информационных технологий, Университета ИТМО.

Учебное пособие разработано для методической помощи бакалаврам, обучающимся по направлению подготовки 10.03.01 – «Информационная безопасность».
В пособии рассмотрены вопросы обеспечения информационной безопасности в зарубежных странах на национальном уровне. Предложены практические задания для изучения систем защиты информации в зарубежных странах, основополагающих нормативно-правовых документов в данной области, а также современных информационных войн, информационного противоборства, информационного воздействия и противодействия. Сформулированы рекомендации по изучению документов ведущих зарубежных стран, устанавливающих государственную политику и стратегию в области информационной безопасности, рекомендации по анализу информационных сообщений в современных средствах массовой информации и коммуникации с точки зрения определения наличия в них признаков манипулирования мнением. Изучаются документы зарубежных стран в области информационных и кибервойн, существующие системы информационной безопасности зарубежных стран (США, страны ЕС) и РФ по обеспечению противодействия информационно-психологическим воздействиям через средства массовой информации и коммуникации.
Учебное пособие может быть рекомендовано бакалаврам, осуществляющим подготовку по направлению «Информационная безопасность», руководителям и специалистам информационных, юридических служб, IT подразделений и подразделений по технической защите информации.

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ **3**

ВВЕДЕНИЕ **4**

ПРАКТИЧЕСКАЯ РАБОТА №1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА **8**

ПРАКТИЧЕСКАЯ РАБОТА №2. МЕТОДЫ И СРЕДСТВА ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА И ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ И ИСПОЛЬЗУЕМЫЕ В СОВРЕМЕННЫХ СМИ И СМК **12**

ПРАКТИЧЕСКАЯ РАБОТА №3. ФАКТОЛОГИЧЕСКИЙ АНАЛИЗ ИНФОРМАЦИОННЫХ СООБЩЕНИЙ ДЛЯ ВЫЯВЛЕНИЯ ПРИМЕНЕНИЯ МЕТОДОВ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ **15**

ОПИСАНИЕ ПРОВЕДЕНИЯ СЕМИНАРОВ **20**

ПЕРЕЧЕНЬ КОНТРОЛЬНЫХ ВОПРОСОВ **23**

ВОПРОСЫ ДЛЯ САМОСТОЯТЕЛЬНОГО ОЗНАКОМЛЕНИЯ **24**

РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА **25**

ПРИЛОЖЕНИЕ 1. ПЕРЕЧЕНЬ СРЕДСТВ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ НА МАССОВОЕ И ИНДИВИДУАЛЬНОЕ СОЗНАНИЕ **28**

ВВЕДЕНИЕ

Основная проблема в обеспечении информационной и кибербезопасности (ИБ и КБ) в глобальном масштабе кроется в необходимости соблюдения баланса между безопасностью и правом на частную жизнь, свободу слова, беспрепятственный обмен информацией. Такой баланс может быть соблюден только с принятием актуальных и действенных законодательных норм. Повышение уровня безопасности и защищенности всегда ведет к снижению приватности, что часто трактуется обществом как нарушение гражданских свобод.

В отношении данной проблемы существует две основные точки зрения, разделяемые разными странами. Взгляды на информационное воздействие и информационные войны у этих стран отличаются, что приводит к постоянным спорам и разногласиям на различных международных форумах (например, на заседаниях ассамблеи ООН).

К первой группе в соответствии с точкой зрения относятся страны, *выступающие за «свободный Интернет» и декларирующие необходимость свободного движения информации*.

Ко второй группе относятся страны, *подчеркивающие необходимость соблюдения информационного суверенитета государства* и, как следствие, выступающие за *введение государственного или международного контроля*. Эти страны рассматривают Интернет как угрозу национальной безопасности. Бесконтрольное Интернет-пространство может таить в себе угрозы существующему политическому устройству и стабильности, учитывая множество случаев, когда так называемые «цветные революции» организовывались с использованием Интернета, социальных сетей и новых технологий связи (в обход обычных операторов). Более того, часто *опасной* считается возможность осуществления информационного воздействия на население вследствие свободного обмена информацией.

На международном, национальном и государственном уровнях существует ряд глобальных угроз безопасности в информационном пространстве. Такие угрозы представляют опасность на всех уровнях организации общества: от индивидуума до государства и мирового сообщества.

На национальном уровне выделяются следующие угрозы:

1. Угрозы киберпреступности.
2. Угрозы кибертерроризма.

На международном уровне можно выделить следующие угрозы:

1. Угрозы информационных и кибервойн.
2. Угрозы кибершпионажа.

На сегодняшний день во многих странах, в частности в США, Интернет (киберпространство) признается таким же полноценным пространством, как воздушное, водное и космическое пространство, и является сферой стратегических и военных интересов. В военных стратегиях и доктринах (стратегии министерства обороны, стратегии национальной безопасности) описывается последовательность шагов, необходимых для обеспечения стратегического преимущества и стабильности в киберпространстве.

Стандартная типовая схема систем защиты информации, применяемая в общемировой практике, представляет собой совокупность ряда взаимосвязанных элементов, действующих на различных уровнях:

1. Международный уровень: правовые меры (международные нормативные и правовые акты).

2. Национальный уровень: правовые меры (национальное законодательство и стандарты, моральные нормы и правила).

3. Уровень информационных систем (ИС): организационная защита информации (ЗИ), техническая и физическая ЗИ, криптографическая ЗИ, программно-аппаратная ЗИ.

В данном учебном пособии основной акцент сделан на изучении ряда национальных и международных правовых документов зарубежных стран, затрагивающих вопросы противодействия угрозам национальной безопасности, таким как кибертерроризм и угрозы информационных и кибервойн. В процессе выполнения практических заданий студенты изучают основные регламентирующие документы стран Европейского союза и Соединенных Штатов Америки в области информационного противоборства и противодействия терроризму и кибертерроризму в открытых сетях; проводят сравнительный анализ подходов и практик противодействия информационно-психологическому воздействию в Российской Федерации и в ведущих зарубежных странах; учатся применять критическое мышление к анализу и интерпретации информационных сообщений современных средств массовой информации и коммуникации (СМИ и СМК).

Информационная война (ИВ, англ. Information Warfare) или *информационное противоборство* – межгосударственное противоборство в информационном пространстве с целью:

- нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам;
- подрыва политической, экономической и социальной систем;
- массированной психологической обработки населения для дестабилизации общества и государства;

- принуждения государства к принятию решений в интересах противоборствующей стороны [1].

Информационное воздействие – воздействие, осуществляемое с применением информационного оружия, то есть таких средств, которые позволяют осуществлять с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия [2].

