

ЦИФРОВІЗАЦІЯ ВИБОРЧОГО ПРОЦЕСУ: РЕАЛІЇ, ПЕРСПЕКТИВИ, ЗАГРОЗИ

Роль сучасних цифрових технологій набуває дедалі більшого значення у виборчих процесах демократій, демонструючи тенденцію широких змін, як позитивних зі зростанням оперативності та прозорості процесів, так і негативних з підвищенням загроз безпеці політичних технологій комунікації, до яких належать вибори. Дослідження основних детермінантів загроз у контексті явищ впливу сучасних інформаційно-комунікаційних технологій на електоральні процеси держав, зумовлюють формування аргументованих висновків впливу зазначених загроз на національну безпеку, збереження інтересів суспільства та захисту держави в цілому. Основною метою даної статті є дослідження і класифікація загроз, пов'язаних з цифровізацією виборчих процедур. Матеріал містить аналізи впливу великих даних, розвитку машинного навчання та штучного інтелекту, а також вдосконалення швидкісного інтернету та розширення можливостей мобільних технологій, що мають вплив на технології політичної комунікації та безпеку виборчих процесів. Задля більш ґрунтовнішого аналізу безпекових аспектів сучасної цифровізації політичних комунікацій проаналізовано поетапність виборчого процесу, який розглядається в контексті конкретних фаз – підготовчої фази та фази проведення виборів і підрахунку результатів. Застосування зазначеного підходу розкриває перспективу комплексного аналізу загроз та їх класифікацію на групи загроз пов'язаних з інформаційною та кібербезпекою, загроз маніпуляції з даними, загроз технічної та організаційної безпеки, та політико-правових загроз. За допомогою використання методів аналізу кейсів, івент-аналізу, систематизації загроз та методу порівняльного аналізу, розглянуто приклади кіберзагроз та маніпуляції даних, проаналізовано законодавчу базу та регулювання вимог щодо захисту персональних даних та безпеки інформаційних систем у різних демократичних державах. В статті підкреслюється необхідність розробки сучасних регуляторних і технічних засобів протидії зовнішнім і внутрішнім джерелам і факторам ризиків. Стаття має практичне значення для державних інституцій, функції яких зосереджені на забезпеченні інформаційної безпеки, виборчих процесах, для аналітичних центрів, тощо.

Ключові слова: псефологія, цифровізація, виборчий процес, інформаційно-комунікаційні технології, мас-медіа, великі дані, штучний інтелект, машинне навчання, кібербезпека, маніпуляція даними, інформаційна безпека, політико-правові загрози, національна безпека, електронне голосування, цифрова інфраструктура, когнітивні функції, електоральна поведінка виборців, демократія.

Постановка проблеми. Розвиток інформаційних технологій впливає на виборчі процеси в усіх державах світу. Особливості цього впливу залежать від типу політичного режиму – демократичного чи авторитарного. У фокусі нашої уваги демократії, де впровадження цифрових технологій у сучасні виборчі процеси пропонує переваги в підвищенні ефективності їх проведення, їхню прозорість та доступність. Проте, виклики питань безпеки в організації зазначених процесів залишаються ключовими для їх вирішення.

Мета статті. Визначити реалії, перспективи та загрози цифровізації виборчого процесу в демократичних державах із застосуванням псефологічного аналізу виборчого процесу.

Аналіз останніх досліджень та публікацій. Дослідження останніх десятиліть того, як кіберрозвиток впливає та змінює демократичну залученість громадян в політичних процесах, залишається актуальним [1]. Швидкий інтернет, мобільні технології, штучний інтелект (ШІ) є нормою в сучасних комунікаційних процесах. Управління політичними кампаніями та цифрова взаємодія за допомогою сучасних інформаційно-комунікаційних технологій (ІКТ) стають все більш поширеним явищем у політичних системах світу. В Україні дослідження даної проблематики також не залишається поза

увагою. Питання цифровізації виборчого процесу розглядали такі українські автори як О. Шевчук [2], І. Чайка та Є. Цокур [3], І. Сікора [4], О. Кравчук та Л. Матвієнко [5], В. Подгорна [6], громадська мережа Опора [7], тощо.

Технологізація виборчого процесу актуалізує для політології питання аналітичного інструментарію. Концептуально оновлена щодо вимог цифрової доби псефологія пропонує поєднання цифрових технологій та політичної науки. Саме на цьому тлі постає можливість аналізу особливостей цифровізації виборчого процесу за умов демократії.

Методологія дослідження. Методологічна основа дослідження цифровізації виборчого процесу в демократичних державах сформована із застосуванням як загальнонаукових принципів, так і політико-орієнтованих методів аналізу. В основі підходу лежить принцип багатофакторності, що передбачає врахування політичних, правових, технологічних, соціокультурних та інформаційних чинників, які формують сучасні електоральні процеси. Принцип детермінізму реалізується через виявлення причинно-наслідкових зв'язків між технологічним прогресом, розвитком ІКТ та трансформацією виборчої поведінки. Принцип системності передбачає розгляд виборчого процесу як інтегрованої двоскладової структури (підготовча фаза і фаза голосування та підрахунку результатів), де кожен етап супроводжується специфічними загрозами. Важливим є дотримання принципу об'єктивності, що забезпечується використанням емпіричних джерел – офіційних звітів, даних соціологічних досліджень, аналітики безпекових структур. Принцип історизму застосовується для простеження еволюції е-виборів, зокрема через порівняльний аналіз досвіду держав, які впроваджували або відмовилися від електронного голосування (наприклад, Німеччина, Естонія, США, Франція). У процесі дослідження використовуються методи аналізу та узагальнення, що дозволяють виокремити ключові ризики цифровізації. Історико-порівняльний метод застосовується для виявлення відмінностей і схожостей у цифрових стратегіях різних демократичних держав. Системний підхід дозволяє комплексно оцінити взаємодію технологічних, нормативно-правових і комунікативних аспектів у виборчому середовищі.

