УДК 324(043.5)
DOI https://doi.org/10.32782/2305-9389/2023.29.26

ВТРУЧАННЯ У ВИБОРИ: ВИДИ ТА ЗАГРОЗИ ДЛЯ СУЧАСНИХ ДЕМОКРАТІЙ

Розік Марія,
кандидат політичних наук,
старший викладач кафедри політології та публічного управління
Волинського національного університету імені Лесі Українки
ORCID ID: 0000-0002-0974-8985

Назарук Наталія,
кандидат політичних наук
ORCID ID: 0000-0003-1463-3768

У статті визначено поняття «втручання у вибори», його основні види та особливості застосування у державах із демократичною формою правління. Виявлено, що процес обрання влади суспільством має велике значення для легітимності всієї політичної системи, а будь-яка спроба втручання з метою вплинути на результат виборів чи завадити їм є порушенням законів держави та міжнародних правил. Тому вибори мають проходити вільно, виборчий процес відбуватися без утручання сторонніх осіб або держав (зовнішнього втручання), а виборці повинні мати можливість формувати думку незалежно, без будь-якого спонукання чи маніпулятивного втручання.

З'ясовано, що різноманітні способи втручання у вибори існували завжди, але в останнє десятиріччя вони стали більш помітними через зміни у виборчому середовищі, поширення нових засобів комунікації та зростання кількості неліберальних акторів, які втручаються у виборчий процес по всьому світу. Визначено, що втручання у вибори порушує право на самовизначення, коли виборці не можуть сформувати думку самостійно, та може стосуватися як спроб, так і змін результатів виборів загалом. Доведено, що потенціал для фальсифікації затьмарює вибори в усіх країнах, навіть у тих, де демократія існує давно.

Виявлено існування двох форм утручання у вибори, які автори об'єднали у внутрішні та зовнішні втручання. Поштовхом для розвитку останніх стали інформаційно-комунікаційні технології, що уможливили вплив суб'єктів політики на виборчий процес поза межами власної держави. Доведено, що найбільш небезпечними є змішані іноземні та внутрішні втручання, основна мета яких – дезорганізація суспільства, уведення до лав керівників держави своїх прибічників, прихильників власної ідеології та інтересів за допомогою методів інформаційного впливу. Тому важливими є встановлення державами чітких правил, розроблення інструментів та програм, спрямованих на захист виборів і демократичних систем, що реагуватимуть на зростаючу загрозу маніпуляцій із боку внутрішніх та іноземних політичних акторів.

Ключові слова: *фальсифікація виборів, утручання у вибори, маніпуляції, фейкові новини, кібербезпека, хакерська атака, виборчі технології.*

Rozik Mariia, Nazaruk Nataliia. Election interference: types and threats to modern democracies

The article defines the concept of the term «election interference», its main types and peculiarities of application in democratic states. It is found that the process of electing the government by society is essential for the legitimacy of the entire political system, and any attempt to interfere with the election results or to prevent them is a violation of the laws of the state and international rules. Therefore, elections should be held freely, the electoral process should be free from interference by unauthorized persons or states (external interference), and voters should be able to form their opinions independently, without any inducement or manipulative interference.

It is found that various ways of interfering in elections have always existed, but in the last decade they have become more prominent due to changes in the electoral environment, the proliferation of new means of communication and the growing number of illiberal actors interfering in the electoral process around the world. The authors determine that interference in elections violates the right to self-determination when voters cannot form an opinion on their own and can relate to both attempts and changes in the election results in general. It is proved that the potential for fraud overshadows elections in all countries, even in those where democracy has existed for a long time.

The authors identify two forms of election interference, which they group into internal and external interference. The impetus for the development of the latter was provided by information and communication technologies, which made it possible for political actors to influence the electoral process outside their own country. It is proved that the most dangerous are mixed foreign and domestic interventions, the main purpose of which is to disorganize society, to introduce their supporters, adherents of their own ideology and interests into the ranks of the state leaders through the methods of information influence. Therefore, it is important for states to establish clear rules, develop tools and programs aimed at protecting elections and democratic systems that will respond to the growing threat of manipulation by domestic and foreign political actors.

