Тип работы: Курсовая работа

Предмет: Информатика (другое)

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Современные информационные технологии (ИТ) имеют огромное значение для современного общества, так как: обеспечивают эффективную связь и коммуникацию между людьми в любой точке мира; предоставляют доступ к информации на различных устройствах: компьютерах, телефонах, планшетах и т.д.; увеличивают производительность и автоматизируют процессы в различных отраслях, таких как производство, здравоохранение, бизнес и т.д.; улучшают качество жизни, например, упрощая процессы покупок, организации путешествий, образования и досуга; обеспечивают безопасность данных и информации; позволяют сокращать затраты на общение, перемещение и хранение информации; помогают в решении большого числа задач и повышают эффективность работы в различных сферах деятельности.
В целом, современные ИТ являются неотъемлемой частью современной жизни и оказывают огромное влияние на все сферы жизнедеятельности человека.
Цель курсовой работы - дать характеристику информационному оружию.
Задачи курсовой работы:
1. Дать классификацию информационного оружия.
2. Изучить назначение и применение информационного оружия.
3. Изучить практические мероприятия по защите от информационного оружия.
Информационное оружие является одним из наиболее важных и актуальных вопросов в современной мировой политике и безопасности. Современные технологии и интернет повышают доступность и интенсивность использования информационного оружия, что ведет к серьезным последствиям для общества, политической стабильности и международной безопасности.

ГЛАВА 1. КЛАССИФИКАЦИЯ ИНФОРМАЦИОННОГО ОРУЖИЯ

1.1. Понятие и виды информационного оружия.

Информационное оружие – это использование информации или мультимедийных технологий для достижения правительственных, международных или военных целей. Оно может включать в себя создание ложной информации, проведение кибератак, манипуляцию публичным мнением, распространение фейковых новостей или использование социальных сетей для монтажа тех или иных криминальных действий. Информационное оружие является эффективным средством воздействия на массовое сознание и может негативно повлиять на политическую, экономическую или социальную стабильность общества.
Информационное оружие можно разделить на следующие классы:
1. Кибер-оружие: включает в себя программы, программное обеспечение, хакерские инструменты и технологии, используемые для нарушения информационных систем, атак на сетевую безопасность, кражи, шпионажа, и других киберпреступлений.
2. Социальное оружие: используется для манипуляции мнениями людей, в том числе с помощью

социальных сетей и массовых коммуникационных технологий. Включает в себя фейковые новости, пропаганду, вирусные видео и другие методы психологического воздействия на общественное мнение.
3. Электронное оружие: включает в себя использование высокочастотных радиоволн, микроволн, и других электромагнитных волн, чтобы нарушить работу электронных устройств, отключить электросети, и прервать связи.
4. Кибер-противодействие: используется для обнаружения, предупреждения и реагирования на кибератаки, в том числе системы мониторинга сетевой безопасности, инструменты анализа данных, и другие средства защиты информационных систем.
5. Интернет-оружие: включает в себя использование Интернета для злоупотребления данными, распространения компьютерных вирусов, причинения вреда и нарушения безопасности.
6. Компьютерное оружие: используется для внедрения вредоносного программного обеспечения в компьютерную систему или в сети, навязывание пользователю информации, кражи данных и прочих действий.
Под информационным оружием подразумевают: вирусы и коварные программы; фишинг и мошенничество в сети; спам и нежелательная реклама; денежные кибератаки и кражи учетных данных; отказы в обслуживании (DdoS-атаки и сбои в работе систем); пропаганда и дезинформация; шпионаж и прослушивание; цензура и ограничение доступа к информации; хакерские атаки и взломы; разведывательная деятельность и утечка информации.
По методам воздействия на информацию информационное оружие подразделяется на информационные системы противника и информационные процессы. Воздействие данного информационного оружия носится радиоэлектронный, программно-технический, информационный и физический характер.
Под физическим воздействием подразумевается применение различных средств огневого поражения: специализированные аккумуляторные батареи генерации импульса высокого напряжения, противорадиолокационные ракеты, биологические и химические средства воздействия на элементарную базу, средства генерации электромагнитного импульса, графитовые бомбы.
Информационные методы воздействия осуществляются с помощью глобальных информационных сетей, средств массовой информации, станциями голосовой дезинформации. Люди являются главным элементов информационной инфраструктуры. Деятельность людей основана на их потребностях. Если правильно рассчитать применение информационно-психологических методов воздействия на людей, то это окажет угрозу уровню безопасности государства.
Информационное оружие может использовать различные методы воздействия на целевую аудиторию:
1. Дезинформация - распространение неправдивой информации с целью ввести в заблуждение и убедить целевую аудиторию в чем-то. Например, дезинформация может использоваться в политических кампаниях или в информационной войне.
2. Манипуляция - использование психологических методов для изменения мнений и поведения аудитории. Например, реклама может использовать методы манипуляции, чтобы заставить людей купить определенный продукт.
3. Утверждение - повторение определенных сообщений, чтобы убедить аудиторию в необходимости чего-то. Например, политические кампании могут использовать утверждение, чтобы убедить людей проголосовать за определенного кандидата.
4. Провокация - создание событий или ситуаций, которые могут привести к определенной реакции или поведению аудитории. Например, провокация может использоваться в информационной войне для создания негативных стереотипов о других странах.
5. Сокрытие - утаивание определенной информации или фактов, которые могут нанести ущерб определенному лицу или организации. Например, журналисты могут использовать сокрытие, чтобы обезопасить источник информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Юдина Ю.А. Возможность применения средств обеспечения средств обеспечения международной безопасности к информационному пространству// Актуальные проблемы российского права, Том 17№ 6(139) июнь 2022г.
2. Валова Ю. И. Информационное оружие в современном мире. // Мировой опыт и экономика регионов России: Сборник научных работ молодых ученых по материалам XIX Всероссийской студенческой научной конференции с международным участием, Курск, 18-19 марта 2021 года. - С. 56-61.
3. Голубенко Н. Ю. Современная война. Война в информационном пространстве // Оригинальные

исследования. - 2021. - Т. 11. - № 1. - С. 111-113.
4. Джанавов И.О. Информационное оружие, как угроза национальной безопасности Российской Федерации//Сборник научных статей студентов юридического факультета северо-кавказского института ВГУЮ (РПА Минюста РФ). Том Выпуск 87/20. Махачкала, 2020г.
5. Вехов В. Б., Ковалев С.А. Проблемы борьбы с кибертерроризмом // Правопорядок: история, теория, практика. - 2018. - № 1(16). - С. 89-93.
6. Черных, С. Н., Зуева С. Н. Информационная война: от прошлого к настоящему // Научное мнение. - 2018. - № 3. - С. 47-53.
7. Чугунова К.Ю. Информационное оружие как угроза национальной безопасности Российской Федерации/ Актуальные проблемы российского права, Том 1 № 1(1) январь 2015г.
8. Козориз Н.Л. Информационная безопасность в глобальном информационном пространстве // Право и государство. 2013. № 7. С. 146-150.
9. Марков А.А. Некоторые аспекты информационной безопасности в контексте национальной безопасности // Вестник СПбГУ. Сер. 12. 2011. Вып. 1. С. 26-35.
10. Расторгуев С.П. Информационная война. М.: Радио и связь, 1999. 416 с.