DOI: 10.18372/2410-7840.24.17377
УДК 004.946.5

ОСОБЛИВОСТІ АНТИУКРАЇНСЬКОГО ІНФОРМАЦІЙНОГО (КІБЕР) ВПЛИВУ НА УКРАЇНУ

Олександр Левченко, Володимир Охрімчук

З дня проголошення незалежності України її інформаційний простір, а з розвитком та впровадженням в усі сфери діяльності суспільства інформаційних технологій і кіберпростір постійно перебуває під потужним іноземним інформаційним та кібервпливами. Гібридна війна, розпочата росією у 2014 року змусило Україну переглянути свої підходи до забезпечення інформаційної та кібербезпеки. А з початком широкомасштабного вторгнення дане питання набуло особливої актуальності. Для ведення антиукраїнського інформаційного (кібер) впливу керівництво росії задіяло значні людські, матеріальні і фінансові ресурси, завдяки чому вдалося ефективно "промивати мізки" не тільки більшості своїх громадян, а й частині наших співвітчизників. Тому, на жаль, це призвело до підтримки частиною українських громадян агресивної політики кремля проти України. В статі здійснено аналіз основних інформаційних операцій росії проти України, а також здійснення кібератак на її критичну інформаційну інфраструктуру. В результаті аналізу встановлені особливості антиукраїнського інформаційного (кібер) впливу на Україну. Знання особливостей здійснення ворогом деструктивних дій в інформаційному та кіберпросторах дасть змогу створити в подальшому ефективні та дієві методи та засоби протидії їм.

Ключові слова: *інформаційна війна, інформаційне протиборство, інформаційно-психологічні впливи, інформаційна боротьба, кіберпростір, кібератака, кіберінцидент.*

ВСТУП

З дня проголошення незалежності інформаційний простір України, а з розвитком та впровадженням в усі сфери діяльності суспільства інформаційних технологій і кіберпростір постійно знаходиться під потужним іноземним інформаційним та кібервпливами. Проте, починаючи з 2014 року, застосування росією технологій гібридної війни, яка переросла у відкриту широкомасштабну війну проти України змусило її відбивати агресію не тільки на суші, у повітрі і морі, а й у інформаційному та кіберпросторах.

Ворог використовує найновіші інформаційні технології для здійснення антиукраїнського інформаційного (кібер) впливу в інформаційному просторі України, власному інформаційному просторі та інформаційних просторах інших держав світу, оскільки наслідки таких впливів мають своє відображення на нашій державі. Це в свою чергу значно ускладнює вживання заходів протидії таким впливам.

Отож, питання відбиття агресії у інформаційному та кіберпросторах залишається надзвичайно важливим, адже необхідно не тільки уміти протистояти наявним загрозам, але також прогнозувати імовірний розвиток подій.

Аналіз публікацій із проблем забезпечення інформаційної та кібербезпеки свідчить про істотний інтерес зарубіжної і вітчизняної наукової спільноти до цієї теми, що зумовлено постійно зростаючим значенням інформаційної боротьби у розв'язанні міждержавних протиріч. Багато закордонних та українських учених зосередилися на дослідженнях походження інформаційних воєн. У роботах [1-4] та багатьох інших наводяться результати всебічного аналізу інформаційної складової локальних війн і збройних конфліктів останніх десятиліть, умов, причин, форм і способів інформаційного протиборства. Робиться висновок про надзвичайну роль інформаційного впливу (ІВ) в досягненні цілей воєнних конфліктів.

Водночас ряд учених присвятили свої дослідження більш глибокому вивченню питань саме ведення інформаційної боротьби, зокрема організації інформаційних операцій, акцій та інших заходів ІВ [5-8] тощо.

Таким чином, аналіз останніх досліджень і публікацій за визначеною темою показав, що вивчення особливостей здійснення інформаційного та кібервпливів дає змогу вироблення ефективних методів та заходів їх протидії, а у окремих випадках й спрацювати на випередження ворога.

