7. Американська дизайнерка Вера Вонг та її команда підтримали Україну. *Радіо Maximum.* 14 березня 2022. URL: https://cutt.ly/uSpTVBA.

8. Як індустрія моди реагує на війну Росії з Україною. *Vogue.* 3 березня 2022. URL: https://cutt.ly/wSdC5Nq.

9. Разом з Україною: Джорджіо Армані провів показ у повній тиші. *Vogue.* 28 лютого 2022. URL: https://cutt.ly/xSd1BCC.

10. UKRAINE FOREVER: на знак підтримки України шотландці зареєстрували новий тартан. *Elle.* 12 березня 2022. URL: https://cutt.ly/OSd9xkY.

11. Джіджі Хадід пожертвує Україні кошти, які заробила під час тижнів моди. *Elle.* 8 березня 2022. URL: https://cutt.ly/ESd3ZRw.

12. Мей Маск підтримує Україну. Вона одягнула вишиванку від луцького бренду. *Перший – канал соціальних новин [сайт].* 13 березня 2022. URL: https://cutt.ly/1Sd5by1.

УДК 327.5:[004.056.5:343.326](470+571)

КІБЕРАТАКИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ: РЕАКЦІЯ МІЖНАРОДНОЇ СПІЛЬНОТИ

А. В. Савчук, Ю. В. Котик

Анотація: У статті висвітлено дії іноземних держав у відповідь на злочинну діяльність Російської Федерації у кіберпросторі, а також чим може бути небезпечна подібна практика РФ. Проаналізовано законодавчу базу, що є основою для відповідних контрзаходів. Виділено санкції, що найчастіше використовуються США та Європейським Союзом у відповідь на кібератаки.

Ключові слова: кіберсанкції, Російська Федерація, США, державні установи.

Останнім часом шпальти світових видань нерідко рясніють повідомленнями про кібератаки, що здійснені з території Російської Федерації або за замовленням її уряду. Атаки в основному спрямовані на державні установи: банки, сайти міністерств, стратегічно важливі об'єкти іноземних держав, а кіберактивність РФ проти України відбувається на постійній основі.

Будь-які зловмисні дії Російської Федерації в цифровому просторі не залишаються без уваги міжнародної спільноти. Зазвичай реагують ті, хто потрапив під приціл хакерів – тобто США або Європейський Союз.

Проте, спочатку варто зрозуміти чим небезпечні кібератаки Російської Федерації загалом і що їй потрібно. До прикладу, пристрасть Росії втручатися в президентські вибори інших держав розглядається як напад на народ, що загрожує цілісності та легітимності демократичного процесу, а також результатів виборів. Російські хакерські групи успішно отримують доступ до різноманітних серверів державних установ, військових даних. На додаток до загроз національній безпеці, які створюють ці атаки, мільярди доларів, які витрачає уряд на відновлення після атак і захист інформації, зокрема секретної, беруться з кишень платників податків. Крім того, існує кілька схем злому, спрямованих на персональні пристрої, включаючи телефони та комп'ютери, у спробі отримати конфіденційні дані користувачів. Банки та фінансові установи протягом останнього десятиліття зазнали численних атак з боку російських хакерських груп, що підкреслило ключові вразливі місця у фінансових системах держав. Також ними було створено найбільший ботнет (мережа комп'ютерів, заражена шкідливим програмним забезпеченням), коли-небудь виявлений, що дозволило їм викрасти дані для входу та паролі для десятків мільйонів онлайн-рахунків, включаючи банківські рахунки, що коштує жертвам великих грошей. На додаток до цих зломів, російський уряд використовує пропагандистські групи для націлювання на ЗМІ, намагаючись викликати паніку та створити загальне почуття недовіри до урядів [1].

Таким чином кібернетичні інструменти використовуються Росією в додаток до політичних та військових інструментів, щоб тиснути на Україну, США та Європу, щоб вони рухалися у напрямку постійних поступок російським інтересам.

