Список використаних джерел

1. Кубрякова Е.С. Вербальная деятельность СМИ как особый вид дискурсивной деятельности / Е.С. Кубрякова, Л.В. Цурикова // Язык средств массовой информации: учеб. пособие для вузов / под ред. М.Н. Володиной. – М.: Академический Проект: Альма Матер, 2008. – С. 183–209.
2. Почепцов О.Г. Языковая ментальность: способ представления мира / Почепцов О.Г. // Вопросы языкознания. – 1990. – № 6. – С. 110–122.

DOI: http://doi.org/10.31617/k.knute.2019-03-19.68

КІБЕРНЕТИЧНА ВІЙНА ЯК РІЗНОВИД ІНФОРМАЦІЙНОЇ ВІЙНИ

Ткачук К. О.
студентка 3 курсу
кафедра маркетингу
Гамова І. В.
к.е.н., доцент
кафедра журналістики та реклами
Київський національний торговельно-економічний університет, Україна

Ключові слова: *кібернетична війна, кібервійна, мережа Інтернет, інформаційні війни, кіберпростір, кібербезпека, кіберзахист, кібератака.*

Keywords: *cyber warfare, cyberwar, Internet, information wars, cyberspace, cybersecurity, cyberdefense, cyberattack.*

З початком розвитку інноваційних технологій і мережі Інтернет, стало очевидним, що це новий період війн – війни сьомого покоління. Сьогодні технології та мережа Інтернет найбільш впливають на людство і є достатньо динамічними. Однією з нових форм воєн, які виникли в цю еру, є кібернетична війна. Це зручна зброя, адже мережею Інтернет користуються всі, і тому вплив може бути здійснений не лише на певну країну, а на весь світ. Така зброя постійно вдосконалюється, через розвиток технологій.

Професор О. О. Мережко дає таке визначення кібервійни: «Кібервійна – використання Інтернету й пов'язаних з ним технологічних і інформаційних засобів однією державою з метою заподіяння шкоди

військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету іншої держави» [1]. З точки зору експерта в області кібербезпеки Р. Кларка: «Кібервійна – це дії однієї національної держави з проникнення у комп'ютери або мережі іншої національної держави для досягнення цілей нанесення збитку або руйнування» [2]. Є й інші зарубіжні та вітчизняні дослідники об'єктом дослідження яких є кібервійни. Тому сьогодні не існує певного сталого визначення цього терміну, але суть залишається незмінною. Хакери (ті, що видобувають інформацію) та кракери (ті, що псують програмно-апаратні засоби) – є головними діючими особами в таких війнах [3, с. 56].

Існують такі форми прояву кібервійн:

- вандалізм – псування інтернет-сторінок, зміна змісту негативними або пропагандистськими матеріалами;
- пропаганда – поширення звернень, що закликають до певних дій, або розміщення відповідної інформації на чужих Інтернет-майданчиках;
- збір інформації – зламування сторінок приватних осіб або окремих організацій для отримання закритої інформації;
- відмова сервісу – атаки з різних комп'ютерів для унеможливлення функціонування сайтів чи комп'ютерних систем;
- втручання в роботу обладнання – атаки на комп'ютери, що виконують адміністративно-контрольні функції в державних, громадських, військових та комерційних організаціях;
- атаки на об'єкти критичної інфраструктури – напад на комп'ютери, що контролюють життєдіяльність міст, зокрема телефонних ліній, водопостачання, електропостачання, пожежної безпеки, транспортного сполучення тощо [3, с. 56–57].

Кібернетичні війни можуть бути технологічними та інформаційними. Яскравим прикладом інформаційної кібервійни є соціальна мережа «Вконтакте», яка містить в собі достатньо пропаганди проти України, проте все ще залишається однією з соціальних мереж, яку відвідують українці (незважаючи на офіційну заборону). За рахунок того, що дана соціальна мережа є російською, користувач автоматично надає всю інформацію російським правоохоронним органам.

Багато країн вже починають розуміти, що чим нижчий рівень кібербезпеки держави, тим більші шанси зазнати ураження від кібератак по інформаційній та інших системах, базах країни. Тому вони потребують постійного покращення кіберзахисту, а особливо Україна. Відповідно до Законодавства України: «Кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також захо-

дів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [4]. Відомим сучасним прикладом кібервійни є російсько-українська кібервійна, яка почалася в 2013 році з російської атаки на інформаційні системи приватних підприємств та державні установи України.

Початок кібервійни передбачає кібератаку. Кібератака відбувається безпосередньо в кіберпросторі – віртуальний простір, в якому можна здійснювати комунікації в мережі Інтернет. Законодавство України визначає кібератаку, як спрямовані або навмисні дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій задля досягнення однієї або сукупності певних цілей [4].

Незважаючи на масштаб та наслідки кібервійн, американській вчений Мартін Лібікі зазначає, що за допомогою кібервійни неможливо роззброїти супротивника, окупувати його територію або змінити політичний режим в країні [5]. Проте все це на фізичному рівні, а той, хто контролює кіберпростір, має значні переваги, включаючи контроль над інформацією і майже всім світом.

Список використаних джерел

1. Мережко О. О. Проблеми теорії міжнародного публічного та приватного права / О. О. Мережко. – 2010. – Режим доступу: www.twirpx.com/file/1827023.
2. Слободянюк А. В. Аналіз небезпеки кібервійни на сучасній світовій арені. / А. В. Слободянюк. – 2017. – Режим доступу: conferences. vntu.edu.ua/index.php/all-hum/all-hum-2017/paper/download/2332/1739.
3. Курбан О. В. Сучасні інформаційні війни у мережевому он-лайн просторі: навч. посіб. / О. В. Курбан. – Київ, 2016. – С.56–57.
4. Закон України: Про основні засади забезпечення кібербезпеки України / Законодавство України. – 2018. – Режим доступу: zakon3.rada.gov.ua/laws/show/2163-19.
5. Запорожець О. Ю. Кібервійна: концептуальний вимір. / Actual problems of international relations. Release 121 (part I). / О. Ю. Запорожець. – 2014. – Режим доступу: journals.iir.kiev.ua/index.php /apmv/ article/download/2378/2111.