ОСНОВНА ЧАСТИНА

Інформаційний простір України протягом тривалого часу знаходиться під потужним іноземним інформаційним тиском. Цей тиск здійснюється як із боку російської федерації, так і з боку окремих держав світу, зокрема США, Німеччини, Великої Британії, Франції, а також і від суміжних з Україною держав, насамперед Польщі, Угорщини, Румунії. Безперечно, найбільший ІВ на населення України здійснюють засоби масової інформації росії [9,10].

Однак цей деструктивний ІВ на Україну і її населення розпочався задовго до війни, ще з часу оголошення нашою державою незалежності 24 серпня 1992 року. З огляду на різні чинники він то посилювався, як, наприклад, під час провокації навколо українського острова Тузла, в період так званих "газових воєн" 2008-2009 років чи коли до влади в Україні прийшла команда Президента В. Ющенка, то послаблювався, як за В. Януковича. Але ніколи цей вплив на Україну й українців не припинявся. Його метою у всі ці роки було встановлення повного контролю над зовнішньою та внутрішньою політикою України і, таким чином, утримання її у сфері свого геополітичного впливу.

Характерним є те, що весь російський вплив здійснювався системно у формі інформаційних операцій та акцій, які проводилися в рамках перманентної антиукраїнської інформаційної кампанії в усіх без винятку сферах життєдіяльності держави – зовнішньополітичній, внутрішньополітичній, економічній, воєнній, військово-технічній, інформаційній та інших.

При цьому головні інформаційні зусилля росії весь цей час були спрямовані на досягнення таких цілей:

у зовнішньополітичній сфері – блокування європейського вектору руху Української держави, протидія євро- і євроатлантичній інтеграції та спонукання до вступу до політичних і економічних союзів під проводом кремля [11];

у внутрішньополітичній сфері – створення керованого хаосу в нашій державі для внесення розколу серед населення України і створення сприятливого підґрунтя для реалізації подальших планів москви;

в економічній сфері – зменшення інвестиційної привабливості української економіки та дискредитація іміджу Української держави як надійного торговельного партнера, надійного транзитера енергоносіїв до Європи; забезпечення розширення присутності російського бізнесу в Україні та просування власних російських економічних інтересів [12];

у військово-технічній сфері – послаблення позицій України як одного з основних конкурентів росії на світовому ринку військової техніки та озброєнь через формування у західної світової аудиторії думки про контрабандне постачання Україною військової техніки та озброєння до конфліктних регіонів світу, підтримку зброєю терористів, про неякісне українське озброєння тощо;

в інформаційній сфері – стійке нарощування російської інформаційної присутності і, зрештою, фактичне домінування в окремих сегментах інформаційного простору України в інтересах охоплення і впливу на свідомість максимальної частки населення нашої країни [13].

З 2014 року метою антиукраїнського ІВ стає створення умов для ліквідації України як унітарної незалежної держави, її розвалу і поділу на три частини: Новоросію, що мала б приєднатися до росії, західну частину, яку росія пропонувала б приєднати до Польщі й Угорщини, та центральну частину, на якій було б встановлено підконтрольну москві владу.

Нова надзвичайно агресивна і потужна інформаційна кампанія з руйнування української державності розгорнулася на декількох напрямах у формі інформаційних операцій, які в результаті аналізу всіх наявних ознак можна ідентифікувати таким чином:

- інформаційна операція з дестабілізації внутрішньої ситуації в Україні, в рамках якої здійснюється: провокування масових акцій громадянської непокори; штучне підігрівання суперечностей між основними політичними силами та їх лідерами щодо шляхів "виведення з кризи" національної економіки, "завершення війни на Донбасі" тощо; підбурювання населення окремих регіонів України до сепаратизму, зокрема на Закарпатті і Буковині (поширення закликів до створення "русинської автономії", "Бессарабської народної республіки" тощо), провокування суспільно-політичного і територіального розколу між населенням Сходу і

Заходу України, розпалювання міжконфесійного протистояння з одночасним наданням інформаційної підтримки УПЦ Московського патріархату та приниженням і звинуваченням у неканонічності новоствореної Православної церкви України [9];