Сфера кібербезпеки демонструє, що коли міжнародному середовищу не вдається знайти спільного рішення щодо реакції, мають місце дії одностороннього характеру. Односторонні кіберсанкції – це обмежувальні економічні заходи тимчасового характеру, що застосовуються проти фізичних, юридичних, державних органів та посадових осіб, які здійснюють, сприяють кібератакам або займаються іншою шкідливою кібердіяльністю. Вони вводяться без будь-якого попереднього дозволу регіональної чи міжнародної організації, тобто відповідно до внутрішнього законодавства штатів.

Сполучені Штати все ще залишаються серйозно вразливими до цілого ряду загроз кібербезпеці з боку Росії. Якщо їх не зупинити, російські кібероперації, ймовірно, і надалі будуть спрямовані на американські установи, інфраструктуру, лідерів і громадян. За словами колишнього директора Агентства національної безпеки Майкла С. Роджерса, хакерські атаки, у тому числі з Росії, коштують Сполученим Штатам «сотні мільярдів доларів» і призведуть до «справді значних, майже катастрофічних провалів, якщо ми не вживемо заходів» [2]. Кремлівські стратеги не так схильні до ризику, як Сполучені Штати, і тому розробили концепцію використання кіберінструментів для примусового впливу. Вони мають більш ніж 15-річний досвід використання цих інструментів. Хоча вони можуть порушити критичну інфраструктуру США, вони вирішили цього не робити. Найуспішнішим використанням Росією кіберінструментів проти Сполучених Штатів було створення фальшивих наративів, які посилюють політичні потрясіння в Сполучених Штатах та Європі [3].

Проте останнім часом США неодноразово попереджають Кремль про наслідки кібератак в тому числі і на Україну. Таким чином керівники Комітету Сенату США із закордонних справ заявляють, що російські кібератаки проти України будуть займати перше місце в списку дій, спрямованих на введення санкцій проти режиму Володимира Путіна. Президент Джо Байден заявив, що США помститься власними кібератаками, якщо Росія завдасть серйозного подібного удару в Україні, але публічно не зобов’язався вводити санкції за кібератаки.

Санкції можна вважати достатньо шкідливими для Росії, оскільки вони можуть калічити економіку та ізолювати Росію від міжнародної торгівлі. Раніше США вводили санкції проти Росії за атаки на американські цілі, наприклад, розгалужену шпигунську операцію SolarWinds, виявлену наприкінці 2020 року, під час якої російські хакери зламали комп’ютерні системи щонайменше десятка федеральних агентств і 100 приватних компаній [4]. Саме після операції SolarWinds, у червні 2021 року під час саміту Байдена-Путіна, президент Байден заявив, що критична інфраструктура повинна бути «заборонена» для кібератак і передав список з 16 областей критичної інфраструктури, які ні за яких обставин не повинні бути об’єктами кібератак [5]. Ця атака, а також багато інших (наприклад, NotPetya або WannaCry) ілюструють поточну проблему міжнародного права: відсутність обов’язкових норм, що регулюють поведінку в кіберпросторі. Як наслідок, у держав залишається лише кілька варіантів, як реагувати та запобігати зловмисній поведінці. Серед доступних альтернатив набирають обертів односторонні кіберсанкції. За атакою послідували жорсткі односторонні санкції США – точніше, санкції щодо суверенного боргу проти Росії та санкції проти шести російських технологічних фірм за підтримку кіберпрограми російських спецслужб.

Загалом, кіберсанкції США, ЄС та Великобританії можуть бути накладені проти фізичних або юридичних осіб, юридичних осіб або органів [6]. Наприклад, відповідно до системи кіберсанкцій США, санкції можуть бути накладені проти «будь-якої особи, визначеної міністром фінансів після консультації з генеральним прокурором та держсекретарем» на підставі того, що несе відповідальність за зловмисну кібер-діяльність або причетність до неї, або за те, що вона «прямо чи опосередковано бере участь у ній».

