УДК 327-049.5 "20"(06)

КРИЗА КІБЕРБЕЗПЕКИ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ: НАСЛІДКИ КІБЕРАТАК

Павлюх М. В.
кандидат наук із соціальних комунікацій,
асистент кафедри міжнародної інформації,
Національний університет «Львівська політехніка»

Розвиток та поширення мережі у світі не тільки сприяє розвитку особистості та створює можливості її всебічного розвитку. Мережа стала середовищем злочинності та аферизму. Кіберзлочинність у Павутині ведеться на усіх рівнях: від особистісного спілкування до загрози національній безпеці.

Російсько-українська кібервійна – складова протистояння між Росією та Україною з періоду розпаду СРСР, яке у 2014 році переросло у відкрите збройне протистояння – російсько-українську війну. В більш загальному значенні, воно є частиною глобального протистояння Росії і Заходу. Перші атаки на інформаційні системи приватних підприємств та державні установи України фіксували під час масових протестів у 2013 році. Російсько-українська кібервійна стала першим конфліктом у кіберпросторі, коли була здійснена успішна атака на енергосистему з виведенням її з ладу.

З 2013 року була створена організація для впливу на суспільну думку, яка стала широко відомою як «тролі з Ольгіна». Вже у 2014 році ольгінські тролі стали активно працювати над формуванням на Заході суспільної думки, необхідної кремлівському режиму. Навіть через два роки після початку війни, у 2016 році, була виявлена мережа ботів у соцмережах, які поширювали в Інтернеті заклики до насилля проти української влади та заклики виходити на «Третій Майдан». Російські провладні Інтернет-ЗМІ та відповідні активісти в соціальних мережах показали дуже високу активність напередодні та під час анексії Криму. Низка російських сайтів, що займаються постійним інформаційно-психологічним протиборством на українському напрямі, активно висвітлювали події, що відбуваються, розміщували публікації з неперевіреною та неправдивою інформацією, здійснювали активне поточне аналітичне коментування ходу подій. Залучення платних тролів, мереж ботів, створення сайтів з викривленими «новинами» стало невід'ємною частиною російської пропаганди, оскільки, як свідчать експерименти, вплив пропаганди на людину тим ефективніший, чим

більше джерел надходження інформації, чим більшою підтримкою вона користується серед решти членів спільноти.

Кіберзагрози українській державі та суспільству умовно можна розділити на два ключових рівні (Д. Дубов, 2014). Перший – «класичні» кіберзлочини – як абсолютно оригінальні, так і вже звичайні, які для своєї реалізації, потребують лише сучасних інформаційних технологій. Другий – злочини, характерні для геополітичної боротьби (або такі злочини на місцевому рівні, які мають потенціал вплинути на політичне становище держави): хактивізм, кібершпигунство та кібердиверсії. Водночас техніки здійснення атак в обох випадках демонструють чимало спільного. Наприклад, фішингові техніки можуть бути використані як для заволодіння коштами громадян, так і з метою кібершпигунства (Д. Дубов, 2014).

Після початку збройної агресії Російської Федерації проти України компанії, що спеціалізуються на наданні послуг кібербезпеки, стали реєструвати зростання кількості кібератак на інформаційні системи в країні. Зазвичай кібератаки були націлені на приховане викрадення важливої інформації, ймовірніше для надання Росії стратегічної переваги на полі бою. Жертвами російських кібератак ставали урядові установи України, країн ЄС, Сполучених Штатів Америки, оборонні відомства, міжнародні та регіональні оборонні та політичні організації, аналітичні центри, засоби масової інформації, дисиденти. З початку російсько-української війни стали з’являтись загони антиукраїнських хактивістів, які називають себе «Кіберберкутом» та проукраїнською «Кіберсотнею Майдану», «Анонімусами» з російською або українською «пропискою».

Під час дочасних Президентських виборів в Україні 2014 року фахівцями CERT-UA було знешкоджено атаки на автоматизовану систему «Вибори». 21 травня 2014 року зловмисники з угруповання КіберБеркут здійснили успішну кібератаку на інформаційну систему «Вибори» Центральної виборчої комісії України. Їм вдалося вивести з ладу ключові мережеві вузли корпоративної мережі та інші компоненти інформаційної системи ЦВК. У результаті атаки, «Перший канал» російського телебачення повідомив своїм глядачам про те, що найбільшу кількість голосів виборців у першому турі на виборах Президента України набрав лідер Правого сектору Дмитро Ярош. Про це йшлося у випуску вечірніх новин, присвяченому позачерговим виборам Президента України.

Висновки. Служби соціальних мереж стали інструментом координації не лише російських пропагандистів, а й російських шпигунів на території України, бойовиків з Росії та загальної організації діяльності терористичних організацій, керованих російськими спецслужбами. Завдяки вдалому використанню (серед іншого) методів соціальної інженерії

активістам центру «Миротворець» вдалося взяти під контроль обліковий запис російської терористки Олени Гейштерової в соціальній мережі «Одноклассники».

Список використаних джерел

1. Білан Н. Б. Особливості Інтернет-комунікації / Н. Б. Білан // Наукові записки Інституту журналістики. – 2015. – Т. 59. – С. 51–54.

2. Доценко Э. Л. Психология манипуляции: феномены, механизмы и защита: монографія / Э. Доценко. – Москва, 2000. – 344 с.

3. Дубов Д. В. Забезпечення національних інтересів України в глобальному та національному кіберпросторах / Д. В. Дубов // Кіберпростір як новий вимір геополітичного суперництва: монографія. – Київ, 2014. – 328 с.

4. Кастельс М. Информационная эпоха: экономика, общество и культура: монографія / М. Кастельс. – Москва, 2000. – 680 с.

5. Могилко С. В. Тролінг як спосіб психологічної маніпуляції в Інтернеті [Електронний ресурс] / С. В. Могилко. – Режим доступу: // http://sjournal.cdu.edu.ua/base/2008/v4/v4pp57-60.pdf.