Особливу роль у дослідженні відіграє емпіричний аналіз – розгляд випадків втручання у виборчі процеси. Представлено аналіз великих даних (ВД) і цифрової аналітики через розгляд застосування високопродуктивних обчислень у псефологічному аналізі. Таким чином, дослідження ґрунтується на поєднанні кількісних та якісних методів, дискурсивного і контент-аналізу, що забезпечує глибину та репрезентативність отриманих результатів.

Виклад основного матеріалу. Задля досягнення мети дослідження доцільно виділяти у виборчому процесі підготовчу фазу, фазу проведення голосувань і підрахунку результатів. Старт передвиборчої гонки в різних державах обмежений своїм внутрішнім законодавством, як-от момент обрання кандидата від партії, початок політичної агітації в медіа, початок фінансування передвиборчої кампанії, обмеження фінансування, тощо. В різних державах такі обмеження затверджені відповідними актами, у Великій Британії це UK PPERA [8], в США це USA FECA [9], у Франції це France Code électoral [10], в Німеччині Germany FEA [11], тощо. Проте, згідно С. Блюменталю політичні кампанії, в силу своїх трансформацій з традиційних політичних практик через вплив на них сучасних технологій і медіа, ніколи не закінчуються [12].

Безпекові ризики, які виникають у результаті використання сучасних ІКТ в зазначених фазах виборчого процесу, і які безпосередньо на нього впливають, поділяються на наступні групи: інформаційна безпека, маніпуляції з даними, кібербезпека, група технічної та організаційної безпеки, група політико-правових загроз, тощо. Кожна група має свої властивості і націлюється на специфічну фазу виборчого процесу. Розгляд впливу безпекових ризиків на окремо кожен етап виборчого процесу надає розуміння різниці джерел ризиків і специфічні характеристики їхнього впливу. Наприклад, якщо розглядати використання інформаційних технологій в фазі проведення безпосередніх голосувань і підрахунку їх результатів, то незважаючи на переваги цифровізації даного процесу, таких як зручність і швидкість, цифрова інфраструктура процесу голосування є об'єктом ризику кібератак, що може призвести як до зриву організації проведення виборів, так і до компрометації їхніх результатів. В підготовчій фазі виборчих процесів об'єктом загрози є вже не цифрова інфраструктура, а сам виборець і його рішення при голосуванні.

З початку цифрової революції другої половини ХХ століття людство зазнало безпрецедентного прискорення змін спровокованих технологічним прогресом, що в свою чергу почало формувати людиною її світосприйняття новими способами. Розвиток ІІІ посилив дані ефекти, внісши нові способи впливу на суспільство з точки зору ефективної взаємодії людини і машини та генерації

накопичення знань з експоненціальною швидкістю. Водночас культурні зрушення, спричинені глобалізацією, урбанізацією та соціальними мережами, посприяли появі нових способів комунікації та поширення знань у глобальних масштабах. Безсумнівно, сучасні технології принесли зручність і швидкість в наше життя, але на соціальному рівні цифрові інструменти змінили спосіб, яким людство спілкується між собою, потенційно впливаючи на тривалість уваги та рівень емпатії [13]. Сучасні технології суттєво прискорили темп життя, що в свою чергу вплинуло на суспільство і методи прийняття рішень в ньому. Швидкий потік неструктурованої інформації великих об'ємів, яка часто змінюється і уточнюється, значно ускладнює можливості людини до критичного її аналізу. Додатково слід зафіксувати факт переорієнтації фокусу людини в сторону розважального контенту [14]. В результаті таких змін, включаючи ультра швидкий потік інформації та її обсяги, людський мозок не може вчасно обробити весь обсяг інформації. Прогрес у галузі ШІ та машинного навчання (МН) представив нові інструменти для збільшення когнітивних функцій як прогностичні аналітики, персоналізовані рекомендації та розумні помічники, які здатні підвищити продуктивність, але викликають занепокоєння стосовно конфіденційності та алгоритмічної упередженості. Відповідно, означені зміни мають суттєвий вплив на трансформацію виборчої поведінки, і є загрозою демократичним політичним системам.