- інформаційна операція із заперечення української державності, в рамках якої на населення України, Західної Європи й Америки та власне російське населення здійснюється потужний ІВ щодо заперечення існування України як окремої держави, просування теорії про її утворення як "геостратегічного проекту Заходу". Посилено нав'язується думка про дезінтеграцію і розпад України як неминучий і закономірний фінал "штучно створеної держави";
- інформаційна операція з дискредитації української влади, в рамках якої активно поширюються провокаційні матеріали щодо неспроможності української влади стабілізувати внутрішньополітичну ситуацію в державі, корумпованості керівництва України та відстоювання лідерами провідних політичних сил виключно власних фінансових і політичних інтересів, нагнітання соціально політичної напруженості та роздмухування невдоволення громадян політикою діючої влади, формування недовіри до вищого державного керівництва України та органів державної влади;
- інформаційна операція з послаблення зовнішньої підтримки України, в рамках якої зусилля російських ЗМІ зосереджуються на звинуваченні України у зриві Мінських домовленостей та невиконанні нею взятих на себе зобов'язань щодо надання особливого статусу самопроголошеним псевдореспублікам "ДНР" і "ЛНР" і проведення виборів на непідконтрольних територіях, на поширенні думки про нібито зацікавленість української влади у продовженні збройного протистояння на Сході країни, на формуванні в країнах Заходу негативного іміджу України як держави, яка ніколи не була самостійною і завжди залежала від росії, а тому неспроможна існувати окремо і бути самостійним об'єктом міжнародної політики, на поширенні фактів про нібито підтримку Українською державою ідей нацизму і фашизму;
- інформаційна операція з протидії євроінтеграційному і євроатлантичному курсові України, в рамках якої російські і проросійські ЗМІ намагаються формувати в нашого населення негативне ставлення до ЄС та НАТО, акцентуючи увагу на кризових явищах та протиріччях між країнами Євросоюзу та стверджуючи, що Україна буде сировинним придатком, а не рівноправним членом ЄС;
- інформаційна операція з провокування ворожнечі між Україною та країнами-сусідами, в рамках якої всіляко спонсоруються ультраправі сили в Польщі, Угорщині і Румунії та підбурюються до висунення історичних і територіальних претензій нашій державі. На жаль, дії цих сил досягають певного успіху. Під їх впливом польські політики вже прийняли ряд рішень, які зачіпають інтереси нашої держави. Також за підтримки росії Угорщина висуває претензії до України щодо нібито обмеження прав і свобод етнічних угорців, що проживають у прикордонних районах, зокрема їх переслідування українською владою за подвійне громадянство та обмеження у мовному питанні;
- інформаційна операція з легітимації "російського статусу" Криму і створення умов для реінтеграції з Україною на умовах Кремля окремих районів Донецької і Луганської областей. Метою цієї операції прогнозовано є фактичне визнання міжнародною спільнотою Криму територією росії та погодження на "особливий статус" Донбасу. З цією метою російські і закордонні проросійські ЗМІ тиражують тези щодо історичної належності півострова ще російській імперії, про "значне покращення" соціально-економічної ситуації в Криму з його включенням до складу РФ та безперспективність його повернення до складу України. Одночасно російські ЗМІ проводять "деукраїнізацію" окупованих територій, витісняючи українську мову, дух і релігію з усіх сфер життєдіяльності.

Окрім наведених вище основних і вже перманентних інформаційних операцій росія проводить ситуативно, залежно від обстановки, що виникає, й інші інформаційні операції, акції та атаки, які мають свою конкретну мету, але в кінцевому підсумку спрямовані на досягнення мети всієї інформаційної кампанії проти України: створення умов для ліквідації України як унітарної незалежної держави. Аналіз багаторічного ІВ на Україну з боку росії, зокрема безпрецедентних за агресивністю,

інтенсивністю і масштабами антиукраїнських інформаційних заходів останнього десятиліття, дозволяє виділити ряд принципових особливостей його організації і проведення [9].

1. Увесь антиукраїнський ІВ росії має виключно системний характер, багатогранність форм ведення і чіткі стратегічні цілі. Всі основні інформаційні заходи санкціонуються на вищому державному рівні, завчасно плануються, ретельно готуються і проводяться скоординовано [14]. Управління ІВ, зокрема формування стратегічних наративів, здійснюється безпосередньо в кремлі. При цьому вище державне керівництво особисто бере участь у започаткуванні ключових інформаційних акцій, надаючи своїми різкими заявами щодо України інформаційні приводи, які одразу супроводжуються широкою інформаційною підтримкою ЗМІ.