Информационно-психологическое воздействие (ИПВ) – целенаправленное производство и распространение специальной информации, оказывающей непосредственное влияние (положительное или отрицательное) на функционирование и развитие информационно-психологической среды общества, психику и поведение населения, руководство страны, военнослужащих. ИПВ включает комплекс специальных психологических операций, мероприятий и акций, проводимых с помощью информации, пропаганды и агитации, подготовленной соответствующим образом и доводимой до объекта (групп объектов) воздействия с помощью различных форм психологического воздействия (печатными средствами, радио– и телевещанием, изобразительными средствами, через непосредственное общение, материальными акциями, через информационные компьютерные сети). Отдельно выделяют *негативное ИПВ*, под которым понимается «сознательно инициируемое влияние (внушение), провоцирующее личностную и социальную напряженность, снижение степени организованности, искажение нравственных критериев и норм, влекущее снижение морально-психологического состояния…» [3].

В предлагаемом пособии представлен цикл практических работ, выполняемых в рамках первой части курса «Системы защиты информации в ведущих зарубежных странах» для основных профессиональных образовательных программ высшего образования бакалавриата по направлению подготовки 10.03.01 – «Информационная безопасность».

Для выполнения работ, представленных в пособии, необходимо изучение теоретического материала по тематикам программы дисциплины, в том числе лекционных материалов и материалов для самостоятельного изучения. Дисциплина включает два цикла практических работ, направленных на приобретение практических умений и навыков.

Первая часть учебно-методического пособия содержит цикл из трех практических работ, связанный со способностью осознавать и анализировать глобальные угрозы безопасности в информационном пространстве: угрозы киберпреступности, угрозы кибертерроризма, угрозы информационных и кибервойн, угрозы кибершпионажа; оценивать общую ситуацию в области защиты информации в зарубежных странах; осознавать социально-экономические и культурные особенности зарубежных стран,

оказывающие влияние на состояние обеспечения государственной информационной безопасности, а также владеть навыками анализа нормативно-правовых документов зарубежных стран в области информационного противоборства, кибертерроризма, информационных и кибервойн; способностью производить фактологический анализ информационных сообщений современных СМИ различных зарубежных стран, выделять факты, определять применяемые методы информационного воздействия.

В соответствии с описанными в пособии рекомендациями студенты выполняют практические работы в малых группах (командах) по 3–4 человека. Процесс работы представляет собой совместную разработку решений и очную защиту отчетов. Работа ведется в соответствии с вариантом задания и направлена на решение общей задачи путем творческого сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности. В результате работы каждая команда совместно представляет публичный доклад. После доклада выступающие отвечают на вопросы преподавателя и студентов-слушателей.

Часть занятий представляют собой занятия типа «case-study» – анализ и разбор реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений. Для выполнения заданий такого типа необходимо заранее (до начала занятия) ознакомиться с методическими указаниями, рекомендованными источниками литературы по данной теме. Кроме этого, необходимо качественно интерпретировать итоги выполнения практической работы, а также подготовиться к ответу на контрольные вопросы. Во время работы рекомендуется активно участвовать в обсуждении и формировании решения для поставленного задания, по итогам проанализировать процесс работы и полученные результаты и выявить ошибки.

Занятия типа «семинар» проводятся на основе разработанного плана, по вопросам которого готовится вся учебная группа. Группа докладчиков совместно готовит реферат, презентацию и доклад по теме семинара. После доклада участники семинара задают вопросы, на которые отвечает выступавшая группа докладчиков.

Самостоятельная работа студентов (СРС) по дисциплине играет важную роль в ходе всего процесса обучения с целью усвоения материала дисциплины. В ходе СРС студенты изучают теоретические материалы, основную и дополнительную литературу, готовят и оформляют реферат, готовятся к докладу и презентации.

Практическая работа №1. Информационная безопасность в системе национальной безопасности государства

Форма проведения:

семинар.

Цель работы:

изучить основные направления обеспечения информационной безопасности как составляющей национальной безопасности в ведущих зарубежных странах в условиях информационного противоборства.

Задачи:

- изучить понятия и сущность информационной войны, информационного противоборства, информационного оружия, его видов, функций и возможностей,
- изучить основные документы, определяющих политику государства в области национальной безопасности в условиях информационной войны и информационного противоборства с целью определения национальных интересов, угроз безопасности государства, источников угроз, основных направлений обеспечения информационной безопасности ведущих зарубежных стран.

Описание:

Методы исследования: теоретическое исследование (поиск, сбор, группировка и анализ информации по теме работы).

Ход выполнения:

Задание для докладчиков:

1. Изучить основные понятия информационной войны, информационного противоборства, их формы, основные черты и особенности. Объяснить сущность понятий: информационная война, информационное противоборство, модели и методы ведения информационных войн.

2. Изучить классификацию, типологию, историю и эволюцию системы ведения информационных войн.

3. Ознакомиться с видами и функциями информационного оружия[1]. Изучить его классификацию, возможности, возможные объекты нападения.

4. Изучить историю развития и применения типов информационного оружия в конфликтах второй половины XX–начала XXI века. Проанализировать современный уровень развития информационного оружия.

5. Изучить информационное противоборство на межгосударственном уровне. Определить возможные субъекты, цели, составные части и методы информационного противоборства на межгосударственном уровне.

6. Изучить компьютерную систему как объект информационного воздействия (с помощью информационного оружия). Изучить и описать методы нарушения конфиденциальности, целостности и доступности информации ***как угроз национальной безопасности***.

7. Изучить основные документы, определяющие политику государства в области национальной безопасности, следующих стран:

   a. Стран Европейского союза: «EU strategic communication to counteract anti-EU propaganda by third parties» [7], «An Open, Safe and Secure Cyberspace» [8].

   b. США (The National Security Strategy) [9].

8. На основании каждого их приведённых документов определить:

   a. угрозы безопасности, существующие на уровне страны или нации (объекты и угрозы информационной войны);

   b. источники угроз (внешние и внутренние);

   c. национальные интересы (в том числе их основные составляющие) и угрозы информационной безопасности в информационной сфере;

   d. основные направления обеспечения информационной безопасности государства, в том числе технических объектов информационной сферы государства в условиях информационной войны.

9. Произвести сравнение и анализ указанных выше документов между собой и с Доктриной информационной безопасности Российской Федерации. Выявить общие черты и отличия.

[1] Здесь под информационным оружием понимается комплекс средств и технологий, предназначенных для получения контроля над информационными ресурсами противника и вмешательства в работу компьютерных и информационных систем (в том числе управления и разведки), аппаратного и программного обеспечения в целях выведения их из строя, нарушения процесса нормального функционирования, получения или модификации содержащихся в них данных, а также целенаправленного продвижения выгодной информации. В рамках данной практической работы методы информационно-психологического воздействия подробно не рассматриваются.

