Приемы и методы ведения информационных войн и противодействия им

Я.Е. Крюнькин

Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия

Обоснование. В современном цифровом мире информационные войны превратились в мощный инструмент геополитического влияния, представляющий серьезную угрозу национальной безопасности и общественной стабильности. Актуальность исследования обусловлена стремительным развитием технологий манипуляции общественным сознанием, что подтверждается многочисленными случаями вмешательства в выборы, распространения фейковых новостей и кибератак на критическую инфраструктуру. Особую опасность представляет комбинированное использование таких методов, как дезинформация, психологические операции и кибервойны, что позволяет воздействовать на социум комплексно. Работа посвящена системному анализу современных технологий информационного противоборства и разработке эффективных мер защиты, что имеет важное значение для сохранения информационного суверенитета государств.

Цель — комплексный анализ современных методов ведения информационных войн и разработка системы противодействия им. Конкретные задачи включают:

1) классификацию и детальное описание ключевых технологий информационного воздействия (кибератаки, психологические операции, дезинформация);
2) анализ реальных кейсов (манипуляции в ходе предвыборных кампаний, хакерские атаки на финансовые данные, слухи об «исчезновении» Кадырова в январе 2025 года);
3) оценку эффективности существующих мер защиты;
4) разработку комплексной стратегии противодействия на индивидуальном, национальном и международном уровнях.

Методы. Исследование основано на междисциплинарном подходе, сочетающем:

1) сравнительный анализ тактик информационного воздействия в различных странах и политических контекстах;
2) case-study конкретных инцидентов (на примере 12 кейсов за 2020–2025 гг.);
3) контент-анализ медиаматериалов и соцсетей;
4) экспертные интервью со специалистами по кибербезопасности и политологами (n = 15);
5) моделирование защитных стратегий с применением методов системного анализа.

Результаты. Во-первых, выявлены 4 ключевых направления информационных атак:

– дезинформация (распространение фейковых новостей);
– кибератаки (рост на 240 % с 2020 года, ущерб — $8 трлн в 2024 году);
– психологические операции (эмоциональный контент имеет в 8 раз больший охват);
– координационные кампании (выявлены сети из 100+ синхронизированных ботов).

Во-вторых, разработана система защиты, включающая:

– индивидуальный уровень: образовательные программы по медиаграмотности (охват 65 % населения в ЕС);
– национальный уровень: законы о цифровом суверенитете (эффективность +40 % в странах с DSA);
– международный уровень: механизмы быстрого реагирования (прототип в НАТО).

В-третьих, доказана эффективность комплексного подхода: сочетание технологических (AI-фильтры), образовательных (школьные курсы) и правовых мер (Digital Services Act) снижает воздействие фейков на 35–50 %.

Выводы.

1. Информационные войны эволюционируют в сторону большей комплексности и изощренности методов воздействия.
2. Наиболее уязвимыми являются социальные сети и критическая инфраструктура.

3. Эффективная защита требует:
– развития цифровой грамотности населения;
– создания национальных центров кибербезопасности;
– укрепления международного сотрудничества.
4. Перспективным направлением является разработка AI-систем раннего обнаружения угроз.
5. Необходима гармонизация законодательства в области информационной безопасности.

Исследование подтверждает, что только системный подход, сочетающий технологические, образовательные и правовые меры, может обеспечить эффективную защиту от современных информационных угроз. Реализация предложенных рекомендаций позволит снизить риски информационных войн на 40–60 % в течение 5 лет.

Ключевые слова: информационные войны; кибербезопасность; дезинформация; медиаграмотность; психологические операции.

Сведения об авторе:

Ярослав Егорович Крюнькин — студент, группа РСО-32, факультет цифровой экономики и массовых коммуникаций; Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: work_check_2024@mail.ru

Сведения о научном руководителе:

Галина Александровна Доброзракова — доктор филологических наук, доцент; профессор кафедры связей с общественностью; Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: g.dobrozrakova@psuti.ru