Key words: *election fraud, election interference, manipulation, fake news, cybersecurity, hacker attack, election technology.*

Процес обрання влади суспільством має велике значення для легітимності всієї політичної системи в демократичних державах. Будь-яка спроба втручання з метою вплинути на результат виборів чи завадити їм є порушенням законів держави та міжнародних правил. Різноманітні способи втручання у вибори існували завжди, але в останнє десятиріччя вони стали більш помітними через зміни у виборчому середовищі, поширення нових засобів комунікації та зростання кількості неліберальних акторів, що втручаються у виборчий процес по всьому світу.

Метою дослідження є визначення поняття «втручання у вибори», їх видів та особливостей застосування як загроз сучасним демократіям.

Згідно з *Міжнародним пактом про громадянські і політичні права,* прийнятим Генеральною Асамблеєю Організації Об'єднаних Націй 16 грудня 1966 р., який набрав чинності 23 березня 1976 р., усі люди можуть «вільно визначати свій політичний статус і вільно здійснювати економічний, соціальний і культурний розвиток» [3]. Це включає право народу створювати власні політичні інститути, розвивати економічні ресурси та керувати власною соціальною та культурною еволюцією. Оскільки право на самовизначення є постійним правом, народ вирішує ці питання шляхом проведення виборів. Отже, вибори мають проходити вільно, виборчий процес повинен відбуватися без утручання сторонніх осіб або держав (зовнішнього втручання), а виборці – мати можливість формувати думку незалежно, без будь-якого спонукання чи маніпулятивного втручання.

Утручання у вибори можна визначити як комплекс прямих та прихованих дій політичних акторів, що мають на меті призвести до змін у поведінці кандидатів, партій, виборців, змінити їхні вподобання задовго до самих виборів або під час виборчого процесу. Утручання у вибори порушує право на самовизначення, коли виборці не можуть сформувати думку самостійно, та може стосуватися як спроб, так і змін результатів виборів загалом.

Автори визначають два види втручання у вибори: ***внутрішнє*** (дії політичних акторів усередині країни) та ***зовнішнє*** (іноземне втручання у вибори, спроби уряду вплинути на вибори в інших країнах). Якщо внутрішнє втручання стосується безпосередньо фальсифікації виробів та зміни результатів виборів, то зовнішнє втручання має на меті підрив громадської довіри до виборчого процесу та загострення соціально-політичного розколу певної держави. Воно не стосується технічних змін в аспекті процесу голосування, таких як реєстрація виборців, вкидання бюлетенів, підрахунок голосів або оголошення результатів виборів. Натомість актори зовнішнього втручання прагнуть вплинути на сприйняття кандидатів суспільством, а також підірвати довіру до виборчих процесів та посилити соціально-політичний розкол серед народу.

Внутрішнє	**Зовнішнє**
Фальсифікація виборів	**Іноземне втручання**
− На етапі підготовки до виборів (розроблення виборчого права, територіальна організація виборів, формування системи комісій та списків кандидатів). − На етапі агітації (використання адмінресурсу, підкуп виборців – прямий та непрямий, зняття невигідних кандидатів, кримінальне переслідування кандидатів, наклеп, «чорний» піар, створення «двійників», цифрове втручання тощо). − На етапі голосування (купівля голосів, метод «каруселі», «мертві душі», використання відкріпних посвідчень, «вкидання» бюлетенів, метод «недійсних бюлетенів», псування бюлетенів тощо).	− Інформаційні заходи (поширення пропагандистських та фейкових новин, платні коментатори, використання ботів (автоматизовані акаунти), викрадення акаунтів у соцмережах). − Технічні засоби/кібератаки (злом, блокування, відключення доступу). − Формування впливу (кооперація з елітами, фінансування партій або кампаній).

Джерело: складено на основі [1; 4; 9]

Перші спроби сфальсифікувати вибори зафіксовані ще в XIX ст. (під час виборів у Нью-Йорку 1844 р. було зареєстровано 55 тис голосів, хоча право голосу мали лише 41 тис виборців) [7]. Десятиліттями ці зусилля вдосконалювалися, і з часом, методи впливу ставали креативнішими. Фальсифікація виборів набувала різних форм, у тому числі фальсифікації на етапі підготовки до виборів, під час голосування, а також неправомірного впливу на виборців, що відбувалися на різних етапах виборчого процесу – від реєстрації до оголошення результатів. Варто зазначити, що потенціал для фальсифікації затьмарює вибори в усіх країнах, навіть у тих, де демократія існує давно.