Вопросы для обсуждения на семинаре:

В начале занятия дайте ответы на следующие вопросы:

1. Вспомните пример информационной войны или применения информационного оружия. Как вам кажется, какие цели преследовались исполнителями, были ли они достигнуты?

2. Какого рода атаки на государственные компьютерные системы могут повлиять на вас и каким образом?

После доклада необходимо разбиться на группы и выполнить следующие задания:

1. Определите влияние информационных войн на индивидуальное и массовое сознание, на человека и общество.

2. Проанализируйте одну из известных атак на государственные информационные системы, определите цели атаки, мотивы атаки, методы проведения.

3. Определите основные направления обеспечения информационной безопасности государства, в том числе технических объектов информационной сферы государства в условиях информационной войны.

Содержание реферата, доклада, презентации:

1. Определение понятий информационной войны, информационного противоборства, их основные черты и особенности, модели и методы ведения. Классификация и типы информационных войн.

2. Описание видов и функций информационного оружия, его классификация, возможности, возможные объекты нападения.

3. Примеры применения информационного оружия в конфликтах второй половины XX–начала XXI века.

4. Современный уровень развития информационного оружия.

5. Описание субъектов, целей и методов информационного противоборства на межгосударственном уровне.

6. Описание компьютерной системы как объекта информационного воздействия, методов нарушения конфиденциальности, целостности и доступности информации как угрозы национальной безопасности.

7. Перечень проанализированных документов, определяющих политику и стратегию государств в области национальной и информационной безопасности.

8. Выявленные угрозы информационной и кибербезопасности, существующие на уровне страны или нации (объекты и угрозы информационной войны). Приводится для каждого государства.

9.Выявленные источники угроз (внешние и внутренние). Приводится для каждого государства.

10. Национальные интересы и угрозы информационной безопасности в информационной сфере. Приводится для каждого государства.

11. Результаты сравнения (по пунктам 7–9) и анализа (в табличной форме) документов, определяющих политику и стратегию государств в области национальной и информационной безопасности.

12. Перечень использованных информационных источников, оформленный в соответствии с требованиями ГОСТ 7.1-2003 (краткая библиографическая запись).

Рекомендованная литература: [4–11].

Практическая работа №2. Методы и средства информационного противоборства и информационно-психологического воздействия и используемые в современных СМИ и СМК

Форма проведения:

семинар.

Цель работы:

изучить методы и средства информационного противоборства и информационно-психологического воздействия, используемые в современных СМИ и СМК.

Задачи:

- изучить угрозы информационно-психологического воздействия, определить каналы реализации угроз;
- изучить средства информационно-психологического воздействия и средств манипулирования мнением.

Описание:

Методы исследования: теоретическое исследование (поиск, сбор, группировка и анализ информации по теме работы).

Ход выполнения:

Задание докладчикам:

1. Изучить основные понятия информационно-психологического воздействия и противодействия, их формы, основные черты и особенности.

2. Изучить виды и механизмы информационно-психологического воздействия на сознание и поведение личности, общества и государства. (в том числе на лица, принимающие решения) [10].

3. Изучить методы информационно-психологического воздействия и манипулирования мнением (на уровне массового и индивидуального сознания).

4. Выявить угрозы информационно-психологического воздействия для личности, общества, государства на основе литературных источников, собственных наблюдений и рассуждений.

5. Выявить коммуникативные каналы, по которым возможна реализация угроз.

6. Изучить системы информационной безопасности зарубежных стран (США, страны ЕС) и РФ по обеспечению противодействия информационно-психологическим воздействиям через СМИ и СМК.

Вопросы для обсуждения на семинаре:

В начале занятия дайте ответы на следующие вопросы:

1. Вспомните хотя бы один пример информационно-психологического воздействия и манипулирования мнением. Какой из подобных фактов произвел на вас наиболее сильное впечатление, изменил ваше мнение в некотором вопросе? Почему это произошло?

2. Испытываете ли вы сложности в выявлении истинного смысла некоторого информационного сообщения, определении цели автора? Легко ли выделять факты в современных информационных сообщениях?

3. Какая тематика в современных СМИ вас интересует с точки зрения отделения фактов от «вымысла»?

После доклада необходимо разбиться на группы и выполнить следующие действия:

1. Провести сравнительный анализ опыта РФ и ведущих зарубежных стран в области противодействия информационно-психологическому воздействию.

2. Определить методы противодействия информационно-психологическому воздействию (методы информационно-психологического противодействия), методы защиты личности от информационно-психологических воздействий в СМИ и СМК.

3. Сформулировать предложения по решению проблем, вызванных негативным влиянием информационных войн.

4. Разработать предложения и рекомендации по совершенствованию действующей политики РФ и государственной политики в информационной сфере с учетом международного опыта.

Содержание реферата, доклада, презентации:

1. Описание существующих техник информационно-психологических воздействия [12–15].

2. Выявленные угрозы информационно-психологического воздействия для личности, общества, государства.

3. Перечень коммуникативных каналов реализации угроз.

4. Перечень методов информационно-психологического воздействия на массовое и индивидуальное сознание и их описание (убеждение, суггестивные и информационно-техногенные методы и средства и так далее).

5. Перечень средств информационно-психологического воздействия на массовое и индивидуальное сознание и их описание, примеры применения этих средств в СМИ и СМК (см. Приложение 1).

6. Описание систем информационной безопасности ведущих зарубежных стран и РФ по обеспечению противодействия информационно-психологическим воздействиям через СМК.

7. Перечень использованных информационных источников, оформленный в соответствии с требованиями ГОСТ 7.1-2003 (краткая библиографическая запись).

Рекомендованная литература: [5, 7, 9–18].

Практическая работа №3. Фактологический анализ информационных сообщений для выявления применения методов информационно-психологического воздействия

Форма проведения:

самостоятельное решение проблемной задачи.

Цель работы:

провести фактологический анализ информационных сообщений СМИ и СМК.

Задачи:

- изучить методы и средства информационно-психологического воздействия, используемые в СМИ и СМК;
- изучить методы фактологического анализа;
- проанализировать информационные сообщения СМИ и СМК.

Краткая теоретическая справка:

Любой текст может включать три основных компонента, важно верно определить каждый из этих компонентов:

- факты, касающиеся новости или возникшей проблемы;
- приемы эмоционального воздействия на аудиторию (на логико-понятийном или понятийно-образном уровне);
- фрагментарное или обстоятельное осмысление ситуации.

Методы информационно-психологического воздействия всегда идут от факта к мотивации. Методы противодействия направлены на «снятие надстроек» над фактами и выработку независимой оценки. Базовая схема искажения фактов представлена на рисунке 1.

