Секция «Конфликты в цифровом обществе: источники, специфика, механизмы решения»

Особенности современных технологий информационных войн

Научный руководитель – Авзалова Эльмира Илгизовна

Данилова Есения Сергеевна
Студент (бакалавр)
Казанский (Приволжский) федеральный университет, Институт социально-философских наук и массовых коммуникаций, Казань, Россия
E-mail: esenya.danilova@gmail.com

Актуальность. С появлением Интернета в повседневности граждан изменению подверглись все сферы их жизни. Процесс коммуникации между властью и обществом стал значительно комфортнее. Сеть упрощает работу СМИ, политиков, поскольку жители государств могут самостоятельно обеспечивать себя нужной им информацией, быть в курсе происходящего вокруг них, в других частях света, участвовать в политической деятельности, формировать международные сообщества. Появилась новая проблема – перевод конфликтов на государственном, международном уровнях в среду Интернета, – в результате чего нашли своё применение технологии ведения информационных войн. Протекающие в Интернете информационные войны имеют высокий разрушительный потенциал. Ввиду использования информационного оружия в них вовлечено множество участников. Это актуализирует проблему информационного суверенитета. Данный вопрос поставлен как никогда остро в нынешнее время, когда Российской Федерации, а также другим государствам необходимо обеспечить безопасность использования гражданами Интернет-ресурсов, но вместе с тем сохранять для них доступность информации. В связи с вышесказанным, нужно выявить особенности ведения информационных войн.

Объект исследования: информационные войны.

Предмет исследования: особенности ведения информационных войн в Сети Интернет.

Цель исследования: определить особенности современных технологий информационных войн.

Задачи исследования:

1. Определить роль Интернет-технологий в политике;
2. Рассмотреть основные задачи информационных войн;
3. Выявить цели информационных войн;
4. Дать определение информационной войны.

В современном мире конфликты часто разгораются в реальности, перетекая в Интернет-пространство, либо происходят уже на просторах сети, либо берут своё начало в Интернете, трансформируясь в военный офлайн-конфликт.

Задачи ведения информационных войн:

- Программирование сознания общества на наведение беспорядка в нём и приведение его в неподконтрольное состояние;
- Негативное воздействие на отношения между партиями, призыв к физическому угнетению инакомыслящих для подрыва доверия общества власти, «политической борьбы» [1];
- Ухудшения условий обеспечения защиты данных, содействие регрессивному руководству страной;
- Внедрение ложных сведений об управлении государством;
- Ухудшение имиджа государства на международной арене;
- Негативное воздействие на интенции страны в сферах жизни;
- Создание и продвижение нового «культурного кода» [1] в государстве-оппоненте;

- Скрытое воздействие на психику жителей государства-врага посредством информации;

- Применение оружия в виде скопления данных [2].

Целями применения технологий ведения информационной войны являются обретение авторитетных позиций во всех сферах жизни общества, особенно в онлайн-среде (это позволяет одной стране воздействовать на управление в другой, обеспечить сетевую безопасность), ведения информационных наступательных атак на противника, повышение результативности «вооруженных сил с помощью повсеместного использования военных информационных функций»[3].

Основные особенности ведения информационных войн: широкомасштабность, дешевизна оружия, воздействие на информационные системы врага, долгосрочный результат, применение информационного оружия (часто в комплексе с физическим), сверхновых всевозможных вирусных программ для подрывной деятельности против систем онлайн и оффлайн безопасности. Технологии ведения таких войн классифицируются по актору, методам и объекту влияния.

Таким образом, информационная война – это совокупность действий политических акторов, состоящих в конфронтации, использующих информацию как основное оружие противостояния и манипуляции с ней для воздействия на политические структуры государства, на его жителей.

Источники и литература

1) Арутюнян, Г., Гриняев, С., Арзуманян Р., Информационные войны новой формации // 21-й век. 2016. №3 (40). С.5-14

2) Казакова, В. А. Мировые информационные войны. Защита информационной безопасности / В. А. Казакова, Т. В. Сидорина, Р. О. Димова // Наука и мир. 2022. № 3. С. 91-95.

3) Попова, С. В., Федоринов В.Е. Цели и последствия информационной войны // Воздушно-космические силы. Теория и практика. 2018. №6 (6). С. 15-20.