2. Антиукраїнський ІВ росії здійснюється на чотири стратегічні цільові аудиторії: на власне російське населення, на населення України, на населення на тимчасово окупованих територіях та на населення Західної Європи і США. У самій росії москва намагається виправдати свої невдачі на фронті шляхом протиставлення собі більш сильнішого ворога у вигляді колективного заходу та блоку НАТО, домагається лояльності росіян до своєї агресивної зовнішньої політики щодо України. При цьому кремль у прямому сенсі зомбує власне населення ненавистю до українців і намагається об'єднати російське суспільство довкола ідей великодержавності, шовінізму та експансіонізму.

В Україні російський ІВ спрямовується на зміну морально-етичних норм і цінностей, національної і релігійної самосвідомості та політичної орієнтації українців на користь москви, на внесення розколу серед населення України і створення сприятливого підґрунтя для реалізації подальших планів кремля.

Населення тимчасово окупованої території України зазнає потужного ІВ. Основні наративи, що звучать при проведенні ІВ це звинувачення в усіх бідах, обстрілах тощо українську владу та Сили оборони, створення ілюзії відбудови та покращення життя на захоплених територіях з метою заручення підтримки.

Європі і всьому світові Росія намагається нав'язати кремлівське бачення подій як виключно правильне та виправдати свої дії щодо України перед світовою спільнотою. Крім того значно посилюється антиукраїнський ІВ направлений на зменшення або повне припинення надання країнами заходу військової допомоги Україні.

3. До проведення антиукраїнських інформаційних заходів росія масштабно залучає національні, іноземні та створені на окупованих територіях України засоби масової інформації.

4. Важливу роль у здійсненні ІВ на населення України й особовий склад Збройних Сил відведено засобам мережної комунікації [15], зокрема російським соціальним мережам "Одноклассники", "ВКонтакте" і "Мой Мир", що належать інтернет-компанії *Mail.RuGroup*, яка лояльна до офіційного Кремля та підконтрольна російським спецслужбам.

5. Антиукраїнський ІВ росії характеризується виключною агресивністю, що значно зросла з початком російсько-української війни. У російських ЗМІ принижується українська мова і культура, паплюжиться все українське. Україна й українці показуються як недонарод, недонація, недодержава.

На всіх мешканців Західної і Центральної України навішуються ярлики: "укри", "хохли", "бандерівці", "нацисти", "фашисти" [16].

Існування Української держави взагалі заперечується, а наша історія крадеться з нахабним присвоєнням собі історичної спадщини Київської Русі.

Тривожним у цій ситуації є те. що таке перекручування історії на російський лад вже закладене в нових шкільних підручниках рф. а це означає, що наступні покоління росіян виростатимуть у зневазі до України та українців.

6. Російський ІВ проводиться надзвичайно нахабно, його цілком можна характеризувати як відверта брехня в очі всьому світові. У будь-яких інформаційних повідомленнях російських ЗМІ щодо України прослідковується необ'єктивність, перекручування і відверта маніпуляція фактами, неприхована брехня.

7. Для прихованого впливу на свідомість і підсвідомість українців росія вже більше двох десятиліть результативно використовує всі можливі інструменти "м'якої сили", а саме російських політиків, істориків, діячів культури і мистецтв, які просувають на терени України російську мову, масову

російську культуру, проросійські переконання і політичні ідеали.

8. Ще однією особливістю російського впливу на свідомість українців і приховане використання для цього релігії. І головним інструментом такого впливу є фактична філія Російської православної церкви в Україні (РПЦ) Українська православна церква, яку вже давно називають із приставкою "Московського патріархату" УПЦ МП. Ця церква формує у своїх парафіян лояльне ставлення до ідеї інтеграції України до російського релігійного та культурно-історичного просторів, докладає активних зусиль для просування так званого "руського міру", а по суті до відновлення контролю Росії над Україною [9].