Крім того, американські рамки передбачають кіберсанкції проти осіб, які «матеріально допомагали, спонсорували або надали фінансову, матеріальну або технологічну підтримку, товари чи послуги» для шкідливої кібер-діяльності. Крім того, кіберсанкції США застосовуються до будь-кого, хто діяв або мав намір діяти прямо чи опосередковано від імені осіб, що підпадають під санкції. Більше того, будь-хто, хто намагався займатися будь-яким із вищезгаданих видів діяльності, також може бути підданий санкції. Поки що США ввели більше кіберсанкцій, ніж ЄС і Великобританія.

Європейський Союз вводить обмеження схожі до тих, що вводить США, але в свою чергу, у 2019 році блок запровадив правову основу для кіберсанкцій, а перші кіберсанкції були оголошені в липні 2020 року. Кілька країн, які не є членами ЄС, висловили бажання приєднатися до кіберсанкцій ЄС. Таким чином в рамках ЄС було створено свого роду структуру спільної дипломатичної реакції на зловмисну кібер-діяльність («Набір інструментів кібер-дипломатії»), яка потенційно повинна вплинути на поведінку можливих агресорів у кіберпросторі. В цьому документі здійснено, в першу чергу, понятійну роботу:

- що варто вважати кібератакою для ЄС;
- виділено дії в кіберпросторі, що можна розглядати як загрозу;
- фактори, які визначають, чи має кібератака значний вплив;
- яких кроків необхідно вживати державам-членам у випадку кібератаки або з метою її попередження (в основному заходи пов'язані з обмеженням пересування територією ЄС фізичних та юридичних осіб, що причетні до здійснення кібератак) [7].

Великобританія, яка офіційно вийшла з ЄС у січні 2020, заявила, що приєднується до блоку в застосуванні санкцій проти кібератак. Крім того Сполучене Королівство прийняло Регламент про кіберсанкції в 2020, який набув чинності в день виходу. В його основі лежить рішення Ради ЄС, проте він є значно конкретизованішим. Регламент накладає фінансові та імміграційні санкції з метою сприяння запобіганню відповідної кіберактивності. Для досягнення зазначеної мети встановлюється ряд заборон та вимог, а у разі їх порушення – відповідне покарання [8].

Щодо нормативного значення кіберсанкцій, вони можуть сигналізувати про «червоні лінії» неприйнятної поведінки в кіберпросторі і таким чином сприяти формуванню правил відповідальної поведінки в кіберпросторі.

Держави Європейського Союзу здатні також окремо від блоку запроваджувати санкції. Прикладом цього можна згадати кібератаку у квітні та травні 2015 року, що повністю паралізувала ІТ-інфраструктуру Бундестагу, і весь парламент довелося відключити на кілька днів, поки це було виправлено. Тоді Меркель публічно звинуватила Росію у хакерстві. В наслідок цього інциденту Німеччиною було запроваджено санкції у вигляді заморожування активів і заборони на поїздки проти керівника Генерального штабу Збройних сил Російської Федерації Ігоря Костюкова та офіцера розвідки Дмитра Бадіна. Міністр закордонних справ Великобританії Домінік Рааб заявив: «Велика Британія стоїть пліч-о-пліч з Німеччиною та нашими європейськими партнерами, щоб притягнути Росію до відповідальності за кібератаки, спрямовані на підрив західних демократій.

У свою чергу на початку грудня 2021 року в Австралії був прийнятий закон, який дозволяє застосовувати санкції у відповідь на значну зловмисну кіберактивність.

Натомість реакція Москви досить типова для неї: санкції розглядаються «ворожими кроками, які підвищують конфронтацію» з погрозами «дати рішучу відповідь» [9].

Існуючі кіберсанкції спрямовані на державні органи, а також на вищих урядовців, і, таким чином, можуть спричинити заморожування активів державних органів разом із забороною на поїздки для вищих державних службовців. Замороження активів державних органів теоретично може порушувати звичайне міжнародне право державного імунітету, але це є дискусійним питанням. Зокрема, не врегульовано, чи користується державним майном імунітет примусового виконання незалежно від наявності судового провадження. Заборони на поїздки, які заважають вищим державним службовцям виконувати свої функції, посягають на імунітет, гарантований таким посадовим особам міжнародним

правом, але цей імунітет гарантується лише посадовим особам, які представляють уряд і, отже, подорожують з цією метою до інших держав.