Що стосується зовнішнього втручання у вибори, то це також не нове явище світового порядку, поштовхом для розвитку якого стали інформаційно-комунікаційні технології, що уможливили вплив суб'єктів політики на виборчий процес поза межами власної держави. Зовнішнє втручання у вибори –

це «гра в довгу»: чимало методів впливу тією чи іншою мірою застосовуються задовго до самих виборів, а впродовж виборчих кампаній їх лише підсилюють. Зовнішній вплив має на меті не привести до влади свого кандидата, а створити сум'яття та дезорганізувати політичну систему країни. Це повільний процес ідеологічної підривної діяльності та психологічної війни, який має на меті змінити у мішеней відчуття реальності та змусити їх діяти на користь супротивника.

Перша суперечка зовнішнього втручання у вибори зафіксована під час правління президента Джорджа Вашингтона в Сполучених Штатах. Під час перебування Вашингтона на посаді революційні Франція та Велика Британія розпочали війну, яка розділила американців на політичні фракції.

Федералісти, такі як віцепрезидент Джон Адамс, намагалися зберігати нейтралітет у конфлікті та зміцнити дипломатію і торгівлю з Великобританією. Республіканці-демократи, такі як державний секретар Томас Джефферсон, симпатизували Французькій революції, яка скасувала французьку монархію, і хотіли зміцнити відносини з Францією. Коли федералісти уклали договір Джея з Британією (договір про дружбу, торгівлю та мореплавство), французький посол у США П'єр-Огюст Адет намагався підкупити американських сенаторів, щоб зупинити його ратифікацію, але зазнав невдачі через брак коштів. Адет змінив тактику, отримавши копію «Договору Джея» [7], і опублікував його в американських газетах, здогадуючись, що багато хто в суспільстві не схвалював його ратифікацію.

Зусилля Адета співпали з президентськими виборами у США 1796 р., першими виборами, що стали предметом суперечки між Адамсом і Джефферсоном. Незадовго Адет опублікував серію листів, у яких попереджав, що обрання Адамса означатиме війну з Францією, щоб схилити виборців на бік Джефферсона. Проте ця кампанія також зазнала невдачі через те, що Адету не вистачало охоплення: листи широко розповсюджувалися лише в кількох містах. Однак Адамс усе ще мав достатню підтримку, щоб виграти голосування та стати другим президентом США.

Протягом XX ст. розвиток засобів зв'язку та міжнародної мобільності дав змогу іноземним агентам здійснювати більш складні зусилля з підриву виборчих систем у всьому світі. Наприклад, під час Другої світової війни Велика Британія та Німеччина намагалися вплинути на американську політику, щоб сприяти або перешкодити американському втручанню у війну. Нацистська ідеологія перебувала під впливом американського руху – євгеніки (віра в еволюційну ієрархію серед людей, засновану на певних ознаках, таких як етнічне чи расове походження, що набула форми наукового расизму та слугувала інтелектуалізації ксенофобії і расових упереджень). Під час Другої світової війни, розуміючи, що вони мають союзників серед білого населення Америки, нацистська партія доклала зусиль щоб вплинути на американські вибори 1940 р. на користь спочатку демократа Джона Л. Льюїса, а потім Республіканської партії [7]. Зокрема, нацистські агенти та симпатики публікували статті в газетах і журналах, поширюючи пропаганду і дезінформацію про британську діяльність у Європі. Тим часом британський уряд, який відчайдушно потребував американського втручання для запобігання окупації, докладав зусиль маніпулювати виборами на користь кандидата від Демократичної партії Франкліна Д. Рузвельта. Британія прослуховувала і стежила за американськими урядовими установами і опублікувала тисячі статей, покликаних просувати відносини Америки з Британією та ідею прямого втручання.

Сьогодні цифрові платформи – нове поле битви за демократію. Формування потоку інформації в Інтернеті є важливою стратегією тих, хто прагне перешкодити демократичній передачі влади через вибори. Діючі політичні актори в усьому світі використовують грубі методи, «зберігаючи» маску народної легітимності. Не існує універсального шаблону втручання у вибори – кожен випадок має унікальну комбінацію методів, ураховуючи цілі, контекст, а також уразливість країни-мішені та її виборчого процесу.