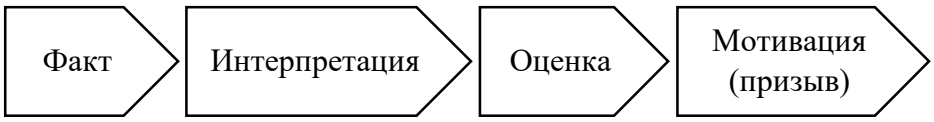

Рисунок 1 – Схема искажения фактов в информационных сообщениях

Снятие ложной мотивации – вопрос «почему?». Снятие ложной оценки – вопросы: «почему так решили, по какой причине?» (возврат к интерпретации факта); «насколько компетентен/искушен в вопросе тот, кто оценивает?» (анализ субъективности). Наличие в тексте большого количества эпитетов, эмоциональной окраски является указанием на то, что

факты искажены ложной оценкой. Также возможно искажение оценки некомпетентностью, непрофессионализмом или предубежденностью; некоторое мнение принадлежит случайному субъекту, далее это мнение выдается за экспертное.

Снятие ложной интерпретации факта – вопрос «можно ли посмотреть на тот же факт по-другому?».

Анализ фактов – вопросы: «кому выгодно освещение данных фактов? кто получает прибыль от освещения факта?».

Описание:

Работа выполняется в группах по 2–3 человека. Тексты информационных материалов (сообщений) прилагаются к отчету по работе.

Методы исследования: теоретическое исследование (поиск, сбор, группировка и анализ информации по теме работы).

Ход выполнения:

1. Изучите особенности информационных атак в современных СМИ, в том числе в СМК (социальные сети, форумы и пр.) – вбросы, дезинформация и пр.
2. Приведите перечень средств информационно-психологического воздействия и манипулирования мнением и их описание (ложные авторитеты, сокрытие фактов, использование ярко выраженной эмоциональной окраски и пр.). При составлении перечня рекомендуется ориентироваться на учебное пособие [19] и материалы в приложении 1.
3. Выберите некоторое событие (информационный повод), вызвавшее активные обсуждения, дискуссии в СМИ и СМК, по тематике которого велось активное информационное противоборство.
4. Для события в целом определите заинтересованные стороны, цели, сценарии, используемые методы информационно-психологического воздействия.
5. Отберите два информационных сообщения, размещенных в СМИ и/или СМК разными сторонами противоборства, на тему события, выбранного в п.4.
6. Проведите фактологический анализ данных сообщений.
7. Приведите признаки применения средств ИПВ и манипулирования мнением, обнаруженные вами в информационных сообщениях.
8. Составьте блок схему алгоритма анализа сообщения и дерево принятия решений о наличии ИПВ в информационном сообщении.

Порядок проведения анализа:

1. Определить характеристику канала коммуникации, СМИ/СМК и влияние их специфики на текст (направленность издания, интересы и потребности аудитории).

2. Дать характеристику текста с точки зрения его содержания: тема, замысел, идея как воплощение целевой установки.

3. Определить отношение автора к тематике сообщения.

4. Определить виды информации, использованной в тексте: описательная (фактологическая), оценочная (рефлексивная), нормативная, приведите обоснование.

5. Определить факторы, которые оказывают решающее влияния в организации фактического материала, выборе форм предъявления фактов и системы доказательств:

- назначение, функция, целевая установка текста – сообщить новость, рассказать о событии, явлении, проанализировать ситуацию, создать некоторый образ личности и прочие;
- объект отображения – область реальной действительности, которой касается сообщение или которую исследует автор статьи;
- предмет отображения и фактическая основа – факт (информационный повод – «жесткая» или «мягкая» новость), ситуация, проблема, человек (а также факт, событие, явления, процессы, ситуации, сообщения СМИ, книги, фильмы – информационные явления, дающие повод для подготовки рецензий, обзоров).

6. Определить источники информации, которыми пользовался автор, и методы работы с информацией на уровне сбора и осмысления:

- источники информации (предметно-вещественная среда, информационная среда, человек, документальные источники, базы данных, интернет-источники, социологические данные, научные факты и пр.)
- методы сбора информации (наблюдение, проработка документов, интервью, эксперимент), ее анализа и интерпретации:

a. общенаучные процедуры (группировка, классификация, систематизация и типологизация),

b. общенаучные методы (анализ, синтез, индукция, дедукция, аналогия, сравнение и т.д.).

7. Описать способы объяснения факта (фактов):

- выяснение частей факта и связей между ними;

– выяснение необходимых условий и обстоятельств существования факта (фактов);

– установление причины факта (фактов);

– обнаружение действий, которые данный факт (факты) производит на окружающее.

8. Определить систему аргументации:

- фактологические аргументы – научные (законы, принципы науки, научные эмпирические факты и законы) и документальные факты, полученные в процессе обыденного наблюдения действительности журналистом или иными людьми (результаты личного наблюдения, свидетельства, полученные от очевидцев или других лиц, учреждений, документальные данные);
- ценностные аргументы – оценки с предъявляемым аудитории основанием (внешние и внутренние, то есть оценки без предъявления аудитории их оснований (скажем, «это плохая пьеса»).

9. Определить роль иллюстративного материала (фото, рисунки, шаржи, диаграммы, схемы, информационная графика, линейки и другие графические элементы). Качество аудио- и видеоряда в электронных СМИ, характеристика навигационных элементов в сетевых СМИ.

10. Дать характеристику взаимоотношений с получателем информации, определить цели публикации (отсутствие или наличие обратной связи, способы воздействия на собеседника). Цели публикации могут быть различными, предусматривающими или не предусматривающими определенное воздействие. Воздействие может быть результатом объективного информирования или информационно-психологического воздействия (манипулирование мнением или дезинформация).

11. Определить методы и средства информационно-психологического воздействия.

12. Проанализировать текст с точки зрения искажения фактов. Дать ответы на вопросы, приведенные в теоретической справке.

Содержание отчета:

1. Выявленные угрозы информационных войн и информационно-психологического воздействия для личности, общества, государства.

2. Перечень коммуникативных каналов реализации угроз.

3. Перечень средств информационно-психологического воздействия на массовое и индивидуальное сознание и их описание.

4. Описание современных форм ведения информационных войн на основе одного выбранного события.

5. Цели, сценарий, использованные методы и средства информационно-психологического воздействия.

6. Фактологический анализ информационных сообщений СМИ и СМК различных сторон конфликта.

7. Выявленные использованные средства информационно-психологического воздействия.

8. Признаки применения средств ИПВ и манипулирования мнением, обнаруженные вами в информационных сообщениях.

9. Блок-схема алгоритма анализа сообщений и дерево принятия решений о наличии ИПВ в информационном сообщении.