Односторонні кіберсанкції також можуть порушувати двосторонні угоди економічного характеру та зобов'язання Світової організації торгівлі. Запроваджуючи односторонні кіберсанкції, які або тягнуть за собою повний економічний бойкот осіб, що потрапили під санкції, як у випадку з кіберсанкціями США, або забороняють надання коштів та економічних ресурсів особам і організаціям, які потрапили під санкції, як це передбачено нормативними актами ЄС, держави відверто діють всупереч своїм зобов'язанням у СОТ. Крім того, кіберсанкції, такі як заморожування активів, майна та власності, можуть призвести до судових позовів про порушення справедливого та рівноправного поводження та інших стандартів режиму, включених до міжнародних інвестиційних угод.

Щодо нормативного значення кіберсанкцій, вони можуть сигналізувати про «червоні лінії» неприйнятної поведінки в кіберпросторі і таким чином сприяти формуванню правил відповідальної поведінки в кіберпросторі [10].

Не дивлячись на постійні спроби міжнародної спільноти «провчити» РФ, повномасштабний напад Росії на Україну яскраво показує, що усі спроби США та держав Європейського Союзу зовсім не є перешкодою на шляху до цілей, що поставила перед собою правляча еліта. Тому до цифрової боротьби до єдналась також найбільша хакерська група – Anonymous. Після відкритого оголошення кібер-війни цією групою ними було здійснено відключення веб-сайтів, що належать російському нафтовому гіганту «Газпрому», підконтрольному державі російському інформаційному агентству RT і численним державним установам Росії та Білорусі, включаючи офіційний сайт Кремля [11]. Таким чином кіберактивність проти України поки що приглушена, незважаючи на поширені прогнози, що військовий напад Росії на країну буде поєднуватися з цифровим шоком. В свою чергу українські веб-сайти зазнали DDoS-атак напередодні наступу, зокрема Міністерство оборони України та ПриватБанк.

Зрозуміло, що потрібен більш ретельний підхід до розуміння, запобігання та реагування на кібератаки в усіх секторах. Сполучені Штати та Європа явно вразливі до кібератак, і оскільки світ продовжує все більше залежати від електронних систем, ці вразливості будуть тільки зростати. Особливо тривожним у цій російській кібертактиці є той факт, що Росія є «єдиною країною на сьогоднішній день, яка поєднує кібервійну з нападами звичайних гармат і танків» і навряд чи Росія припинить їх використовувати найближчим часом.

Abstract. The article highlights the actions of foreign states in response to the criminal activities of the Russian Federation in cyberspace, as well as the dangers of such practices of Russia. The legal framework that is the basis for appropriate countermeasures is analyzed. The sanctions that are most used by the United States and the European Union in response to cyberattacks are highlighted.

Keywords: cyber sanctions, Russian Federation, USA, government agencies.

СПИСОК ЛІТЕРАТУРИ

1. Fuchs M., Kenney C., Perina A. Why Americans Should Care About Russian Hacking. American Progress. 14.02.2017. URL: https://www.americanprogress.org/article/why-americans-should-care-about-russian-hacking/
2. Pellerin C. Cybercom Chief Details U.S. Cyber Threats, Trends. U.S. Department of Defense. 21.11.2014. URL: https://www.defense.gov/News/News-Stories/Article/Article/603696/
3. Lewis J. Russia and the Threat of Massive Cyberattack. Center for Strategic and International Studies. 04.02.2022. URL: https://www.csis.org/analysis/russia-and-threat-massive-cyberattack
4. Miller M. On Ukraine, senators put cyberattacks top-of-list for sanctions. Politico. 09.02.2022. URL: https://www.politico.com/news/2022/02/09/senators-consider-sanctions-russian-ukraine-00007529
5. Soldatkin V., Pamuk H. Biden tells Putin certain cyberattacks should be 'off-limits'. Reuters. 17.06.2021. URL: https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/
6. Atwood K., Gaouette N. Biden imposes new sanctions on Russia in response to election interference and cyber hacks. 15.04.2021. URL: https://edition.cnn.com/2021/04/14/politics/russia-sanctions-expel-officials-hacking-election/index.html
7. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019D0797