До загроз інформаційної безпеки під час підготовчого етапу у виборчому процесі можна віднести дезінформацію у соцмережах (боти, фейк новини, дипфейки), соціальну поляризацію, мікротаргетинг у соцмережах щоб поглибити суспільні розколи через замовлення маніпулятивної реклами націленої на окремі групи виборців, нелегітимне використання персональних даних (злиті дані з соцмереж), тощо. Серед основних чинників, які мають прямий вплив на виборця під час підготовчої фази виборчого процесу, є великі обсяги неструктурованої інформації, які виборець отримує з сучасних мас-медіа, і які в свою чергу використовують великі дані (ВД). Сучасні медіа, до переліку яких входять новинні медіа, соціальні мережі, відеоблогінг, платформи створення коротких відеороликів, тощо, націлені на виборця, який приймає рішення на основі здобутої в означених типах медіа інформації. Через складну, а іноді застарілу і неактуальну регуляцію в області збереження і використання персональних даних в демократичних державах, соціальні мережі та мас-медіа, в алгоритмах яких використовуються ВД та їх дата-аналіз, є об'єктом використання впливу на цільову аудиторію, тобто на виборця. Ефективність даного впливу залежить від обсягів ВД та їх якості, а також алгоритмічною складовою в контексті рішення того, як такі дані використовувати. Загалом, проблематика в питаннях регуляції в сфері використання ВД, отримання та зберігання персональних даних, а також загальна проблематика глобалізації світу, яка дозволяє створювати нові інтернет платформи в будь-якій точці світу і розповсюджувати серед них будь-яку інформацію, ігноруючи регуляторну політику конкретних держав в інформаційно-комунікативному полі, стають потужним інструментом задля політичного впливу на виборця. Через відсутність контролю над глобальними інтернет-ресурсами, останні можуть мати алгоритми розповсюдження таргетованої інформації на окремі цільові аудиторії згідно зібраних і проаналізованих по даним цільовим групам ВД. В 2018 році генеральні прокурори декількох штатів США проводили розслідування щодо неправомірного використання британською компанією Cambridge Analytica Ltd особистих даних 50 мільйонів користувачів мережі Facebook [15]. Компанія пропонувала розробити детальні психологічні профілі кожного американського виборця та змодельовати тип особистості людини [16], щоб передвиборчі кампанії могли якнайкраще на нього/неї вплинути. Маючи дані про мільйони користувачів згаданої соціальної мережі, було розміщено близько 6 мільйонів різних повідомлень і цитат тоді ще майбутнього кандидата в президенти США Д. Трампа для обраних категорій людей.

Джерела отримання ВД, які можуть використовуватися в підготовчій фазі організації виборчого процесу, можна розділити на наступні: дані з соціальних медіа задля аналітики трендів, настроїв, громадської думки, тощо; дані з проведених цільових і загальних опитувань; дані з веб-аналітики, за допомогою якої вивчається і аналізується поведінка користувача на умовному сайті, та його вподобання; дані з моделей споживання новин, які допомагають з'ясувати як саме і коли люди споживають ті чи інші новинні ресурси; публічні дані з державних реєстрів та дата-сетів, як наприклад реєстраційні дані виборців, податкові дані, тощо. Протягом підготовчої фази виборчого процесу, а здебільшого поза терміном даної фази, що часто є порушенням виборчого законодавства, політичні сили використовують ті чи інші ресурси задля виконання збору даних від аудиторії, їх аналізу задля коректування виборчої чи політичної стратегії, та поширення вже таргетованої інформації серед конкретних структурованих груп виборців.

ВД допомагають медіа представити більш точну, своєчасну та релевантну інформацію про своїх користувачів. І. Косуке, за допомогою ресурсів високопродуктивних обчислень PicScie (Pacific Science Center), запропонував новий підхід в розумінні сучасних моделей голосування [17], що змінює правила політичного аналізу в американській політиці. Його дослідження ґрунтуються на відкритих даних, що містять детальну інформацію про 180 млн американських виборців, яка оновлюється кожні 6 місяців. Такі дані надаються провідною позапартійною фірмою L2[18], яка постачає дані про виборців політичним партіям, кандидатам, соціологам, консультантам, тощо. За допомогою обчислювальних потужностей Тихоокеанського Наукового Центру PicScie І. Косуке розробив методологію, яка дозволяє детально вивчати великі обсяги даних, знаходити в величезних пулах інформації закономірності, та робити висновки як місцеві моделі голосування змінюються з часом незалежно від щільності населення в регіонах. Поміж даних отриманих з L2, І. Косуке використовує в своїх обчислювальних алгоритмах широкий спектр додаткових джерел, що надає його прогнозам результатів виборів вражаючу точність. За допомогою МН група І. Косуке може простежити навіть вплив політичною сегрегації за місцем проживання.

Наданий приклад демонструє можливості використання ВД за допомогою МН з даних отриманих з відкритих джерел. Проте відкриті джерела надають лише частину даних, які можна опрацювати в умовах сучасних технологічних реалій. Цікавим залишається опрацювання даних отриманих незаконним чи неетичним шляхом.

Слід також розглянути загрози з маніпуляціями даними під час підготовчих етапів виборчого процесу, до яких відносяться фальсифікації результатів (втручання в цифрові протоколи), неправдиве підрахування (через зміну електронних алгоритмів), несанкціонований доступ до виборчих БД, знищення або модифікація даних виборців. Загрози з маніпуляціями даними мають вплив як на підготовчу фазу, так і на фазу проведення голосувань і підрахунку результатів. В 2024 році, в фазу підготовки до президентських виборів у США, ФБР підготувало огляд[19] прикладів можливих загроз маніпуляцій з виборчими даними. В звіті описуються кілька прикладів внутрішніх загроз, пов'язаних із безпекою виборів, обговорено потенційні сценарії, які можуть виникнути під час виборчого циклу 2024 року, та надано рекомендації щодо того, як зменшити ризик, пов'язаний із внутрішніми загрозами. Проте, аналітичний центр ідентифікації ризиків та аналізу «дарк-нету» Constella Intelligence Inc. у 2024 році зафіксував витoki даних про виборців у США [20], що циркулюють у «дарк-неті», і які становлять приблизно 78% усіх даних про виборців. Зазначений факт підкреслює унікальну вразливість держави, зумовлену децентралізованою виборчою системою та розгалуженою інфраструктурою даних про виборців.

