УДК 34

ИНФОРМАЦИОННАЯ ВОЙНА В СЕТИ ИНТЕРНЕТ

Мосина Д.О., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *информационная война, Интернет, внешнее воздействие, информационная опасность, информация.*

В данной статье рассматривается вопрос об информационной войне в виртуальном мире. Разбирается то воздействие на современный мир на новом уровне, где каждый человек подвержен угрозам через сеть Интернет.

Информационная война – это межгосударственное противостояние в информационном пространстве, целью которого является нанесение ущерба информационным процессам, системам и ресурсам, другим критически важным структурам [1].

Информационная война преследует три цели:

- контролировать информационное пространство, чтобы его можно было использовать, защищая при этом функцию военной разведки от действий противника (контринформация).

- Использовать контроль над информацией для нанесения информационных ударов по противнику.

- Повысить общую эффективность вооруженных сил за счет широкого использования функций военной разведки [2].

В информационной войне есть три основных этапа:

1. Определение цели (зачем это нужно и что должно быть получено в результате);

2. Стратегия: учет четырех основных элементов техники коммуникации (подготовка сообщения, определение канала, выбор коммуникатора и целевой аудитории сообщения);

3. Тактический план действий [3].

Информационные войны могут вестись как между государствами, так и внутри одного государства между различными политическими, социальными и экономическими группами. Информационные войны могут быть открытыми, когда стороны находятся в явном конфликте друг с другом, или закрытыми, когда информационные операции проводятся без ведома общественности.

Виды информационных войн:

- Командно-управленческая – направлена на каналы связи между командованием и подчиненными с целью лишения последних управления и координации сверху;

- Разведывательная война – предусматривает собрание ценной информации для нападения и собственной защиты;

- Электронная война – подразумевает выведение из строя электронных средств связи: компьютерных сетей, сотовых вышек, радиоузлов и т. д.;

- Психологическая война – пропаганда и информационная обработка населения, то есть, «промывка мозгов»;

- Хакерская война – определенные действия, которые приводят к сбоям в работе связи, оружием в данном виде войны выступают компьютерные вирусы, взломы и получение доступа к любым данным и несанкционированное их использование с целью шантажа;

- Экономически информационная война – полагает информационную блокаду и информационный империализм;

- Кибервойна – ставит перед собой цель захватить компьютерные данные и выследить объект с целью дальнейшего шантажа [4].

СМИ активно используют слабые стороны друг друга, распространяя политическую и экономическую дезинформацию, перефразируя контексты, используя различные комбинации и информационные игры. Кроме того, СМИ этих стран насыщают общественность информацией о том, что происходит в соседних странах, чтобы изменить их настроения.

Чтобы не поддаться влиянию шумихи, важно обладать критическим мышлением, способностью анализировать данные, логическим мышлением и, в конечном счете, определенным мировоззрением и знаниями. Однако в целом многие пользователи

Интернета не обладают аналитическими способностями, легко поддаются внушению и просто следуют за толпой [5].

«Приемы противодействия в информационной войне:

1. Критическое мышление и информационная грамотность

Люди должны научиться анализировать информацию, проверять ее достоверность и источники, а также различать факты от мнений и дезинформации.

2. Образование и просвещение

Образование и просвещение играют важную роль в борьбе с информационными войнами. Школы и университеты должны включать в свои программы обучение по информационной грамотности и критическому мышлению.

3. Проверка источников информации

Важно проверять источники информации, особенно в ситуациях, когда она кажется сомнительной или вызывает сомнения. Проверка фактов и подтверждение информации у независимых и достоверных источников помогут избежать распространения дезинформации.

4. Развитие критического отношения к информации

Необходимо развивать критическое отношение к информации и не принимать все, что говорится или пишется, на веру. Важно задавать вопросы, искать альтернативные точки зрения и собирать достаточно информации, прежде чем делать выводы.

5. Сотрудничество и обмен информацией

Сотрудничество и обмен информацией между государствами, организациями и общественностью могут помочь в борьбе с информационными войнами. Обмен опытом, разработка совместных стратегий и координация действий могут повысить эффективность защиты от информационных войн» [6].

Библиографический список:

1. Образовательный портал «Справочник» [Электронный ресурс]. – Режим доступа: https://spravochnick.ru

2. Познайка.Орг [Электронный ресурс]. – Режим доступа: https://poznayka.org

3. Лаборатория [Электронный ресурс]. – Режим доступа: http://www.advlab.ru

4. Виды информационных войн по сферам их ведения [Электронный ресурс]. – Режим доступа: http://wasmagazine.tilda.ws

5. Воронина, И. А. Сеть Интернет как способ ведения информационной войны на современном этапе / И. А. Воронина, А. В. Кирпичникова // Вопросы российского и международного права. – 2023. – Т. 13, № 8-1. – С. 123-127.

6. Научные Статьи.Ру [Электронный ресурс]. – Режим доступа: https://nauchniestati.ru

7. Голубев С. В. Актуальные вопросы информационной безопасности // / С. В. Голубев, С.А. Голбуева // Материалы научно-практической конференции «Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения». – Ульяновский ГАУ. – 2022. – С. 552-557.

INFORMATION WARFARE ON THE INTERNET

Mosina D.O.
Scientific supervisor – Golubev S.V.
FSBEI HE Ulyanovsk SAU

Keywords: *information warfare, Internet, impact, danger, information.*

This article raises the issue of information warfare in the virtual world. The impact on the modern world at a new level is considered, where everyone is exposed to threats via the Internet.