Базарний С.В. ад'юнкт кафедри ЗІТ та ІБ Національного університету оборони України ім. І. Черняховського

ПРОБЛЕМИ ТА НАСЛІДКИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ НА СИСТЕМУ МАСОВОЇ КОМУНІКАЦІЇ З МЕТОЮ ДЕСТАБІЛІЗАЦІЇ ПОЛІТИЧНОЇ СИТУАЦІЇ В КРАЇНІ

З початком повномасштабного вторгнення російської федерації на територію України, ворог розпочав не тільки ведення активних бойових дій а й застосував технології інформаційних операцій. На підставі аналізу відкритих джерел на початковому етапі проведення «спеціальної воєнної операції» рф (далі СВО), на території України було встановлено та зафіксовано в інформаційній безпеці наступне:

1. Результати, яких зс рф спромоглися досягти в інформаційному просторі:

досягли повної підтримки населенням рф дій влади;

не сприйняття міжнародною спільнотою агресивної та загарбницької політики рф проти України;

насичення інформаційного простору рф інформацією про «перемоги» зс рф підчас проведення СВО;

провалом заходів введення в оману Збройні Сили України, далі ЗСУ;

вороже ставлення населення України до бойових дій зс рф;

паніка населення на тимчасово окупованих територіях.

2. Для отримання достовірної інформації, у кожній області створено офіційні Telegram-канали голів облдержадміністрацій[1].

3. Для подання інформації про пересування та місцезнаходження частин, підрозділів та ворожої техніки створені чат боти.

4. Першочергове завдання інформаційного спротиву проти рф стало блокування #давайзамир, які розповсюджують російську (проплачену) пропаганду. Можна дійти висновку, що їм байдужа цільова аудиторія, тому для блокування їх треба робити наступне:

переходимо за посиланням-тиснемо на аккаунт-тиснемо на три крапки зверху праворуч-«скарга»-«поскаржитися на аккаунт»– «неприйнятний

контент»– «пропаганда ненависті»-«відправити».

5. Відбулися суттєві зміни щодо правил користування у соціальних мережах, один з вагомих прикладів:

Meta тимчасово дозволять закликати до насильства щодо Путіна, російської армії та росіян [2].

6. В російському інформаційному просторі з'явився цікавий документ, де узагальнюється досвід війни з Україною, який контрастує з доповідями російських генералів про те, що під контролем і хід самої операції, її строки, досягнення цілей та мети. В цьому полягає велика помилка та складність ситуації, яка склалася для ворога.

Група відповідальних за ідеологічний напрямок, яка займалася створенням проросійських настроїв на території України допустила провал СВО по всіх напрямках. Підставою для такого прозріння стало вибухом «інформаційної бульбашки», в якій тримали президента рф В. Путіна, якого по каналах фсб/свр/гру накачували стратегічною та тактичною дезінформацією, щодо підготовки до вторгнення в Україну, розповідаючи йому байки про військову слабкість українського народу та «беззубість» колективного Заходу, про незначні ефекти для економіки рф від СВО, яка була розрахована максимально до 2 травня.

Результати, яких зс рф спромоглися досягти в кіберпросторі:

"зламання" сайтів силових структур та розміщення на них фейкової інформації;

часткове створення сприятливих умов в інформаційному просторі щодо оточення ЗСУ;

не готовність населення тимчасово окупованої території відкрито висловлювати негативне ставлення стосовно ЗСУ;

повний провал в поширенні панічних настроїв серед особового складу ЗСУ;

повний провал в залякуванні військовослужбовців ЗСУ;

створено угруповання хакерів рф Killnet для ведення боротьби в

кіберпросторі;

угруповання хакерів рф Killnet заблокувало роботу сайту угрупованнями з кібербезпеки Anonymous;

розповсюджено шкідливе програмне забезпечення FormBook через e-mail jowhar@xintongwood.club для блокування, комп'ютерів, виведення із ладу систем управління об'єктів критичної інфраструктури, збору та передачі необхідної інформації до рф;

заблоковано сторінки в Facebook та e-mail Mirohost фізичних та юридичних осіб, які займаються питаннями інформаційної безпеки.

Для підтримки та безпеки України компанія Google посилила захист для українців через свої інструментарії:

тимчасово відключили деякі функції Google Maps в Україні, зокрема інформацію щодо автомобільного трафіку та завантаженості доріг;

додали інформацію про центри для біженців та мігрантів у сусідніх країнах.

Для юридичної та психологічної підтримки Google Startups Campus у Варшаві будуть надавати юридичну та психологічну підтримку біженцям з України. Google виділяє кошти місцевим організаціям, які допомагають біженцям, які прибувають до Польщі, а також для неурядових організацій у Словаччині, Румунії та Угорщині.

Google впровадила санкції та обмеження для росіян:

призупинили рекламу Google у Росії – більшу частину комерційної діяльності у рф, зокрема рекламу на ресурсах Google та в мережах по всьому світу для всіх російських рекламодавців, нові підписки на Cloud, Google Pay, функціонал для більшості сервісів та функції монетизації для глядачів YouTube у рф;

для протидії російській пропаганді продовжується робота щодо значного обмеження рекомендацій у всьому світі для низки російських державних ЗМІ на платформах Google. (У Європі видаляються з Google Play програми російських державних ЗМІ – RT та Sputnik. Відповідно до Регламенту Ради ЄС (ЄС) 2022/350, компанія видалила RT і Sputnik із результатів пошуку в Європейському

Союзі) [3].

Захист від DDoS-атак:

розширено право на участь у Project Shield, безоплатному захисті від DDoS-атак, щоб українські урядові вебсайти й посольства по всьому світу могли залишатися в мережі, захищати себе та продовжувати пропонувати свої найважливіші послуги. Понад 150 сайтів використовують цю технологію.

Висновки. Отже, можна стверджувати, що СВО стрімко стають важливим та ефективним інструментом політики національної безпеки, набувають ключових позицій в арсеналі спецслужб різних провідних країн світу а також нажаль і в росії. Цей факт, а саме проведення СВО рф на території України, змушує нас активно звернути увагу на проблематику побудови ефективної сучасної автоматизованої системи захисту від таких заходів, оперативного (бойового) управління, зв'язку, розвідки та спостереження. Набуває розвитку в секторі безпеки і оборони України спроможність ефективно реагувати на зростаючу кількість загроз у кіберпросторі та здатність забезпечувати автоматизацію процесів добування (збору), обробки, аналізу та відображення розвідувальної інформації, інформаційні технології, у тому числі електронні комунікації, здійснювати обмін інформацією про обстановку з державами – членами НАТО та державами – партнерами НАТО.

Список використаних джерел:

1.https://auc.org.ua/novyna/uvaga-oficiyni-kanaly-dlya-otrymannya-dostovirnoyi-informaciyi-u-kozhniy-oblasti.

2.(https://dev.ua/news/vkontakte1646919231?utm_source=tg&utm_medium=msg&utm_campaign=news_dev_ua_channel&utm_content=vkontakte_1646919231).

3.https://ko.com.ua/google_pidtrimuye_ukrayinu_po_vsim_napryamkam_140547