Корнилова А.А.
Научный руководитель – к.и.н., доцент, зав. каф. ЭТиМК М.Е. Гусарова
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: ankornil0va@yandex.ru

Информационная война и информационная безопасность

Информация сопровождает человека на протяжении всей его жизни. Однако, в современном мире это окружение становится все активнее благодаря новым технологическим разработкам в сфере информационно-коммуникационных технологий.

Сознание восприимчиво к информации, которую подают преимущественно в определенной, визуальной и чувственно осязаемой форме. Такое воздействие содержит наибольшие возможности для манипулирования массовым сознанием и чаще всего затрагивает различные сферы политических, идеологических, социальных и экономических отношений. Таким образом, массовое сознание оказывается под моральным, воспитательным, и идеологическим воздействием. Создается определенный информационный контент, влияющий на массовое восприятие и усвоение соответствующих данному контенту поведенческих правил, соединенных с моральными и повседневными примерами не только реального, но искусственного исполнения [1].

Актуальность и значимость исследований в области информационных войн и обеспечении информационной безопасности, определяется тем, что на сегодняшний момент важно создать эффективную систему государственного противостояния информационной войне для любой страны мира.

На международной арене успешное ведение информационной войны может обеспечить огромное влияние на мнение мировой общественности. А неумелое использование информационных средств может, наоборот, ухудшить положение страны, негативно повлияв на собственную экономику, политику и общественное настроение, в том числе внутриполитическое. Таким образом, последствия информационной войны могут быть самыми разнообразными:

- трансформация общественного сознания;
- нарушение информационной безопасности государства, общества и личности;
- получение выгоды в политической, экономической, финансовой и военной сфере;
- нарушение деятельности государственных, финансовых, коммуникационных сетей и информационных систем;
- обладание конфиденциальной информацией, доступ к электронным системам и сетям.

Следует отметить, что информационные войны в настоящее время являются реальностью. Фактически информационная война превратилась в своего рода военное противостояние в форме насилия, которое затрагивает как врага, так и его народ, а в качестве оружия используется дезинформация [2].

Войны начинаются с разжигания ненависти между народами и группами людей. Каждый из нас является объектом и потенциальной жертвой информационной войны. Поэтому информационная безопасность — это вопрос выживания не только государств, но и отдельных личностей. Для того, чтобы защитить себя, необходимо научиться выбирать источники информации и фильтровать поступающие через них сведения. Также может быть полезным узнать приемы и способы ведения информационных войн, чтобы узнавать их приметы в потоке встречающейся информации.

Чтобы обезопасить себя от недостоверной информации Фонд защиты национальных ценностей рекомендует пользователям Интернета:

- подписываться на новостные ленты разных СМИ, чтобы иметь возможность сверять информацию. Современные средства массовой информации реагируют на новости настолько оперативно, что все реальные события отражаются в их лентах почти одновременно (разница в несколько часов);

- ставить на самое последнее место в списке достоверных источников эмоциональные сообщения в личных чатах;

- не распространять недостоверную информацию, не рассылать непроверенные новости друзьям, не публиковать ссылки на них в комментариях;

- проверять интересующие новости на официальных сайтах;

- обращать внимание на опровергающие сообщения в СМИ. Одним из методов борьбы с дезинформацией является официальное опровержение уполномоченными органами;

- обдумывать свои действия и проверять наличие весомых оснований следовать какому-либо призыву из сообщений. Страховкой собственной безопасности является логическая проверка чьих-либо призывов к действиям [3].

Информационная безопасность личности определяется способностью нейтрализовать воздействие по отношению к опасным, дестабилизирующим, деструктивным, ущемляющим интересы личности информационным воздействиям на уровне, как внедрения, так и извлечения информации. Информационная безопасность личности в России является базовой составляющей национальной безопасности России. Она напрямую влияет на эффективную работу органов государственной власти, является неотъемлемым фактором в борьбе с организованной преступностью и мировым терроризмом. Проблемы, связанные с повышением безопасности информационной сферы, являются сложными, многоплановыми и взаимосвязанными. Они нуждаются в постоянном, пристальном внимании государства и общества. Развитие информационных технологий способствует объединению усилий с целью разработки методов и инструментов, позволяющих достоверно оценивать угрозы безопасности в информационной сфере и адекватно реагировать на них.

Литература

1. Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017. 124 с.

2. Фролов Н. В. Социальные сети как инструмент ведения информационных войн // Социодинамика. 2018. № 8. С. 1–6.

3. Фонд защиты национальных ценностей (Электронный ресурс) // Режим доступа: https://fznc.ru/