Великі авторитарні держави, такі як Росія і Китай, були причетні до кібератак та інформаційної війни, пов'язаної з виборами в демократичних державах. У лютому 2019 р., за три місяці до федеральних виборів в Австралії, служби безпеки повідомили про кібератаку на комп'ютерні мережі парламенту та трьох основних політичних партій, яку приписували Міністерству державної безпеки Китаю. Напередодні президентських виборів у квітні-травні 2019 р. Центральна виборча комісія України зіткнулася з хвилею кібератак, найімовірніше, із Росії. Напередодні проміжних виборів у США в листопаді 2018 р. корпорація «Майкрософт» виявила, що підрозділ, пов'язаний із російською військовою розвідкою, створив вебсайти, схожі на вебсайти Сенату США та відомих аналітичних центрів, щоб обманом змусити відвідувачів розкрити конфіденційну інформацію та паролі. Різні групи впливу також поширювали дезінформацію в Twitter, Facebook і YouTube під час виборів до Європейського Парламенту в травні 2019 р. [6]. Таке транскордонне втручання має на меті посіяти розкол, підтримати обраних кандидатів і підірвати демократію.

Згідно з даними Freedom House, державні та недержавні суб'єкти найчастіше використовують інформаційні заходи для спотворення медіаландшафту, що зробило його найпопулярнішою тактикою

зовнішнього втручання у вибори [4]. Серед них – маніпулювання контентом, а саме: *пропагандистські новини, фейкові новини, платні коментатори, боти (автоматизовані акаунти) і викрадення справжніх акаунтів у соціальних мережах*. Основою для поширення дезінформації є фабрикація або умисне спотворення новинного контенту для обману аудиторії, забруднення інформаційного простору, мета якого – створення плутанини та непевності, коли люди не можуть зрозуміти, що відбувається насправді. Використання підробленої особистості або фальшивої Інтернет-персони застосовується для онлайн-просування політичної реклами, насамперед на сторінках соціальних медіа, з метою просувати або штучно роздувати популярність/непопулярність певних політичних партій, кандидатів, політичних фігур (наприклад, політична кампанія Дарта Вейдера на виборах президента і парламенту в 2014 р.).

Використання фальшивих акаунтів, тролів та автоматичних ботів у соціальних мережах та онлайн-форумах застосовується для збільшення охоплення й видимості дезінформації, розпалювання соціальної фрагментації та поляризації. Так, у 2014 р. було створено мережу ультрапатріотичних груп у Фейсбуку, які пов'язані з акаунтом Степана Мазури, що модерувалися з Росії, та закликали українців повалити ваду [1]. Віртуальний агент впливу вдавав із себе українського патріота, який розчарувався у владі, й закликав до силового повалення влади в Україні. Такі форми фальсифікації особистості мають різні цілі: метою створення фальшивого акаунту в соціальних медіа може бути поширення дезінформації, організація події або ж підбурювання суспільної реакції під виглядом альтернативної ідентичності, щоб запобігти викриттю та імітувати справжню поведінку. Мотивом для фішингу є крадіжка облікових даних користувача для проведення кібератаки.

Найбільші платформи вжили чимало заходів для протидії такому впливу. З'явилися механізми фактчекінгу, підвищення прозорості реклами, більшої прозорості груп та сторінок, соцмережі знаходили та припиняли діяльність «ботоферм», прибирали фейкові акаунти, почали застосовуватися освітні та попереджувальні заходи, обмін інформацією між Інтернет-гігантами та розвідкою.

Технічні заходи зовнішнього втручання у вибори найчастіше націлюються на конкретні вебсайти, стосуються хакерських операцій проти державних інституцій (хакерський злам під час виборів 2016 р. у США) або впливових суспільних організацій (аналітичні центри, громадські організації та медіа), опозиційних сил та виборчої інфраструктури. Атаки на інфраструктуру охоплюють різні специфічні кібертактики, які включають будь-які спроби проникнути в систему електронного голосування країни, бази даних виборців або споріднені ІТ-мережі (атаки на сайт ЦВК напередодні виборів 2014 р.) [5]. Зокрема, ці тактики можуть включати DDOS-атаки, злам баз даних виборців (щоб зібрати інформацію/змінити дані) або маніпулювання передачею електронного голосування чи підрахунком голосів із метою змінити результати виборів. Окрім того, такі атаки застосовують для підриву функціональності ключових ІТ-систем та мереж для ослаблення конкретних партій та кандидатів, особливо опозиційних.