10. Выводы по работе, включающие предложения по противодействию информационно-психологическому воздействию на уровне личности.

11. Перечень использованных информационных источников.

Защита работы проходит в форме защиты отчета.

Варианты заданий:

Необходимо самостоятельно произвести подбор событий и информационных сообщений СМИ и СМК и согласовать его с преподавателем.

Рекомендованная литература: [5, 7, 9–18].

ОПИСАНИЕ ПРОВЕДЕНИЯ СЕМИНАРОВ

Часть практических занятий проводится в виде семинара по теме занятия для систематизации теоретических и фактических знаний в определенном контексте (подготовка и презентация материала по определенной теме, обсуждение поставленных и возникающих вопросов, формулирование выводов и заключения).

На занятиях семинарского типа докладчики готовят реферат, презентацию и доклад по основной теме семинара.

После доклада все участники семинара задают вопросы, на которые отвечают докладчик и другие члены группы. Вопросы и ответы составляют центральную часть семинара. Оценивается качество реферата, качество доклада, качество презентации, активность в участии в работе семинара, качество ответов на вопросы.

Ход занятий:

Семинар (90 минут) состоит из 3 логических частей:

1. Доклад по центральной теме семинара, около 45 минут – группа докладчиков.
2. Вопросы аудитории по докладу – около 15–20 минут. Вопросы задают студенты и преподаватель.
3. Дискуссия. После ответов на вопросы происходит обсуждение по теме семинара (25–30 минут), разворачивается дискуссия по проблемам, поднятым в работе. Производится подведение итогов.

Описание заданий на семинар для всех групп участников:

Часть 1. Основная часть семинара

Группе докладчиков к занятию необходимо предоставить реферат, презентацию и подготовить общий групповой доклад. Важно, чтобы материалы разных авторов не повторялась ни в реферате, ни в ходе доклада. Контроль данного вопроса производит руководитель группы.

Реферат по центральной теме семинара заранее (за 2–3 дня до занятия) передается для ознакомления преподавателю.

Основная часть реферата состоит из разделов, написанных каждым участником группы (1 раздел – 1 автор). Каждый раздел, по сути, представляет собой микроисследование.

Презентация и доклад по теме семинара. Доклад носит характер полного аргументированного изложения центральной темы семинарского занятия. Излагают сущность исследования, защищаемой точки зрения, собственные позиции. Аргументируют, обосновывают, иллюстрируют позицию.

Часть 2 и Часть 3. Вопросы и дискуссия

В ходе семинара слушатели готовят вопросы докладчикам, которые они задают группе выступающих после доклада. Любой вопрос может быть переадресован слушателям семинара. Как известно, способность поставить вопрос предполагает подготовленность по соответствующей теме. Соответственно, чем основательнее подготовка, тем более глубокие и квалифицированные вопросы могут быть заданы. Поэтому все студенты к занятию готовят подборку современной литературы, новых книг, научных статей или новостей по теме семинара. Более того, рекомендуется подготовить перечень интересующих вопросы, относящиеся к теме семинара.

Активность слушателей поощряется и оценивается дополнительно. Для получения дополнительной оценки за семинар необходимо проявить активность в работе, изучить дополнительный материал и участвовать в дискуссии по подготовленным вопросам. Оценивается умение задавать продуманные, четко сформулированные дополнительные вопросы.

На основе вопросов и ответов разворачивается дискуссия.

В конце занятия производится подведение итогов, оценивается выступление докладчиков и остальных участников семинара. Оценивается продуктивность всей дискуссии, правомерность выдвинутых гипотез и предложений, сделанных выводов. Высказывается мнение о вкладе того или иного участника дискуссии в нахождение общего решения и т.д.

Оценка работы на семинаре:

Докладчики

Оценивается:

a. качество реферата в целом (логичность, последовательность, актуальность материала) – 0 / 3 / 4 / 5 – групповая оценка;
b. качество доклада в целом (логичность, последовательность, наличие выводов) – 0 / 3 / 4 / 5 – групповая оценка;
c. качество презентации в целом (логичность, последовательность, наличие выводов) – 0 / 3 / 4 / 5 – групповая оценка;
d. качество представленного материала – 0 / 3 / 4 / 5 – индивидуальная оценка;
e. качество доклада (доклад был произведен самостоятельно, представлен логично) – 0 / 3 / 4 / 5 – индивидуальная оценка;
f. качество презентации (помогает ли презентация в восприятии материала, содержит ли графический материал, наглядные изображения)– 0 / 3 / 4 / 5 – индивидуальная оценка;
g. активность в участии в работе семинара 0 / 3 / 4 / 5 – индивидуальная оценка;

h. качество ответов на вопросы 0 / 3 / 4 / 5 – групповая и индивидуальная оценка.

Остальные участники

Оценивается:

a. Активность в работе на семинаре 0 / 3 / 4 / 5 – индивидуальная оценка
b. Качество вопросов 0 / 3 / 4 / 5 – индивидуальная оценка

ПЕРЕЧЕНЬ КОНТРОЛЬНЫХ ВОПРОСОВ

1. Понятие кибертерроризма.
2. Понятие кибершпионажа.
3. Атаки на государственные ИС и ИС критически важных объектов.
4. Понятие информационной войны.
5. История информационных войн.
6. Основные черты и особенности информационной войны.
7. Модели и методы ведения информационной войны.
8. Информационное оружие. Виды и функции.
9. Возможные объекты нападения с применением информационного оружия.
10. Основы информационного противоборства.
11. Основы информационно-психологического воздействия. Основные каналы информационно-психологического воздействия.
12. Основы противодействия информационному воздействию.
13. Методы и средства информационно-психологического воздействия.
14. Угрозы информационно-психологического воздействия для личности, общества, государства.
15. Основные документы Российской Федерации и зарубежных стран в области противодействия угрозам национальной информационной безопасности: кибертерроризму и кибер- и информационным войнам, а также в области противодействия информационному воздействию.

ВОПРОСЫ ДЛЯ САМОСТОЯТЕЛЬНОГО ОЗНАКОМЛЕНИЯ

В данном разделе представлены дополнительные темы рефератов и статей. Перечень тем дополняется преподавателем.

1. Конкурентная разведка и информационная война (черный PR и методы противодействия, методы социальной инженерии).
2. Репутационные риски личности.
3. Репутационные риски общества (компании, банка).
4. Практические аспекты и способы минимизации репутационных рисков, применение специализированного ПО и сервисов.
5. Госизмена и сотрудничество со спецслужбами иностранного государства. Преступления и наказания.
6. Использование зарубежных банков лицами, имеющими доступ к государственной тайне.
7. Wikileaks: война с секретами.

РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

Основная литература:

1. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. — СПб., 2017.