З початком широкомасштабного російського вторгнення (24 лютого 2022 року) ворожа пропаганда набуває небувалих розмахів. Країна-агресор нічого не шкодує для досягнення своїх цілей в інформаційному та кіберпросторах. Так із січня по березень 2022 року з російського бюджету витратили 130 млн. дол. на статтю "засоби масової інформації". У ці ж місяці 2021 року на ЗМІ було витрачено 40 млн. дол, тобто витрати зросли в 3,2 рази [17].

Таким чином, для ведення антиукраїнського ІВ керівництво росії задіяло значні людські, матеріальні і фінансові ресурси, завдяки чому вдалося ефективно "промивати мізки" не тільки більшості своїх громадян. а й частині наших співвітчизників. Тому, на жаль, це призвело до підтримки частиною українських громадян агресивної політики кремля проти України.

Проте війна в Україні точиться не лише на фронті та у інформаційному просторі, а й у кіберпросторі [18, 19].

Агресія росії в кіберпросторі почалася задовго до 2014 року, але триває й досі. Перед початком агресії проти України було розгорнуто кілька успішних кампаній кібершпигунства [19].

Перші атаки на інформаційні системи приватних підприємств та державних установ України було зафіксовано ще під час масових протестів наприкінці 2013 року. Уже тоді більше 22 підприємств та державних установ України були заражені комп'ютерним хробаком, який потім отримав назву "*Uroboros*" [102]. Головною метою його було викрадення інформації, в тому числі персональних даних та паролів доступу до інформаційних ресурсів.

Але у відкриту, тобто активну фазу війни в кіберпросторі росія перейшла в травні 2014 року, під час президентських виборів, коли російські хакери на 20 годин вивели з ладу інформаційну систему Центральної виборчої комісії України "Вибори".

Згодом у липні 2014 року офіційний веб-портал Президента України зазнав потужної *Distributed Denial of Service* (розподілена кібератаки типу "відмова в обслуговуванні", *DDoS*) атаки, протягом якої він декілька годин був недоступним, і пресслужба глави держави була змушена розповсюджувати інформацію через інформагентства.

З того часу кібератаки (КбА) стали більш масштабними, почали охоплювати енергетичну сферу та державні фінансові установи. Зокрема дії росії проти України стали першим випадком успішної КбА на цивільний об'єкт критичної інфраструктури. В ніч на 23 грудня 2015 року російськими хакерами було проведено успішну атаку на внутрішню мережу "Прикарпаття обленерго". В ту ніч було вимкнено близько 30 підстанцій, унаслідок чого близько 230 тисяч мешканців на кілька годин залишилися без світла. Нападники змогли отримати доступ до корпоративної мережі компанії завдяки вдалому зараженню комп'ютера одного із співробітників троянським ШПЗ "BlackEnergy" [20, 21].

Ще одну КбА на енергетичну сферу було здійснено 18 грудня 2016 року на підстанції "Північна" в Києві, коли протягом 2 годин через збій в автоматиці управління більшість споживачів північної частини правого берега Києва та прилеглих районів області залишилися без струму. В результаті втручання виникли збої в роботі телемеханіки й було відключено підстанції, від яких живиться низка стратегічних об'єктів області: підприємства, державні установи та населення [19].

Іншу масштабну КбА, під час якої постраждали сайти Міністерства фінансів, Держказначейства, Пенсійного фонду, було здійснено в грудні 2016 року. Унаслідок цієї КбА було знищено частину інформації, а також виведено з ладу обладнання. У зв'язку з цим сталися затримки з бюджетними виплатами на сотні мільйонів гривень. Для виведення з ладу серверів державних фінансових

установ зловмисники використовували "*KillDisk*" (програма для знищення файлів з комп'ютерів (серверів), а також троянську програму "*Black Energy*", ту саму, що і в атаці на "Прикарпаття обленерго" [19, 20]. Але наймасштабнішою атакою, яку на собі відчув кожен українець, вважається атака з використанням вірусу "*NotPetya*". Ця КбА відбулася 27 червня 2017 року, було заражено близько 12 тисяч персональних комп'ютерів, більшість із яких належала приватним українським організаціям, а також Уряду, банкам, державним енергетичним компаніям, київському аеропорту та метрополітену. Від атак постраждала значна кількість приватних компаній, торгові мережі (*METRO Cash&Carry, Novus, Fozzy*, Епіцентр, Рост тощо), телеком-оператори (Київстар, *Vodafone*, *Lifecell*), мережі заправних станцій (*WOG, KLO*), транспортні та енергетичні компанії.