Виборча система Канади спирається на складну мережу ІТ-систем, постачальників та персоналу, що також є ризиком для втручання і маніпуляції з даними виборців. Н. Іслам, С. Кім, і М. Піруз підготували статтю [21], спрямовану на протидію даним вразливостям перед федеральними виборами в Канаді 2025 року, а також для зміцнення стійкості суспільства до кіберзагроз. В документі представлено комплексну національну оцінку кіберзагроз відповідно до Спеціальної публікації NIST 800-30, зосереджену на виявленні та пом'якшенні ризиків кібербезпеки. Дослідження визначає три основні загрози: кампанії з «misinformation, disinformation, and malinformation» (MDM); атаки на критично важливу інфраструктуру і системи підтримки виборів; та шпигунство з боку зловмисників.

Вирішення зазначених проблем пов'язаних із загрозами з маніпуляціями з даними вимагають узгоджених зусиль з боку членів виборчих комісій, експертів з кібербезпеки та політиків задля забезпечення цілісності та безпеки демократичних виборів.

Наступна група загроз включає питання кібербезпеки, технічні та організаційні загрози, їх вплив на фазу проведення голосувань і підрахунку результатів. Зазначені загрози для виборчих процесів носять здебільшого технічний та психологічний і соціально-інжиніринговий характер, і проявляються у вигляді фішингових атак, криптоджекінгу, встановлення шпигунського, чи сталкерського ПЗ, а також DoS-атаки. Дані загрози також можна віднести до обох фаз виборчого процесу – підготовчого та фази проведення голосувань.

До технічних і організаційних загроз можна віднести збої систем електронного голосування (через навантаження, помилки, поломки), недостатній захист інфраструктури (відсутність резервних систем, відсутність шифрування, тощо), помилки адміністраторів або людський фактор при обслуговуванні техніки та використанні непрозорих, або закритих систем голосування без незалежного аудиту.

23 жовтня 2024 року, за два тижні до дня президентських виборів США, Центр аналізу загроз

Microsoft (MTAC) надав репорт [22], в якому йдеться про спостереження зусиль Росії, Ірану та Китаю, які спрямовувалися на підлив демократичних виборчих процесів у США. За допомогою наданої інформації, уряд США вжив заходів, що викривали кіберактивність та вплив іноземних супротивників, пов'язаних з виборами 2024 року. Зазначені заходи включали викриття надсилань зловмисними іранськими кіберсуб'єктами «викрадених, непублічних матеріалів з кампанії колишнього президента Трампа 2016-2020» як особам, що тоді були пов'язані з кампанією президента Байдена, так і американським медіа-організаціям. Також мало місце звинувачення трьох іранських суб'єктів у операції зі злому та витоку інформації, спрямованій проти кампанії Трампа-Венса [23].

Поміж звіту від Центру аналізу загроз Microsoft, американська компанія з розробки технологій з кібербезпеки ReliaQuest відвітувала [24] про свої очікування щодо зростання ризиків кіберзагроз з наближенням до дня проведення виборів. За їхніми оцінками даний період часу має високу вірогідність кібератак, які націлюються не лише на об'єкти інфраструктури самого виборчого процесу, а і на виборців та на представників великого бізнесу. За очікуваннями ReliaQuest, групи «постійних розширених загроз» (Advanced Persistent Threat – АРТ [25]), планували організувати спроби зірвати вибори в США за допомогою зломів та витоку інформації, дезінформаційних кампаній, та атак на виборчу інфраструктуру. Очікувались надсилання фішингових електронних листів з виборчою тематикою та з вбудованими в них хакерського поштового програмного забезпечення «SocGholish», яке діє як завантажувач. Вбачалося, що фішинг буде основним початковим вектором доступу для кіберзлочинців з груп АРТ, які прагнутимуть перешкодити виборам. До репорту також додавалися очікування випадків з шахрайством з крипто-валютою, реєстрацію доменів з помилками для виманювання пожертв та інвестицій. Слід відзначити, що починаючи з 2006 року групи АРТ постійно моніторяться і поповнюються в єдиному реєстрі [26] задля своєчасного їх виявлення за описом їх активності, характеристикам та зв'язкам.

Ще одним прикладом прояву кібератак та загроз технічного і організаційного характеру під час виборів був факт атаки російською хакерською групою урядових веб-сайтів Румунії в день голосувань другого туру президентських виборів в 2025 році [27]. Були уражені веб-сайти Конституційного суду Румунії, головний урядовий портал, сайт Міністерства закордонних справ Румунії та сайти кандидатів у президенти, за фактом чого одразу було запроваджено слідство.

Дані випадки свідчать про те, що розвиток ІКТ та сучасної цифровізації демократичних процесів мають прямий вплив на національну безпеку, збереження життєво-важливих інтересів суспільства і держави в цілому, і потребують значної уваги під час організації політичних технологій комунікації, до яких належать вибори. У цьому контексті особливої актуальності набуває псефологія як галузь політології, що не тільки аналізує електоральні процеси, тенденції та результати виборів, але й оцінює ймовірність цифрових втручань, кібератак, інформаційних маніпуляцій та впливу дезінформації, алгоритмічної упередженості. Потрібно зауважити, що якщо активність кіберзлочинців можна зафіксувати завдяки захисному програмному забезпеченню та сучасним підходам і методам у боротьбі з кіберзагрозами, то загрози, що пов'язані з маніпуляціями даних, чи загрози інформаційної безпеки потребують більш глибокого аналізу та сучасної нормативно-правової бази, яка б відповідала викликам сучасних ІКТ.

