

*А.А. Гузова, А.Н. Круница,
студенты ФП БГЭУ
Научный руководитель – к.полит.н. Н.Ю. Веремеев*

КИБЕРБЕЗОПАСНОСТЬ

Кибербезопасность (или информационная безопасность) – это область знаний, практик и технологий, которые направлены на защиту компьютерных систем, сетей, программного обеспечения и данных от угроз, связанных с киберпреступностью, кибершпионажем, кибератаками и другими формами киберугроз. В нашем современном информационном обществе, где компьютерные системы и сети играют ключевую роль во многих аспектах жизни, кибербезопасность стала критически важной. Мы хотим выделить основные аспекты кибербезопасности на примере киберугроз:

1. Защита паролей: Используйте сильные пароли для всех учетных записей и регулярно их обновляйте. Пароли должны быть уникальными и содержать комбинацию букв, цифр и специальных символов.

2. Обновления и патчи: Регулярно обновляйте все программное обеспечение на компьютерах и устройствах, включая операционные системы, браузеры, антивирусные программы и другие приложения. Обновления и патчи часто содержат исправления уязвимостей, которые могут быть использованы хакерами.

3. Антивирусное программное обеспечение: Установите надежное антивирусное программное обеспечение на все устройства и регулярно обновляйте его. Антивирусная программа может обнаруживать и блокировать вредоносные программы, вирусы и другие угрозы.

4. Образование и осведомленность: Обучите себя и своих коллег / сотрудников основам кибербезопасности. Распространяйте информацию об основных методах атак, фишинге, социальной инженерии и т.д. Учитесь распознавать подозрительные электронные письма, ссылки и вложения, чтобы избегать попадания в ловушки.

5. Резервное копирование данных: Регулярно создавайте резервные копии всех важных данных и храните их в отдельном и защищенном месте. Резервные копии помогут восстановить данные в случае атаки или потери данных.

Кибербезопасность играет важную роль в защите частной информации, бизнес-данных, государственных секретов и общественной безопасности. Эффективная кибербезопасность требует постоянного внимания, инвестиций в технические и организационные меры безопасности, а также осведомленности и ответственности со стороны всех участников информационного пространства.

Информационная война – это конфликт, в котором стороны используют информационные средства и методы для достижения своих целей и влияния на общественное мнение, как правило, враждебно настроенных стран или организаций.

В информационной войне стороны стремятся контролировать поток информации, чтобы повлиять на оппонента или дестабилизировать его, дезориентировать противника. Они могут использовать различные методы, такие как:

1. Пропаганда во время войн: Во время вооруженных конфликтов стороны могут использовать мощные информационные механизмы для распространения пропаганды и манипуляции общественным мнением. Например, во время войны в Сирии различные стороны использовали социальные сети, чтобы распространять свою точку зрения и дезинформацию о противнике.

2. Манипуляция фейковыми новостями: В Интернете появляется все больше фейковых новостей, которые могут быть использованы в информационной войне. Примером может служить распространение ложных сообщений о катастрофах, терактах или других событиях с целью вызвать панику и нестабильность.

3. Создание ботов и аккаунтов для манипуляции: В информационной войне могут быть использованы боты и фейковые аккаунты в социальных сетях для массового распространения определенной информации или манипуляции общественным мнением. Например, такие аккаунты могут создавать и распространять сообщения, поддерживающие определенную политическую точку зрения или дискредитирующие оппонентов.

4. Экономические интересы: Коммерческие организации и компании могут вступать в информационную войну для защиты своих бизнес-интересов или уклонения от негативного общественного мнения. Например, компании могут использовать техники репутационной информационной войны для подрыва конкурентов или скрывания недостатков своих продуктов.

Это лишь несколько примеров информационной войны. Она становится все более актуальной в современном мире, поскольку информационные технологии играют все более важную роль в нашей жизни.

Литература:

1. Панарин, И. Н. СМИ, пропаганда и информационные войны / И. Н. Панарин. – М. : Поколение, 2012. – 260 с.
2. Воронцова, Л. В. История и современность информационного противоборства / Л. В. Воронцова, Д. Б. Фролов. – М. : Горячая линия – Телеком, 2006. – 192 с.
3. Гриняев, С. Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. – Минск : Харвест, 2004. – 448 с.
4. Гриняев, С. Н. Интеллектуальное противодействие информационному оружию / С. Н. Гриняев. – М. : Синтег, 1999. – 232 с.
5. Колесов, Э. Е. Информационная война в военных конфликтах второй половины XX столетия: исторический аспект / Э. Е. Колесов. – Киев : Национальная академия обороны Украины, 2007. – 345 с.