Капитанчук В.В., Акимов А.О., Лубнина А.А. Влияние информационного оружия на человека// Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31)ч.1 с. 19–22

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

ВЛИЯНИЕ ИНФОРМАЦИОННОГО ОРУЖИЯ НА ЧЕЛОВЕКА

Капитанчук В.В., Акимов А.О., Лубнина А.А.
ФГБОУ ВО "Ульяновский институт гражданской авиации имени Главного маршала авиации Б.П. Бугаева", Ульяновск, Россия (432071, Ульяновская область, г. Ульяновск, ул. Можайского, зд 8/8) *e-mail: lubniaha0@mail.ru*

Информационное оружие считается одним из основных средств ведения информационных войн, с помощью воздействия на информационные системы и процессы противника. Оно применяется для хищения информационных массивов и дезорганизации технических средств. Поэтому важно знать не только классификацию информационного оружия, но и методы борьбы с ним.

Ключевые слова: Информационное оружие, информационная война, национальная безопасность.

THE IMPACT OF INFORMATION WEAPONS ON HUMANS

Kapitanchuk V.V., Akimov A.O., Lubnina A.A.
Ulyanovsk Institute of Civil Aviation named after Chief Marshal of Aviation B.P. Bugaev, Ulyanovsk, Russia (432071, Ulyanovsk region, Ulyanovsk, Mozhaisky str., building 8/8) *e-mail: lubniaha0@mail.ru*

Information weapons are considered to be one of the main means of conducting information wars by influencing the information systems and processes of the enemy. It is used to steal information arrays and disorganize technical means. Therefore, it is important to know not only the classification of information weapons, but also the methods of combating them.

Keywords: Information weapons, information warfare, national security.

Информационное оружие - это средства и методы воздействия на информационные системы, которые могут привести к нарушению их функционирования или к разрушению информации. [5]

Информационное оружие способно представлять опасность для национальной безопасности каждой страны. Оно представляет из себя совокупность средств, инструментариев, а также всевозможных методов с целью ликвидирования и формирования сбоев в работе технического оборудования вместе с воздействием на конкретную область пользователей.

Национальная безопасность - данное состояние защищенности страны от внутренних, а также внешних угроз. Именно она гарантирует устойчивое развитие государства и защищает остро значимые интересы личности, общества, в том числе молодое поколение, кроме того страны в разных областях жизнедеятельности. [1]

Информационное оружие имеют все шансы применять для подрыва национальной безопасности Российской федерации.

Понятия и виды информационного оружия

Прежде чем обращаться к разбору ИО, необходимо разобраться, откуда все началось.

Первые упоминания об информационной войне можно найти в работах американского ученого Ричарда Хелма в 1948 году. [6] В России же термин «информационная война» появился в конце 80-х годов XX века.

Информационная война - это процесс противоборства человеческих общностей, направленный на достижение политических, экономических, военных или иных целей стратегического уровня, путём воздействия на гражданское население, власти и (или) вооружённые силы противостоящей стороны. [1]

Расходы Российского бюджета на армию в 2022 году составляет $56,148 млрд. такую оценку приводят «Ведомости». А в США за последние 10 лет объем инвестиций в информационное оружие вырос на 900%. В 2021 году $17,4 млрд из $21,8 млрд вложений в информационные войны пришлось на стартапы, штаб-квартиры которых находятся в США (они могут вести исследования и разработку в других странах). По вышеприведенным данным, разница бюджета РФ на всю армию и бюджет США, выделяемый лишь на информационные войны, составляет 2,7. Таким образом, США уделяет большее внимание ИО, нежели Россия. [2], [3]

Так, информационное оружие может быть использовано в рамках информационной войны для достижения политических, экономических, военных или иных целей стратегического уровня

Важно понимать, что начинать защиту от информационного оружия необходимо с молодёжи, т.к. ИО может быть использовано для манипулирования и убеждения людей, а также для распространения неправдивой информации и фейковых новостей. На сегодняшний день большая часть молодежи проводит много времени в интернете, поэтому случайно могут стать жертвой информационного оружия. Месенджеры, такие как Telegram и WhatsApp, а также фейковые аккаунты могут быть использованы как часть информационного оружия. Они могут распространять фейковые новости и информацию, которая может повлиять на общественное мнение и даже на результаты выборов.