За винятком загроз кібербезпеки та загроз технічного і організаційного характеру, на фазу проведення голосувань і підрахунку результатів мають також політико-правові загрози. Як вже згадувалося вище, одним з основних форм захисту виборчого процесу від різного типу загроз є правове поле, тобто законодавча база, яка регулює виборчі процеси в державі. До політико-правових загроз виборчим демократичним процесам відносяться: відсутність законодавства або регулювання цифрових виборів; залежність від іноземного програмного забезпечення; маніпуляції через приватні компанії, які надають ІТ-послуги для проведення виборів; втрата довіри громадян до виборів; тощо. Дана група ризиків має вплив на виборчі процеси в державі в цілому.

В виборчому законодавстві держави здебільшого регламентуються правила обрання кандидата від політичної партії, дозвіл на початок політичної агітації в медіа, початок і кінець фінансування передвиборчої кампанії, обмеження фінансування, тощо. Окрім зазначених законодавчих правил також існує регуляція поширення персональних даних громадян, як виборців в контексті голосувань. В Сполучених Штатах це HIPAA [28], в Європейському Союзі GDPR [29]. Дані документи регулюють правила зберігання персональних даних громадян і заборону їх розповсюдження, що є основою їх захисту від негативного впливу на них. Проте не всі держави мають відповідну політику захисту даних своїх громадян, або ж такі регуляції існують, але носять лише декларативний характер.

Проблеми дотримання прав і свобод громадян в країнах електоральної демократії, чи тим більше в багатопартійних чи однопартійних автократіях [30], юридичної незалежності, слабкої гнучкості в регуляції питань по збору і обробці персональних даних громадян зовнішніми акторами, сигналізують про політико-правову загрозу для виборчих процесів пов'язаних із сучасною діджиталізацією. В однопартійних автократіях часто передбачається законодавча база, яка закладає юридичне підґрунтя для дозволу використання сучасних технологій при зборі даних своїх громадян, аналізу суспільних настроїв, і корегування мотивації населення, позитивної чи негативної. Умови відсутності політичної конкуренції та спрощення законодавчої системи в питаннях інформаційної політики, надають керівництву такої держави легітимізації своєї влади [31]. Окрім аналізу спорідненості розвитку цифрових технологій та сучасного процесу комунікації між політиками та виборцями у передвиборчій фазі виборів, в окремих державах існують спроби розгляду та запровадження сучасних технологій в організації самих голосувань. Мова йде про електронні голосування на різних платформах та за допомогою різних методів реалізації. Проте відмічається різне ставлення окремих держав до зазначеного питання. Останніми роками в багатьох демократіях на різних рівнях порушується питання запровадження електронного голосування, проте ризикові аспекти стримують реалізацію даних ініціатив. Зазначене питання підіймалося з різних точок зору, як наприклад наданні можливості голосувати громадянам з обмеженими можливостями [32], або організація голосувань під час COVID-19 пандемії. В різних дискусіях по даній ініціативі, експерти з безпеки знаходять суттєві ризики вразливості у впровадженні електронних голосувань. У 2024-му році штат Каліфорнія одностайно відхилив запит на впровадження електронного голосування [33] посиляючись на безпекові вразливості. А пілотне тестування мобільного застосунку для голосувань Voatz у 2020 році в штатах Західна Вірджинія, Юта, Колорадо та ін. зазнало критики з боку безпекового аудиту та розслідування Массачусеттського Технологічного Інституту [34]. В Європейському Союзі на рівні Європарламенту також неодноразово підіймається питання перспективи застосування технологій електронного голосування, обговорюються дотичні ризики та готовність інфраструктури [35, 36].

Проте серед європейських акторів спостерігається помітний зсув у бік використання ключових технологій для покращення політичної комунікації та процедур голосування. Влада Бельгії, Болгарії, Естонії, Франції та одного округу Португалії вже застосували електронні методи голосування. До того ж, політичні партії активно запроваджують технології кампаній, що ґрунтуються на аналізі ВД, у державах Європи — зокрема в Німеччині, Іспанії, Франції, Італії, Угорщині та Нідерландах. Експерти очікують, що політичні партії й надалі використовуватимуть ІІІ для покращення своїх комунікаційних стратегій. Окреслюючи ризики та можливості, пов'язані з технологіями ІІІ та МН, розглядається оновлена законодавча база, яка регулює інструменти керування даними, які використовуються політичними партіями для створення та розповсюдження контенту. Політичні партії та постачальники софтверних рішень для створення контенту підпадають під низку обмежень щодо обробки даних, зобов'язань щодо прозорості, та вимог щодо управління ризиками відповідно до Загального регламенту захисту даних (GDPR), Директиви про конфіденційність у електронному вигляді (e-PD) [37] і Закону про цифрові послуги (DSA) [38]. У 2024-2025 роках набули чинності Регламент про прозорість і таргетування політичної реклами (ТТРА) [39] і Закон про штучний інтелект (AIA) [40], які регламентують окреслену проблематику в державах Європейського Союзу.