Не виключенням стала і військова сфера. За словами екс-командувача Головного управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України генерал-лейтенанта Володимира Рапка починаючи з 2014 року, зафіксовано інтенсивне збільшення кількості КбА різного ступеня складності, направлених на порушення функціонування інформаційно-комунікаційних систем ЗС України [22]. Як правило, це *DDoS* атаки на системи й розповсюдження шкідливого програмного забезпечення.

Наприклад, одним із пристроїв кібербезпеки було зафіксовано *DDoS* атаки на веб-сайт Міністерства оборони України – більше 6 тисяч звернень до сайту на секунду [23].

За своєю географією найбільше атак відбувається з території Росії, але також можуть використовуватись майданчики союзних нам країн для проведення КбА, що ускладнює остаточну ідентифікацію.

Від початку війни тренд на зростання кількості КбА зберігається. Так, у ІІІ кварталі 2022 за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та КбА було опрацьовано 24 млрд. подій. Кількість зареєстрованих та опрацьованих кіберінцидентів зросла – від 64 до 115.

У ІІІ кварталі 2022 року фіксується істотне зростання активності хакерських груп щодо розповсюдження шкідливого програмного забезпечення, серед якого є як програми, що викрадають дані, так і ті, які спрямовані на знищення даних. Порівняно зі статистичними даними за ІІ квартал 2022 року, кількість кіберінцидентів з високим рівнем критичності зросла на 128%.

Порівняно з І та ІІ кварталами, у ІІІ кварталі 2022 року кількість критичних подій кіберінцидентів, джерелом яких є IP-адреси росії, зросла у 35 разів. Також, порівняно з ІІ кварталом 2022 року, майже вдвічі зросла кількість детектованих подій ІБ, пов'язаних із активним скануванням, джерелом яких є IP-адреси росії [24]. Проаналізувавши дії росії в кіберпросторі, можливо виділити ряд принципових особливостей їх організації і проведення.

1. Вплив на критичну інформаційну інфраструктуру здебільшого має перманентний характер.

2. Кіберпростір використовується росією як для проведення кібератак на Україну так і для проведення інформаційних операцій.

3. Завжди спостерігається активізація дій росії в кіберпросторі в період важливих подій, політичних чи економічних змін у країні. Крім того відбуваються збільшення кіберінцидентів перед початком бойових дій. Тож можна вважати, що КбА тісно пов'язані з проведенням військових, інформаційних операцій чи політичних кроків. Так, наприклад, більше ніж за місяць до повномасштабного вторгнення на територію України в середині січня росія провела масштабну КбА проти понад 20 українських урядових установ, намагаючись знизити здатність країни протистояти майбутньому воєнному нападу з боку москви.

4. Головні цілі росії у кіберпросторі наступні:

-шпіонаж (отримання розвідданих щодо логістики, озброєння, планів та операцій Сил безпеки та оборони);

-спроби виведення з ладу об'єктів критичної інформаційної інфраструктури;

-позбавлення доступу громадян до державних послуг та сервісів, банківського обслуговування тощо.

5. За атрибуцією абсолютна більшість кіберінцидентів пов'язана з хакерськими угрупуваннями, що фінансуються урядом рф. Зокрема, це *ARMAGEDDON / GAMAREDON /PRIMITIVE BEAR* (ФСБ рф), *SANDWORM* (ГУ ГШ ЗС рф

(ГРУ)), *APT28/FANCY BEAR* (ГУ ГШ ЗС рф (ГРУ)), APT29 / COZY BEAR (СЗР рф), *UNC 1151/ GHOSTWRITER* (Міністерство оборони рб), *XAKNET, KILLNET,* "Киберберкут" *Z - TEAM, CYBERARMYOFRUSSIA _ REBORN*, (проросійські кібертерористи) та інші [25].