С целью эффективного использования информационного оружия в практике, выделяется ряд ключевых проблем:

1. Проводятся провокации общественно-политической напряженности внутри государства, церковных, а также национальных конфликтов, кроме того многочисленных массовых волнений;
2. Манипуляции сознаниями жителей этого, либо другого государства, формирование атмосферы аморальности, пропаганды отрицательного взаимоотношения к культурному наследию;
3. Подрыв авторитетности страны в интернациональной степени, препятствие партнерства вместе с иными государствами;
4. Нарушение контролирования при государства армией и техникой;

5. Нанесение вреда стране в сфере политические деятели, экономики, общественной, а также иных областях работы.

Информационное оружие можно разделить на несколько видов:

1. Оружие, основанное на информационных технологиях;
2. Оружие, оказывающее энергетическое и химическое воздействие;
3. Информационно-техническое оружие;
4. Информационно-психологическое оружие. [4]

Характерные черты и разновидности информационного оружия.

Информационное оружие различается от обыкновенного оружия тем, что никак не несет прямого боевого нрава, а также никак не применяет насильственных операций в процессе использования. Оно влияет на сознание, а также дух человека, а не на его плоть. Различием между информационным оружием и простым вооружением являются такие свойства, как управляемость, скрытность, универсальность, экономичность, а также доступность.

Основная цель ИО – контроль информационных ресурсов противника или вмешательство в его систему с целью ее дезорганизации, вывода из строя телекоммуникационных сетей, компьютерных систем.

Методы борьбы с информационными войнами

Существует множество методов защиты от информационного оружия. Они могут включать в себя:

1. Образование и повышение осведомленности: обучение людей критическому мышлению и анализу информации может помочь им распознавать и отвергать фальшивую или манипулятивную информацию.
2. Защита информационных систем: использование антивирусного программного обеспечения, фильтров спама и других технологий для защиты компьютерных систем от вредоносных программ и атак.
3. Регулирование и контроль: государственные органы могут регулировать распространение информации и контролировать ее содержание, чтобы предотвратить распространение ложной или вредоносной информации.
4. Международное сотрудничество: страны могут работать вместе, чтобы бороться с информационным оружием на международном уровне.
5. Разработка и применение новых технологий: постоянное развитие новых технологий для обнаружения и противодействия информационному оружию.

Эти методы могут быть использованы в сочетании друг с другом для эффективной защиты от информационного оружия.

Подводя итоги, можно говорить о том, информационное оружие рассматривается как уникальный вид оружия, которое по своей сути является наиболее эффективным средством противоборства, чем, ставшее традиционным, вооружение и военная техника.

Список литературы

1. Справочник Автор24 [Электронный ресурс]. - https://spravochnick.ru/zhurnalistika/informacionnye_voyny/ (дата последнего обращения: 14.03.23)

2. "Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2023 год и на плановый период 2024 и 2025 годов" (утв. Минфином России) [Электронный ресурс]. - https://www.consultant.ru/document/cons_doc_LAW_429950/eb09eba19c8dba0bb509d61dacbd966b79f236ab/ (дата последнего обращения: 16.03.23)
3. Информационная безопасность вооруженных сил РФ [Электронный ресурс]. - https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-vooruzhennykh-sil-rf/ (дата последнего обращения: 06.04.23)
4. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. - СПб.: Наукоемкие технологии, 2017. - 546с.
5. Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. – М.: Харвест, 2004. – 426с.

References

1. Reference book Author24 [Electronic resource]. - https://spravochnick.ru/zhurnalistika/informacionnye_voyny / (last accessed: 14.03.23)
2. "The main directions of budget, tax and customs tariff policy for 2023 and for the planning period of 2024 and 2025" (approved by the Ministry of Finance of the Russian Federation) [Electronic resource]. - https://www.consultant.ru/document/cons_doc_LAW_429950/eb09eba19c8dba0bb509d61dacbd966b79f236ab / (last accessed: 03/16/2013)
3. Information security of the Armed forces of the Russian Federation [Electronic resource]. - https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-vooruzhennykh-sil-rf / (last accessed: 06.04.23)
4. Makarenko S.I. Information warfare and electronic warfare in network-centric wars of the beginning of the XXI century. - St. Petersburg: Science-intensive technologies, 2017. - 546p.
5. Grinyaev S. N. The battlefield is cyberspace. Theory, techniques, means, methods and systems of information warfare. – M.: Harvest, 2004. – 426p.