2. Макаренко С.И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. №3. URL: https://cyberleninka.ru/article/n/informatsionnoe-oruzhie-v-tehnicheskoy-sfere-terminologiya-klassifikatsiya-primery (дата обращения: 24.11.2019).

3. Макаров В.Е. Политические и социальные аспекты информационной безопасности. Монография. – Таганрог: Изд–ль С.А. Ступин, 2015. – 349с.

4. Доктрина информационной безопасности Российской Федерации. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 02.10.18).

5. Государственная система защиты информации. URL: http://dehack.ru/gos_szi/ (дата обращения: 02.10.18).

6. Государственные стратегии кибербезопасности URL: http://www.securitylab.ru/analytics/429498.php (дата обращения: 02.10.18).

7. EU strategic communication to counteract anti-EU propaganda by third parties. URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0441+0+DOC+PDF+V0//EN (дата обращения: 02.10.18).

8. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (дата обращения: 02.10.18).

9. National Security Strategy Archive. URL: http://nssarchive.us/ (дата обращения: 02.10.18).

10. Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны [Электронный ресурс] : учебное пособие / А.В. Манойло, А.И. Петренко, Д.Б. Фролов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 340 с. — Режим доступа: https://e.lanbook.com/book/5175. — Загл. с экрана.

11. Ющук Е.Л. Боевой блоггинг-инструмент конкурентной разведки //Защита информации. Инсайд. – 2007. – №. 6. – С. 30–33. URL: https://yushchuk.livejournal.com/91386.html (дата обращения: 02.10.18).

12. Ющук Е.Л. Практика управления репутацией в Интернете. Я выиграл судебный процесс «Профессор Евгений Ющук против депутата Леонида Волкова» — по оскорблениям, которые депутат Леонид Волков позволил себе неоднократно в Живом Журнале и Твиттере. Пожалуй, Twitter впервые в отечественной практике стал доказательством в суде именно в процессе "Ющук против Волкова". URL: http://www.ru-ci.ru/Upravlenie-Reputatsiej-v-Internete-Sud-Informatsionnaya-vojna.html (дата обращения: 02.10.18).

13. Ющук Е.Л. Один из вариантов анализа информации в СМИ специалистом конкурентной разведки. URL: http://ru-ci.ru/Analiz_SMI.html (дата обращения: 02.10.18).

14. Ющук Е.Л. Публикации по теме Информационной войны. URL: http://ru-ci.ru/Contents_Info_War.html (дата обращения: 02.10.18).

15. Грачев Г.В., Мельник И.К. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия //М.: ИФ РАН. – 1999. – Т. 63. URL: http://www.globalmedia51.ru/old/50marketing21.pdf (дата обращения: 02.10.18).

16. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. URL: http://www.rus-lib.ru/book/32/Yrid_psihologiaj/Gracev/Gratev.htm (дата обращения: 02.10.18).

17. Зелинский С., Нагавкина Л.С., Фёдоров А. В. Информационно-психологическое воздействие на массовое сознание: средства массовой коммуникации, информации и пропаганды как проводник манипулятивных методик воздействия на подсознание и моделирования поступков индивида и масс. – Скифия, 2008. URL: http://i.сергейзелинский.рф/u/52/a5857ee75411e49c7fc71d237f39f2/-/Sergey%20Zelinskiy.%D0%98%D0%BD%D1%84%D0%BE-%D0%BF%D1%81%D0%B8%D1%85%D0%BE%20%D0%B2%D0%BE%D0%B7%D0%B4.pdf (дата обращения: 02.10.18).

18. Дзялошинский И.М., Дзялошинская М.И. Манипулятивные технологии в СМИ //Москва. – 2006.

19. Политология : учебник / под ред. М.А. Василика, И.Е. Тимерманиса. – М. : Проспект, 2013. – 618 с.

Дополнительная литература:

20. Аверченков В.И., Кондрашин Г.В., Рудановский М.В., Рытов М.Ю. Системы защиты информации в ведущих зарубежных странах: учебное пособие. М.: ФЛИНТА. 2011. 225 с. – Режим доступа: https://e.lanbook.com/book/44743

21. Малюк, А.А. Этика в сфере информационных технологий. [Электронный ресурс] / А.А. Малюк, О.Ю. Полянская, И.Ю. Алексеева. — Электрон. дан. — М. : Горячая линия-Телеком, 2011. — 288 с. — Режим доступа: http://e.lanbook.com/book/5172 — Загл. с экрана.

Приложение 1. Перечень средств информационно-психологического воздействия на массовое и индивидуальное сознание

Перечень средств информационно-психологического воздействия на массовое и индивидуальное сознание приведен из учебника: Политология : учебник / под ред. М. А. Василика, И. Е. Тимерманиса. – М. : Проспект, 2013. – 618 с.

Использование авторитетов (групп влияния)

Метод состоит в использовании авторитетных, известных для целевой аудитории людей или групп. В качестве таких групп влияния могут выступать известные политические деятели, деятели культуры, известные актеры, руководители предприятий, преподаватели высших и средних учебных заведений и т.д.

Для эффективности данного метода важно присутствие следующих факторов: доверие к представителю группы влияния, его известность, высокие профессиональные качества, личные достоинства, высокий официальный пост (в прошлом или настоящим), его близость с целевой группой электората и т.д. Как пример, негативные высказывания голливудских звезд против, тогда еще кандидата в президенты США, Дональда Трампа.

Утвердительные заявления

Метод состоит в распространении различных утверждений, которые представлены в качестве факта, при этом подразумевается, что эти заявления самоочевидны и не требуют доказательств. Эти утверждения могут быть как достоверными, так и нет.

Победившая сторона

В данном методе эксплуатируется желание людей быть на стороне победителя, аудитория убеждается в необходимости действовать так, чтобы оказаться «на выигравшей стороне», быть «как все». В избирательных кампаниях метод часто используется в виде следующих пропагандистских тем: «Кандидат N – кандидат номер один» или «Кандидат N – кандидат победитель», а также в закреплении темы «Все равно победит N». Например, в избирательной кампании по выборам главы исполнительной власти одного из регионов РФ одна из «избирательных команд» использовала сочетание «… состоятся выборы Президента N», закрепляя в

сознании электората связь между выборами Президента и фамилией действующего президента, создавая иллюзию его однозначной победы.

Принуждающая пропаганда

Данный тип воздействия использует слова и выражения, имеющие принуждающий характер. Например, в избирательных кампаниях часто используются листовки с лозунгом: «Голосуй за N» и «Выбери N».