ВИСНОВКИ

Таким чином, сьогодні Україна змушена протистояти широкомасштабній агресії росії не тільки на фізичному полі бою, а й у інформаційному та кіберпросторах. В результаті аналізу структури, змісту та особливостей антиукраїнського ІВ на Україну встановлено, що її інформаційний та кіберпростори знаходиться під постійним тиском із боку багатьох держав світу. Але найбільшого деструктивного впливу Україна зазнає від росії у формі надпотужної інформаційної кампанії з руйнування української державності, в рамках якої скоординовано проводяться інформаційні операції в усіх без винятку сферах життєдіяльності країни – зовнішньополітичній, внутрішньополітичній, , військово-технічній, економічній, воєнній, інформаційній та інших. Увесь російський вплив здійснюється виключно системно, із залученням великої кількості сил і засобів та задіянням значного фінансового ресурсу.

Кіберпростір, в свою чергу ворогом використовується як для здійснення кібератак на критичну інформаційну структуру України так і для проведення інформаційних операцій проти нашої країни.

Отже, знання особливостей здійснення ворогом деструктивних дій в інформаційному та кіберпросторах дасть змогу створити ефективні та дієві методи та засоби протидії їм.

ЛІТЕРАТУРА

[1] Інформаційні виклики гібридної війни: контент, канали, механізми протидії: аналіт. доп. / за заг. ред. А. Баровської. Київ: НІСД, 2016. 109 с.

[2] Почепцов Г. Г. Сучасні інформаційні війни. Київ: Києво-Могилянська академія, 2015. 497с.

[3] В. Хорошко, Ю. Хохлачова, Т. Пірцхалава, І. Іванченко Інформаційна зброя як інструмент інформаційної війни // Захист інформації. 2022. Т. 24, №2. С. 50–58.

[4] Почепцов Г.Г. Информационные войны. Москва: Релф-бук, 2001. – 576 с.

[5] Толубко В. Б., Рось А. О. Складові інформаційної боротьби // Наука і оборона. 2002. № 2. С. 23-28.

[6] Гапеєва О. Л. Міждержавне протиборство в інформаційній сфері на пострадянському просторі (1991-2017 рр.): історико-системне дослідження: монографія. Львів: "Тріада плюс", 2017. 424 с.

[7] Грищук Р. В., Канкін І. О., Охрімчук В. В. Технологічні аспекти інформаційного протиборства на сучасному етапі // Захист інформації. 2015. Т. 17, № 1. С. 80-86.

[8] Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ: Інтертехнологія, 2009. 164 с.

[9] Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: http : / / surl.li / ewssq (дата звернення: 25.01. 2023).

[10] Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія / О. В. Левченко. Житомир: ЖВІ, 2020. 180 с. ISBN 978-617-7992-08-9

[11] Солодкий С. Інтеграція України до ЄС: російський чинник. URL: http://surl.li/ewssl (дата звернення: 15.01.2023).

[12] Гібридна війна: сутність, виклики та загрози: зб. матер. Круглого столу (Київ, 8 липня 2021 р.). [Електронне видання]. Київ: НА СБУ, 2021. 189 с URL: https://academy. ssu. gov. ua /uploads/ p_57_28744724.pdf

[13] Левченко О. В., Косогов О. М. Методика виявлення заходів негативного інформаційного впливу на основі аналізу відкритих джерел // Системи обробки інформації. 2016. № 1 (138). С. 100-102.

[14] Радковець Ю. І. Ознаки технологій "гібридної війни" в агресивних діях Росії проти України // Наука і оборона. 2014. № 3. С. 36-42.

[15] Демартино А. П. "Криве дзеркало". Роль соціальних мереж в операції Російської Федерації з окупації Криму. Київ: Самміт-Книга, 2020. 248 с.

[16] Левченко О. В. Еволюція гібридної війни Російської Федерації проти України // Наука і оборона. 2017. № 2. С. 11-16.

[17] Росія втричі збільшила витрати на пропаганду під час війни з Україною URL: http://surl.li/ ewssh (дата звернення 1.02. 2023).