В цілому можна зробити висновок, що демократії загалом не демонструють узгодженої або одностайної готовності до повномасштабного впровадження технологій електронного голосування – ані у вигляді електронних машин на виборчих дільницях, ані у форматі дистанційного інтернет-голосування. Частина держав таких як Бельгія, Болгарія, Естонія вже реалізували певні форми е-вотингу, однак їхній досвід вважається винятковим. Інші держави або відмовилися, або призупинили спроби впровадження (Італія, Франція, Ірландія, Нідерланди тощо). В 2023 році в Нідерландах на урядовому рівні піднімалося питання про відновлення можливості запровадження електронних голосувань [41], проте також зазнало критики. Слід зазначити, що електронне голосування мало місце застосування в Німеччині та Нідерландах в 2006-2007 роках [42, 43], але зазнало сильної критики через брак технічних можливостей на той час, та з безпекових міркувань. Тож більшість держав ЄС не схильні до запровадження інтернет-голосування, посиляючись на ризики та соціальну невідповідність, проте мають місце активні обговорення даного питання на найвищому європарламентському рівні [44]. Враховуючи юридичну автономію кожної держави у виборчій політиці, уніфікація або гармонізація е-вотингу в межах ЄС наразі малоімовірна. Але слід зауважити, що країни Балтії демонструють ефективність в застосуванні онлайн голосувань поряд з класичним

закритим голосуванням [45]. Також цікавими є спостереження за розробкою і спробою запуску електронного голосування за допомогою технології блокчейн у Південній Кореї [46].

Висновки. Цифровізація виборчих процесів в демократичних державах залишається складним питанням для вирішення. Через свою багатшаровість вона вимагає всеосяжного розгляду, яке має поєднувати і позитивну складову, як наприклад ефективність, доступність і прозорість, і негативну – як безпекові загрози.

Загалом, необхідно засвідчити, що вибори все більше проявляють себе не лише як акт громадянської волі, а й як арена цифрового протистояння. Впровадження інформаційно-комунікаційних технологій у виборчі процеси пропонує переваги у вигляді оперативності та прозорості виборчого процесу. Проте зростає також і значущість безпекових питань. Типологія останніх розподіляється між кібербезпекою, організаційно-технічною безпекою, безпекою щодо маніпуляції даними, інформаційною безпекою, політико-правовою безпекою. За таких умов особливого значення набуває псефологія, що дозволяє системно осмислити вплив цифрових технологій на виборчий процес.

Цифрові технології не скасовують демократичні принципи, а адаптують їх до змін в інформаційному середовищі та нових форматів політичної взаємодії.

Подальші дослідження цифровізації виборчого процесу мають використовувати аналітичний потенціал псефології та зосереджуватися на актуальних трансформаціях усіх фаз виборчого процесу, безпекового виміру зазначених трансформацій, порівнянню міжнародного досвіду у цій сфері. Особливої уваги потребують механізми підвищення прозорості виборчого процесу та зростання довіри до його результатів. Демократії мають адаптуватися до усіх аспектів цифрової епохи, зберігаючи при цьому свої засадничі цінності.

Бібліографічний список:

1. Hanschitz, G. Digitalization of Politics and Elections. *Springer Nature*. 2017 URL: https://link.springer.com/rwe/10.1007/978-3-319-06091-0_3-1, DOI: 10.1007/978-3-319-06091-0_3-1
2. Шевчук О. Цифровізація виборчого процесу: потреби та перспективи реалізації. *Наукові перспективи. Матеріали XV-ої Міжнародної науково-практичної конференції*. 2021. С. 62.
3. Чайка І., Цокур Є. Цифровізація виборів в Україні і світі: етичні виміри феномену. *Humanities Studies*. 2024. № 20 (97). С. 140. DOI: 10.32782/hst-2024-20-97-16
4. Сікора І. Довіра електорату до електронних технологій у виборчому процесі: світовий досвід. *Вісник Національного технічного університету України «КПІ». Політологія. Соціологія. Право*. 2024. № 3(63). С. 64-70. DOI: 10.20535/2308-5053.2024.3(63).313502
5. Кравчук О., Матвієнко Л. Модернізація виборчих процесів засобами штучного інтелекту як інноваційний механізм публічного управління. *Науковий вісник Вінницької академії*. 2025. № 1(7). С. 107-114. DOI 10.32782/2786-5681-2025-1.13
6. Подгорна В. Цифрові платформи та їхній вплив на політичну сферу. *Проблеми політичної психології*. 2021. № 10(24). С. 301-309. DOI: 10.33120/porp-Vol24-Year2021-81
7. Громадська мережа Опора збирає і опрацьовує інформацію з проблематики виборів у сучасних реаліях. <https://www.oporaua.org/category/vybory>
8. Political Parties, Elections and Referendums Act. *UK government Legislation*. 2000. URL: <https://www.legislation.gov.uk/ukpga/2000/41/contents>
9. US Federal Election Campaign Act. *Federal Election Commission*. Washington. D.C. 20463. 1971. URL: <https://www.fec.gov/files/legal/aos/1989-29/1061516.pdf>
10. France Code électoral. 1907. *Journal officiel de la République française*. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070239/
11. Federal Elections Act. *Federal Law Gazette*. 1993. URL: https://www.bundeswahlleiterin.de/en/dam/jcr/4ff317c1-041f-4ba7-bbbf-1e5dc45097b3/bundeswahlgesetz_engl.pdf
12. Blumenthal S. The permanent campaign: inside the world of elite political operatives. *Beacon Press*. Boston. 1980. P. 2-10, 94-115. URL: <https://archive.org/details/permanentcampaign00blum/mode/2up>
13. Farkaš I. Transforming Cognition and Human Society in the Digital Age. *Biol Theory*. 2024. DOI: 10.1007/s13752-024-00483-3
14. Matthes J., Heiss R., and Scharrel H. The distraction effect. Political and entertainment-oriented content on social media, political participation, interest, and knowledge. *Computers in Human Behavior*. 2023. № 142. DOI: 10.1016/j.chb.2022.107644
15. Detrow S. What Did Cambridge Analytica Do During The 2016 Election? *National Public Radio*. 2018. URL: <https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election>
16. Murray S., Reston M., Bash D. and Perez E. Inside the Trump campaign's ties with Cambridge Analytica. *CNN*. 2018. URL: <https://edition.cnn.com/2018/03/21/politics/trump-campaign-cambridge-analytica/index.html>