Использование ценностных слов (относящихся к основным ценностям общества)

Метод состоит в использовании эмоционально интенсивных слов, которые тесно связаны с основными ценностями, мнениями общества и являются убедительными без дополнительной информации, и связывании их с необходимыми идеями или людьми. Данный метод апеллирует к таким чувствам, как любовь к стране, дому, желание мира, свободы, желание гордиться родиной и т.д. Для этого используются слова, связанные с такими понятиями, как дом, семья, дети, материнство, патриотизм, любовь, мир, счастье, здоровье, прогресс и т.д.

Например, в избирательной кампании в одном из регионов РФ для кандидата-женщины использовался лозунг «N – женщина-мать», который использовал эмоциональную окраску понятия материнства. В ходе исследования речей спикера палаты представителей Конгресса США Ньюта Гинрича (Newt Gingrich) было установлено, что для описания своей партии он использовал следующие положительно окрашенные слова: активность, создание, искренний, помощь, вызов, изменение, дети, выбор, граждане, убеждения, крестовый поход, обязанность, доверие, семья, свобода, работа, мечта, возможность, мир, благосостояние, защита, права, сила, успех, видение, реформы, социальное обеспечение и др.

Неопределенные выражения (положительно окрашенные)

Метод имеет много общего с методом «использования ценностных слов», но основан на использовании выражений с не уточненным смыслом. Аудитории предлагается возможность искать собственные интерпретации. Например, в избирательных кампаниях нередко встречаются лозунги «Я добьюсь правды (справедливости)», которые, несмотря на неясный, лишенный «конкретики» смысл в ряде случаев воспринимаются электоратом положительно.

Перенос положительного образа

Суть метода состоит в проекции позитивных качеств человека (авторитет, поддержка, престиж) или какого-либо объекта, предмета или моральных ценностей (индивидуальной, групповой, внутриорганизационной, национальной и т.д.) на другого человека или группу. Например, во время президентской избирательной кампании во Франции 1965 г. «избирательная команда» кандидата Жана Леканюэ создавала ему имидж «французского Кеннеди», перенося положительный образ Кеннеди на кандидата. В частности, для этого использовались плакаты с изображением кандидата и надписью «Завтра … Жан Леканюэ … новый человек … Франция в движении». «Такой же, как все, как мы».

Метод состоит в том, чтобы увеличить доверие той или иной аудитории, обеспечивая идентификацию того или иного человека или группу с этой аудиторией. Для этого кандидатов «очеловечивают». Например, в ходе кампании партии И. Рыбкина использовались телевизионные ролики с фотографиями его детства, студенчества, начала трудовой деятельности («такой же, как все мы»). Стандартным приемом при реализации метода являются съемки и фотографии кандидата в семье, с детьми, на природе, производстве, рассказ о хобби и т.д.

Наименьшее зло

Суть метода состоит в «мягком» признании того, что определенное лицо или курс является неприятным, но любой другой приведет к результатам намного худшим. Эта тема была одной из основных в избирательно кампании Президента РФ Б.Н. Ельцина в 1996 году. Во время масс-медиа войны «Чубайс-Березовский» в одной из газет была опубликована статья с заголовком «Двойка по поведению? Зато силен, шельмец, в арифметике», вместе с дополнительной информацией о профессионализме А.Б. Чубайса.

Упрощение проблемы

Многим людям не доставляет удовольствия долго разбираться в той или иной проблеме, а намного удобнее получить простой ответ на свои вопросы. С другой стороны многим непрофессионалам приятно услышать что, например, «юриспруденция – это просто опыт каждого человека, запутанный применением хитрых слов», а «современное искусство – просто чепуха», таким образом, люди потворствуют своему чувству превосходства и опасению признать, что эти области находятся вне их понимания. Суть метода упрощения состоит в использовании этих психологических особенностей человека. Сложные социальные, политические, экономические или военные проблемы сводятся к простым

интерпретациям. Например, в президентской избирательной кампании избирательная команда В.В. Жириновского использовала серию телевизионных роликов, в которых лидер ЛДПР «популярно» объяснял причину экономических проблем России.

Общественное неодобрение

Используется для создания иллюзии неодобрения тех или иных действий со стороны общественного мнения. Основная задача метода – создание негативного образа того кандидата или группы. Часто реализуется путем подбора различных высказываний «групп влияния», «представителей» различных слоев населения, различных социологических опросов и т.д.

Неопределенные выражения и намеки, несущие негативную окраску

При использовании данного метода аудитории предлагается возможность самой находить собственные интерпретации. Используется против отдельных людей, групп, идей и эксплуатирует общественные стереотипы и латентные подозрения. Часто используется в форме следующих намеков: «Ну, вы понимаете, на что обычно живут такие чиновники, как N».

Перенос неодобрения и негативного образа

Метод переноса неодобрения состоит в создании неодобрения тех или иных персон, действий или идей через демонстрацию тех групп, которые одобряют данные идеи или действия, поддерживают эти персоны, но относятся к числу имеющих низкое доверие, тех, которых боятся, ненавидят или презирают и др. Если группа, поддерживающая определенную политику, относится к числу подозрительных, презираемых или не вызывающих доверия, другие группы могут изменить свою позицию.

Метод переноса негативного образа состоит в проекции негативных качеств человека или какого-либо объекта, предмета или моральных ценностей (индивидуальной, групповой, внутриорганизационной, национальной, патриотической и т.д.) на другого человека или идею для того, чтобы дискредитировать его.

Например, во время избирательной кампании 1986 г. во Франции социалисты выпустили плакат с изображением волка с длинными зубами и надписью: «А почему, милые правые, у вас такие большие зубки?».

Другой пример: во время масс-медиа войны «Чубайс-Березовский», о которой уже упоминалось ранее, одна из статей, направленная против Б.А. Березовского, развивала следующую тему: «…чеченский командир

говорит: …почему бы не любить Березовского, он если и украдет, то не у нас, а у России… нам что-то достанется», также в статье приводились данные о близких отношениях Б.А. Березовского и А. Коржакова. Таким образом, происходит перенос отрицательного образа чеченского командира и А. Коржакова на Б.А. Березовского.

Наклеивание ярлыков

Метод аналогичен методу «перенос неодобрения и негативного образа» и состоит в эксплуатации предрассудков и стереотипов населения через «наклеивание ярлыка». Ярлык квалифицирует этот объект как что-то, чего аудитория боится, ненавидит, испытывает отвращение, находит подозрительным или нежелательным и др.

В России в качестве таких ярлыков в разное время использовались слова партократ, дерьмократ, коммуно-фашист, красно-коричневый и др. Уже упоминавшийся спикер палаты представителей США Ньют Гинрич для описания его оппонентов (демократической партии) использовал следующий набор негативных слов («ярлыков»): жалость, обман, принуждение, обвал, падение, коррупция, кризис, задержка, уничтожение, деструктивность, поглощение, ставить под угрозу, неудача, провал, некомпетентность, болезнь, предательство, бюрократия, тратить время, радикальность, ложь, лицемерие и др.