У 2017 р. відбулася одна з наймасштабніших хакерських атак на українську інфраструктуру – кібератака з використанням вірусу, який спочатку був названий Petya, а пізніше – NotPetya. Вірус блокував комп'ютерні системи компаній, вимагаючи за розблокування 300 доларів у біткоїнах. Напад відбувся на третину банківських установ, великі поштові корпорації, а також уряд, низку енергетичних компаній (у тому числі регіональних), редакції великих медіахолдингів. Кібератаки на бізнес чи державні органи можуть мати одну з трьох цілей: вимагання грошей та шантаж; популяризація шахрая, який здійснює напад; дестабілізація ситуації у державі [2]. У даному випадку атаки вірусу Petya не мали на меті фінансового інтересу та відбувалися з метою досягнення максимальних суспільних наслідків, резонансу: атака на казначейство припала на кінець фінансового року, на «Укрзалізницю» – перед вихідними, коли люди масово намагались отримати квитки. Вірус Petya зупинив третину економіки України на три дні, що призвело до великих збитків, тому сьогодні ватро говорити не лише про фізичну охорону об'єктів, а й інформаційну, оскільки кібернапади мають більший потенціал збитків.

Формування впливу (кооперація з елітами, фінансування партій або кампаній) використовується з метою впливу на ухвалення рішень на національному рівні, а також на громадську думку в країні-мішені. Основним завданням такого впливу є налагодження сприятливих стосунків із ключовими елітами з державного та приватного секторів. Створення стосунків може здійснюватися у цілій низці форм, зокрема бізнесових та торговельних стимулів, академічного та інституційного впливу (існування в Україні УПЦ МП), «угод про співробітництво» з політичними партіями (керівна російська партія «Єдина росія» має кілька таких угод з європейськими партіями), а також використання окремих оперативників-шпигунів для проникнення у цільові кола (справа Марії Бутіної у США) [9]. Сюди ж відноситься і відкрите або приховане надання фінансування певній партії чи електоральній кампанії. Значним викликом для боротьби із зовнішнім впливом є використання зовнішніми гравцями внутрішніх посередників.

Висновки. Отже, розвиток сучасного суспільства тісно пов'язаний з Інтернет-середовищем, наслідком чого став активний вплив кіберпростору на формування політичної спрямованості та поведінки особистості, її політичної ідентичності. Існують різні форми втручання у вибори, які автори об'єднали у внутрішні та зовнішні втручання. Найбільш небезпечними є змішані іноземні та внутрішні втручання, основна мета яких – дезорганізація суспільства, уведення до лав керівників держави своїх прибічників, прихильників власної ідеології та інтересів за допомогою методів інформаційного впливу. Тому важливими є встановлення державами чітких правил, розроблення інструментів та програм, спрямованих на захист виборів і демократичних систем, що реагуватимуть на зростаючу загрозу маніпуляцій із боку внутрішніх та іноземних політичних акторів.

Література:

1. Десять російських методів втручання у вибори. Українські приклади. *Texty.org.ua.* 2019. URL: https://texty.org.ua/articles/93080/Desat_rosijskyh_metodiv_vtruchanna_u_vybory_Ukrajinski-93080/.
2. Купєцкі Р., Брийка Ф., Хлун Т. Втручання Росії у вибори в демократичних країнах. Посібник з дезінформації. Частина 2. *Куншт.* 2022. URL: https://kunsht.com.ua/articles/vtruchannya-rosii-u-vibori-v-demokratichnix-krainax-posibnik-z-dezinformacii-chastina-2.
3. Міжнародний пакт про громадянські і політичні права від 19 жовтня 1973 р. *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/995_043#Text.
4. Digital Election Interference. *Freedom Hourse*. 2019. URL: https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/digital-election-interference.
5. Foreign Cyber Interference in Elections. *Foreign Cyber Elections Interference.* 2021. URL: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2969&context=ils.
6. Foreign Threats to the 2020 US Federal Elections. *Intelligence Community Assessment.* URL: https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.
7. Issitt M. Election Interference: Overview. *EBSCO Information Services.* URL: https://www.ebsco.com/sites/default/files/acquiadam-assets/Points-of-View-Reference-Center-Election-Interference-Overview.pdf.
8. Rothkirch P. Foreign Election Interference: A Violation of the Right to Self-Determination. *Völkerrechtsblog.* 16.11.2022. DOI: 10.17176/20221116-095506-0.
9. Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks. *Carnegie Endowment for International Peace.* URL: https://www.jstor.org/stable/pdf/resrep21009.6.pdf.