17. Big Data Informs a Paradigm Shift in Political Analysis. *Princeton Research Computing*. 2016. URL: <https://researchcomputing.princeton.edu/news/2018/big-data-informs-paradigm-shift-political-analysis>
18. Database of U.S. voter records, including demographic information, historical voting records, and party affiliations. *L2-data*. URL: <https://www.l2-data.com/>
19. U.S. Federal Elections: The Insider Threat. *United States Election Assistance Commission*. 2024. URL: https://www.eac.gov/sites/default/files/2024-06/2024_General_Elections_Insider_Threat.pdf
20. Potential Cybersecurity Threats to the 2024 U.S. Election: Voter Database Leaks. *Constella AI*. 2024. URL: <https://constella.ai/2024-u-s-election-voter-database-leaks/>
21. Islam N., Kim S., Pirooz M., and Shvetsov S. Cyber Threats to Canadian Federal Election: Emerging Threats, Assessment, and Mitigation Strategies. *Computer Science. Cryptography and Security Arxiv*. Cornell University. 2042. DOI: 10.48550/arXiv.2410.05560
22. Watts C. As the U.S. election nears, Russia, Iran and China step up influence efforts. *Microsoft Threat Analysis Center*. Microsoft. 2024. URL: <https://blogs.microsoft.com/on-the-issues/2024/10/23/as-the-u-s-election-nears-russia-iran-and-china-step-up-influence-efforts/>
23. The First Major Cyberattack of the 2024 Election. *The New York Times*. 2024. URL: <https://www.nytimes.com/2024/08/27/podcasts/the-daily/hacking-2024-election.html?>
24. 2024 US Election: Top Cyber Threats & Organizational Impacts. *ReliaQuest*. 2024. URL: <https://reliaquest.com/blog/2024-us-election-top-cyber-threats-organizational-impacts/>
25. Lindemulder G. What are advanced persistent threats? *IBM*. 2024. URL: <https://www.ibm.com/think/topics/advanced-persistent-threats>
26. Groups register. *MITRE ATT&CK*. URL: <https://attack.mitre.org/groups/>
27. Russian hacker group attacks Romanian government websites on election day. *Politico*. 2025. URL: <https://www.politico.eu/article/russia-hacker-group-romania-election-day-constitutional-court-vote/>
28. Health Insurance Portability and Accountability Act (HIPAA). *US government Centers for Disease Control and Prevention*. 1996. URL: <https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html>
29. General Data Protection Regulation (GDPR). *Official Journal of the European Union*. European Union. 2018. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
30. Full democracy data. *Our World in Data*. 2023. URL: <https://ourworldindata.org/grapher/full-democracy-lexical>
31. Feldstein S. The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance. *Oxford University Press*. 2021. URL: <https://books.google.com.ua/books?id=W3QjEAAQBAJ&lpg=PP1&lr&pg=PP1#v=onepage&q&f=false>
32. Discussion on Elections Online Voting. *CSPAN*. 2020. URL: https://archive.org/details/CSPAN_20201022_081100_Discussion_on_Elections_Online_Voting/
33. California Voter Foundation and Verified Voting Urge Veto of Assembly Bill 2159. *California Voter Foundation and Verified Voting*. 2024. URL: <https://verifiedvoting.org/wp-content/uploads/2024/09/CA-2159-veto-CVF-VV1.pdf>
34. Newman L.H. Voting App Flaws Could Have Let Hackers Manipulate Results. *Wired*. 2020. URL: <https://www.wired.com/story/voatz-voting-app-security-flaws/>
35. The arrival of e-voting and campaign technologies in Europe: Promise, perils and preparedness. *European Parliamentary Research Service*. European Parliament. 2024. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762321/EPRS_BRI\(2024\)762321_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762321/EPRS_BRI(2024)762321_EN.pdf)
36. Study on E-Voting practices in the EU. *European Commission*, B-1049 Brussels. JUST/2021/OP/0002. 2023. URL: https://commission.europa.eu/document/download/23076478-987e-4dea-b9ef-df5e0dfd6cd2_en?filename=DG_JUST_EVoting_Report_pdf.pdf
37. Electronic Privacy Directive (e-PD). Directive 2002/58/EC of the European Parliament and of the Council. *Official Journal of the European Communities* European Union. 2002. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058>
38. Digital Services Act. (DSA). Regulation (EU) 2022/2065 of the European parliament and of the council. *Official Journal of the European Union*. European Union. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>
39. Transparency and targeting of political advertising (TTPA). Regulation (EU) 2024/900 of the European parliament and of the council. *Official Journal of the European Union*. European Union. 2024. 2024/900. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400900
40. Artificial intelligence act (AIA). Regulation (EU) 2024/1689. *European Parliamentary Research Service*. European Parliament. 2024. 2024/1689. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)
41. Pereira L. Why does the Netherlands still not have electronic voting? *Dutch Review*. 2023. URL: <https://dutchreview.com/news/why-netherlands-no-electronic-voting/>
42. Sebes E. J. Electronic Voting Banned in Germany. *OSET Institute*. 2013. URL:

