

ИНФОРМАЦИОННАЯ ВОЙНА

Рыбко В.Ю., студентка 2 курса факультета непрерывного образования по подготовке специалистов для судебной системы

Научный руководитель — Сафонова Ю.А.

Дальневосточный филиал федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия»

***Ключевые слова:** информационная война, кибер-атака, информация, информационное оружие, война, киберпространство, безопасность.*

Данная статья рассматривает актуальные вопросы, связанные с ведением информационной войны, информационные атаки как способы ведения борьбы, информационного воздействия и причины возникновения данной проблемы.

Введение. «Война и подготовка к войне затрагивают все сферы управления общественной жизни людей: административно-политическую, социально-экономическую и культурно-мировоззренческую, что требует всестороннего учета феномена при анализе проблем международной безопасности. Постоянно обновляются стратегии, военно-технические средства войны. Противостояние охватывает не только морскую, сухопутную и воздушную среды, теперь к ним добавилось киберпространство. Киберпространство — весьма специфическая сфера деятельности и среда, которая имеет относительно автономный характер и оказывает огромное влияние на развитие экономики, политической жизни, культуры, техносферы, и тем более военного дела. Задача повышенной сложности здесь — это выявление источника угрозы и источника «кибер-атак», устранение эффекта анонимности. Киберпространство превращается в катализатор нового спектра угроз и повышенной степени стратегической неопределенности.»[1]

Каждое базовое техническое, технологическое новшество всякий раз вызывает обострение давних или же порождает новые трудности. Неправомерное искажение, фальсификация, устранение или разглашение конкретной части информации наносят вещественный и нравственный убыток почти всем субъектам (государству, юридическим и физическим лицам), участвующим в процессах информационного взаимодействия.

В России Интернет активно развивается. Обеспечено подключение к сети сотен тысяч компьютеров индивидуальных, корпоративных и государственных пользователей. И спрос на услуги глобальной информационной сети в нашей стране продолжает расти ускоряющимися темпами. Стремительное развитие компьютерных технологий, международных компьютерных сетей и всё более широкое их использование в государственных структурах России обостряет ведение информационной войны, а вследствие этого непрерывно обостряет сопутствующую этим процессам проблему обеспечения информационной безопасности.

Информационную войну можно рассматривать как особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы и средства силового воздействия на информационную сферу этих государств. Информационные войны могут происходить и внутри страны — например, при столкновении политических противников, особенно в ситуациях обострения борьбы за власть и т.д. Информационные войны ведутся с помощью информационного оружия, внедрение которого по производительности сравнимо с действием оружия массового поражения.

Информационное оружие выделяет собой совокупность средств, методик и технологий, обеспечивающих возможность силового воздействия на информационную сферу неприятеля с целью разрушения его информационной инфраструктуры, систем управления государством.

Главные площадки воздействия — социальные сети. Объект воздействия — молодежь, пользователи социальных сетей.

«Информационная война — это разновидность боевых действий, в которых ключевым объектом воздействия является информация,

хранящаяся или циркулирующая в системах противника. Оружием информационной войны являются устройства и методы обработки информации, которые используются для широкомасштабного, целенаправленного, быстрого и скрытного воздействия на военные и гражданские информационные системы противника с целью подрыва его экономики, снижения степени боеготовности и боеспособности с целью способствовать достижению окончательной победы».[2]

В современном мире информация является необходимым элементом, обеспечивающим функциональность любой системы наряду с материальным оборудованием. Качество информации, которой владеют стороны противоборства, напрямую влияет на их боеспособность. Например, в ВВС анализ результатов разведки и прогноз погоды являются основой для разработки полетного задания. Точность навигации влияет на эффективность выполнения задания.

«Существует два вида информационных атак: косвенная и прямая.

Косвенная	Прямая
Допустим, мы хотим ввести командование противника в заблуждение относительно места распространения авиационной части.	
Построить ложный аэродром, разместить там макеты самолетов и имитировать деятельность по их техническому обслуживанию.	Внедрить ложную информацию о местонахождении той же авиационной части прямо в хранилище врага, чтобы при принятии решений командование оперировало ложными данными.

В информационной войне важны также чисто технические приемы – повторяемость фраз, фото-, видео-, звукомонтаж, прерывание программ последними новостями, требующих заострения внимания на событии или фактах, выстраивание перед новостными программами краткой повестки дня для манипуляции выгодной информацией».[3] Простой приём, когда населению дают самим сделать неверный вывод из материала прессы. Дается сразу ошибочный выбор, так как половина невыгодных фактов просто умалчивается.

Заключение. Одной из основных причин зарождения информационной войны, которая уже по своему характеру занимает положение между «холодной» войной и реальными боевыми действиями с участием вооруженных сил является стремление определённых субъектов «...единолично обладать информационными ресурсами и использовать их для удовлетворения своих интересов и

противодействия интересам вероятных конкурентов... Информация и информационные технологии при этом начинают выступать в качестве объектов угроз, что порождает проблему информационной безопасности».[4]

Библиографический список:

1. Балаева Е. Пять самых известных информационных войн/ Е. Балаева. – Текст: электронный // SmartNews : [сайт] – URL: <http://smartnews.ru/articles/13363.html?ysclid=l197blmdeh> (дата обращения: 28.11.2022)
2. Бартош А. А. Основы международной безопасности. Организации обеспечения международной безопасности : учебное пособие для вузов / А. А. Бартош. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 320 с. — (Высшее образование). — ISBN 978-5-534-11783-7. — URL: <https://urait.ru/bcode/493387/p.59> (дата обращения: 21.11.2022) – Текст : электронный.
3. Панкратова Н.В. Информация как определяющий фактор социально-экономического развития/ Н.В. Панкратова. – Текст: электронный // Научная электронная библиотека eLIBRARY: Журнал Весник БГУ: [сайт] – URL: <https://elib.bsu.by/bitstream/123456789/40850/1/38-41.pdf?ysclid=lbjaui99pe428923071> (дата обращения: 24.03.2022)
4. Суворова Г.М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — URL: <https://urait.ru/bcode/496741/p.106> (дата обращения: 24.03.2022) — Текст : электронный.

INFORMATION WARFARE

Rybko V.Yu.

Keywords: *information warfare, cyber attack, information, information tool, war, cyberspace, security.*

This article examines topical issues related to the conduct of information warfare, information attacks as ways of leading the war, information impact and the causes of this problem.