Использование пугающих тем и сообщений

Пугающие темы и сообщения являются одними из самых эффективных средств воздействия. Как правило, реализация этого метода направлена на стимулирование тех или иных действий аудитории. В случае избирательных кампаний этими действиями может быть голосование «за» или «против» того или иного кандидата. Побочной, а в ряде случаев и основной, задачей этого метода выступает разрушение положительного имиджа и создание отрицательного. В этом случае тот или иной кандидат, партия, политико-финансовая группа представляется в качестве угрозы жизни, безопасности и благосостояния граждан, устойчивости социальной системы общества и т.д.

Так, в кампании Президента США 1964 года избирательная команда Линдона Джонсона использовала телевизионный ролик с маленькой девочкой, которую уничтожал ядерный взрыв, который ассоциировался с его конкурентом Барри Голдуотером. Во Франции правые выпустили брошюру «Теряешь лишь раз в жизни», которая имела антисоциалистскую направленность. На обложке находился крестьянин, заключенный в стилизованную под тюрьму избирательную урну, а брошюра содержала угрозы обобществления собственности, потери продуктивности хозяйств,

оболванивания детей в контролируемых коммунистами сельских школах – в случае победы социалистов.

Заострение внимания

Этот метод во многом сходен с методом «упрощение проблемы». Сложные идеи, события или действия другой стороны сводится к тому или иному уязвимому для нее пункту.

Имитационная дезинформация

Метод состоит во внесении изменений в пропаганду другой стороны. Эти изменения придают ей другое направление, снижают доверие к ней, создают негативный образ. Используется в виде подмены листовок, высказываний кандидатов или групп. Например, в ходе одной из кампаний были выпущены листовки с избирательной программой и дизайном листовок другой стороны, однако программа содержала положения, неприемлемые для электората. Другим примером применения метода является выпуск поддельной листовки за подписью одного из кандидатов с сообщением о снятии своей кандидатуры, что имело место в одном из регионов РФ.

Прямое опровержение

Метод состоит в прямом опровержении всех элементов пропаганды другой стороны.

Игнорирование

Состоит в игнорировании элементов и тем другой стороны, основан на том предположении, что негативная тема, остающаяся «на слуху», приносит больший ущерб по сравнению с темой, появившейся на короткий промежуток времени. Наиболее эффективен в случае незначительности темы, небольших ресурсов другой стороны для его «раскручивания», а также в случае высокой достоверности негативной информации.

Отвлекающая пропаганда

Метод состоит в отвлечении и переносе внимания целевой аудитории с тем пропаганды другой стороны на другие темы. Достаточно часто используется государственной властью. Например, общеизвестным становится тот факт, что за моментами активизации критики Президента США по «сексуальной линии» практически сразу же активизировались темы Ирака, нанесения бомбовых и ракетных ударов, террористов и т.д. В России, в моменты различных кризисов, возникала тема захоронения В.И. Ленина и др.

Уменьшение значимости темы

Метод основан на переносе акцентов на менее негативные элементы темы, кратком затрагивании и «неупоминании» темы и т.д. Используется совместно с методом отвлекающей пропаганды.

Превентивная пропаганда и опережение

Метод состоит в превентивном использовании пропагандистской темы, которая может быть использована другой стороной, с измененными и смягченными компонентами или элементами для уменьшения доверия к теме. Более того, контрпропаганде в целом свойственен именно опережающий характер. В практике психологических операций часто используется в форме опережающего выдвижения обвинений к другой стороне. В избирательных кампаниях нередко используется путем выдвижения очевидно надуманных обвинений к кандидату, с последующим широким опровержением этих обвинений.

Ограничительные меры

В избирательных кампаниях метод трансформируется в работу по сбору и уничтожению наглядной агитации конкурентов, нарушению циклов ее производства и распространения.

Использование эвфемизмов

Данный метод схож с использованием метода «наклеивания ярлыков», только наоборот. Состоит в замене общепризнанных и эмоционально окрашенных обозначений тех или иных объектов или фактов на слова, имеющие меньшую эмоциональную окраску или менее понятные.

Псевдологические выводы

Метод состоит в использовании неправильных логических выводов. Например, на основе факта поддержки кандидатом идеи об увеличении вмешательства государства в экономику и того факта, что коммунисты также выступают за вмешательство в экономику, делается вывод, что кандидат – коммунист. В качестве разновидности метода выступает его совместное использование с методом «выборочный подбор информации», когда логические выводы делаются на основе специально ограниченного массива информации. В избирательных кампаниях особенно часто используется при проведении различных социологических опросов, развитии и поддержке пропагандистских тем и т.д.

Нарушение логических и временных связей между событиями

Используется для снижения эффекта «воздействия» другой стороны, а также создания иллюзии тех или иных тенденций и ситуаций. Например, с помощью метода предупреждается неявное создание (или, напротив, создается) из отдельных негативных фактов общей существенно негативной тенденции или фона. Применяется совместно с методами «выборочный подбор информации» и «псевдологические выводы».

Замена источника сообщения

Метод является противоположностью метода «имитационная дезинформация» (замена содержания при неизменном источнике сообщения) и состоит в замене источника сообщения для увеличения или уменьшения доверия к сообщению. Например, для уменьшения доверия к тому или иному факту приводится источник, не заслуживающий доверия. Напротив, для того чтобы избежать предположений в «ангажированности» и, таким образом, увеличения доверия к сообщению, производится «дистанцирование» и приводится какой-либо независимый источник. В качестве распространенного варианта выступает сообщение, появляющееся в зарубежных странах с последующей «ре-публикацией» со ссылкой на зарубежный источник.

Формирование окружения

Метод состоит в специальном формировании информационного окружения вокруг того или иного факта для снижения или, напротив, увеличения его эффекта или степени доверия к нему. Например, если факт, действительно имевший место, подается в окружении ложной информации, это приводит к снижению к нему доверия.

Уменьшение значимости темы

Метод основан на переносе акцентов на те элементы события или темы, которые имеют меньшую негативную окраску, кратком затрагивании и «неупоминании» темы, использовании нейтральных или противоречивых комментариев и т.д. Используется совместно с методом «формирование окружения».

Выборочный подбор информации

Суть метода состоит в специальном подборе тех фактов, которые являются более выгодными для одной из сторон. В дальнейшем набор этих фактов используется в телевизионных передачах, публикациях, выступлениях, создавая иллюзию той или иной тенденции или ситуации.

Воробьева Алиса Андреевна

Коржук Виктория Михайловна

Системы защиты информации в ведущих зарубежных странах

Часть 1

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверский пр., 49