8. The Cyber (Sanctions) (EU Exit) Regulations 2020. Legislation.gov.uk. URL: https://www.legislation.gov.uk/uksi/2020/597/contents/made
9. US imposes sanctions on Russia over cyber-attacks. BBC News. 16.04.2021. URL: https://www.bbc.com/news/technology-56755484
10. Bogdanova I., Callo-Müller M. Unilateral Economic Sanctions to Deter and Punish Cyber-Attacks: Are They Here to Stay? EJIL:Talk. 07.12.2021. URL: https://www.ejiltalk.org/unilateral-economic-sanctions-to-deter-and-punish-cyber-attacks-are-they-here-to-stay/
11. Milmo D. Anonymous: the hacker collective that has declared cyberwar on Russia. The Guardian. 27.02.2022. URL: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

УДК 32.019.51:791.2](470+571)

АНТИУКРАЇНСЬКА ПРОПАГАНДА В СУЧАСНОМУ РОСІЙСЬКОМУ ІСТОРИЧНОМУ КІНЕМАТОГРАФІ

А. О. Семеній

Анотація. У даній роботі розглядається втілення образу українця в сучасному російському історичному кінематографі, його трансформація та основні теми. Аналізується низка російських фільмів на предмет антиукраїнської пропаганди та її основних методів. З'ясовується реакція українського суспільства на відверту ксенофобію в російських фільмах. Специфіка дослідження теми передбачає застосування загальнонаукових (дослідницького, аналітико-синтетичного, узагальнення) та спеціальних історичних (проблемно-хронологічного, історико-порівняльного, історико-генетичного) методів.
Ключові слова: кінематограф, націоналіст, війна, пропаганда, міф.

Відразу зі своєю появою кінематограф став одним з найефективніших засобів державної пропаганди. З приходом до влади більшовиків кіноресурс використовувався на максимум, а пропагандистська машина працювала з неймовірною потужністю. Проте і після розпаду Радянського Союзу ситуація майже не змінилася – влада Російської Федерації продовжує використовувати фільми у власних цілях, а контроль за кіновиробництвом з кожним роком лише зростає.

Питання російсько-української інформаційної війни загалом та у кіно зокрема висвітлено переважно у вітчизняних працях. Зокрема, це аналітична доповідь «Інформаційні виклики гібридної війни: контент, канали, механізми протидії» колективу науковців під головуванням А. Баровської [9], монографія О. С. Власюка «Кремлівська агресія проти України: роздуми в контексті війни» [4], статті Д. О. Коваля та Т. Р. Короткого [10], У. Коруц [11], С. П. Сегеди та В. П. Шевчука [18], О. Семенової [19].

У кінематографі найпоширенішою тематикою, яка найбільш підтримується державою, залишається історико-патріотична. Російська влада виховує нові покоління патріотичних мас, і кінематограф, як найпопулярніший вид мистецтва, допомагає йому в цьому. Окреме місце в цій ніші зайняло зображення українців. Важливо відзначити, що з часів розпаду СРСР відбулася певна еволюція в образі «українця». Якщо раніше він зображався неосвіченим, часто нерозумним меншим братом, поширюючи серед глядачів тезу про меншовартість українського народу, то в сучасному російському історичному кіно українці часто постають підступними, жорстокими, хоч і досі неосвіченими, ворогами. Володимир Цибулько зазначає: «Для Росії дуже важливим є телебачення, де росіянам весь час розказують, хто є українці. Російська людина вірить телевізору, вірить друкованому слову, вірить в існування ворогів» [5].

У зв'язку з новим етапом російсько-української війни та повномасштабним вторгненням Російської Федерації в Україну залишається актуальним аналіз підготовки російського населення до війни проти українського народу за допомогою кінопропаганди.