[18] Грищук Р. В. Основи кібернетичної безпеки: Монографія / Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.

[19] Охрімчук В. В. Метод побудови шаблонів потенційно небезпечних кібератак на комп'ютерні системи та мережі військового призначення : дис. канд. техн. наук: 21.05.01 / Охрімчук В. В. Житомир, 2021. 170 с.
[20] Кібератаки Російської Федерації. хронологія. URL: http: // surl. li / ewssc (дата звернення: 20.01.2023).
[21] Положенцев А., Гнатюк С. Black Energy як загроза об'єктам критичної інфраструктури України // "Information, communication, society" (ICS-2016). LVIV 2016. С. 32-33.
[22] Підрозділи кібернетичної безпеки Збройних Сил України перейшли на бойовий режим роботи. URL: http: // surl.li / ewsrw (дата звернення: 18.01. 2023).
[23] Під час захоплення українських кораблів були DDoS-атаки на сайт Міноборони. URL: http:/ /surl.li/ewsrt (дата звернення: 18.01.2023).
[24] Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки оперативного центру реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України URL: http: // surl. li / ewsrl (дата звернення: 27.01.2023).
[25] Толуб Н. Кібервійна рф проти України: як працюють російські хакери та воюють українські кібервійська. URL: http: // surl. li / ewssy (дата звернення: 28.01.2023).

FEATURES OF ANTI-UKRAINIAN INFORMATION (CYBER) INFLUENCE ON UKRAINE

Since the day of independence of Ukraine, its information space and cyberspace, after the development and implementation of information technologies in all spheres of society, are constantly under powerful foreign informational and cybernetic influences. The hybrid war launched by Russia in 2014 forced Ukraine to reconsider its approaches to ensuring information and cyber security. And with the beginning of a large-scale invasion, this issue became especially urgent. To carry out anti-Ukrainian information (cyber) influence, the Russian leadership used significant human, material and financial resources, thanks to which it was possible to effectively "brainwash" not only the majority of its citizens, but also a part of our compatriots. Therefore, unfortunately, this led to the support of a part of the Ukrainian citizens of the Kremlin's aggressive policy against Ukraine. The article analyzed the main information operations of Russia against Ukraine, as well as the implementation of cyber-attacks on its critical information infrastructure. As a result of the analysis, the features of anti-Ukrainian information (cyber) influence on Ukraine were established. Knowledge of the features of the enemy's destructive actions in the information and cyberspace will make it possible to create effective methods and means of countering them in the future.
Keywords: information war, information conflict, information and psychological influences, information struggle, cyber space, cyber-attack, cyber incident.

Левченко Олександр Віталійович, заслужений. діяч науки і техніки. України, доктор військових наук, професор, начальник Житомирського військового інституту імені С. П. Корольова.
Oleksandr Levchenko, honored science and technology figure of Ukraine, doctor of military sciences, professor, head of Korolov Zhytomyr military institute.
E-mail: zvir@post.mil.gov.ua.
Orcid ID: 0000-0001-6254-591X.

Охрімчук Володимир Васильович, кандидат технічних наук, професор кафедри захисту інформації та кібербезпеки Житомирського військового інституту імені С. П. Корольова.
Volodymyr Okhrimchuk, candidate of technical sciences, professor at the Chair of Information Protection and Cybersecurity of Korolov Zhytomyr military institute.
E-mail: okhrimchuk84@ukr.net.
Orcid ID: 0000-0001-7518-9993.

DOI: 10.18372/2410-7840.24.17378
УДК 004.7:004.056.5

МОДИФІКОВАНИЙ МЕТОД ВИЯВЛЕННЯ DDoS-АТАК ПРИКЛАДНОГО РІВНЯ НА РЕСУРСИ ВЕБСЕРВЕРІВ

Аркадій Кравчук, Володимир Погорелов

Кількість підключених до мережі Інтернет пристроїв збільшується щороку, разом з тим частішають випадки проведення DDoS-атак, які спричиняють простій атакованої системи. Основною проблемою захисту є вчасне виявлення атаки в режимі реального часу та встановлення її джерела. Атаки прикладного рівня схожі