<https://www.oseinstitute.org/blog/electronic-voting-banned-in-germany>

43. Re-evaluation of the Use of Electronic Voting in the Netherlands. *NDI*. 2013. URL: <https://www.ndi.org/e-voting-guide/examples/re-evaluation-of-e-voting-netherlands>

44. The arrival of e-voting and campaign technologies in Europe: Promise, perils and preparedness. *European Parliamentary Research Service*. European Parliament. 2024.

URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762321/EPRS_BRI\(2024\)762321_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762321/EPRS_BRI(2024)762321_EN.pdf)

45. Lithuanian government seeks to introduce online voting this year. *The Baltic Times*. 2013. URL: https://www.baltictimes.com/lithuanian_government_seeks_to_introduce_online_voting_this_year/

46. South Korea to develop blockchain voting system. *The Voting News* and *Verified Voting*. 2018 URL: <https://thevotingnews.com/%e2%80%8bsouth-korea-to-develop-blockchain-voting-system-zdnet/>

References:

1. Hanschitz, G. (2017). Digitalization of Politics and Elections. *Springer Nature*. URL:

https://link.springer.com/rwe/10.1007/978-3-319-06091-0_3-1, DOI: 10.1007/978-3-319-06091-0_3-1

2. Shevchuk O. (2021). Tsyfrovizatsiia vyborchoho protsesu: potreby ta perspektyvy realizatsii. *Naukovi perspektivy. Materialy XV Mizhnarodnoi naukovo-praktychnoi konferentsii*, 62.

3. Chaika I., Tsokur Y. (2024). Tsyfrovizatsiia vyboriv v Ukraini I sviti: etychni vymiry fenomenu. *Humanities Studies*, 20 (97), 140.

4. Sikora I. (2024). Dovira elektoratu do elektronnykh tekhnolohii u vyborchomu protsesi: svitovi dosvid. *Visnyk Natsionalnoho tekhnichnoho universytetu Ukrainy «KPI»*. *Politolohiia. Sotsiolohiia. Pravo*, 3(63), 64-70.

5. Kravchuk O., Matviienko L. (2025). Modernizatsiia vyborchykh protsesiv zasobamy shtuchnoho intelektu yak innovatsiinyi mekhanizm publichnogo upravlinnia. *Naukovi visnyk Vinnytskoi akademii*, 1(7), 107-114.

6. Podhorna V. (2021). Tsyfrovi platformy ta yikhni vplyv na politychnu sferu. *Problemy politychnoi psykholohii*, 10(24), 301-309.

7. Hromadska merezha Opora zbyraie ta opratsovuie informatsiiu z problematyky vyboriv u suchasnykh realiakh. <https://www.oporaua.org/category/vybory>

8. Political Parties, Elections and Referendums Act. (2000). *UK government Legislation*. URL: <https://www.legislation.gov.uk/ukpga/2000/41/contents>

9. US Federal Election Campaign Act. (1971). *Federal Election Commission*. Washington. D.C. 20463. URL: <https://www.fec.gov/files/legal/aos/1989-29/1061516.pdf>

10. France Code électoral. (1907). *Journal officiel de la République française*. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070239/

11. Federal Elections Act. *Federal Law Gazette*. (1993). URL: https://www.bundeswahlleiterin.de/en/dam/jcr/4ff317c1-041f-4ba7-bbbf-1e5dc45097b3/bundeswahlgesetz_engl.pdf

12. Blumenthal S. (1980). The permanent campaign: inside the world of elite political operatives. *Beacon Press*. Boston, 2-10, 94-115.

13. Farkaš I. (2024). Transforming Cognition and Human Society in the Digital Age. *Biol Theory*.

14. Matthes J., Heiss R., and Scharrel H. (2023). The distraction effect. Political and entertainment-oriented content on social media, political participation, interest, and knowledge. *Computers in Human Behavior*, 142. DOI: 10.1016/j.chb.2022.107644

15. Detrow S. (2018). What Did Cambridge Analytica Do During The 2016 Election? *National Public Radio*. URL: <https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election>

16. Murray S., Reston M., Bash D. and Perez E. (2018). Inside the Trump campaign's ties with Cambridge Analytica. *CNN*. URL: <https://edition.cnn.com/2018/03/21/politics/trump-campaign-cambridge-analytica/index.html>

17. Big Data Informs a Paradigm Shift in Political Analysis. (2016). *Princeton Research Computing*. URL: <https://researchcomputing.princeton.edu/news/2018/big-data-informs-paradigm-shift-political-analysis>

18. Database of U.S. voter records, including demographic information, historical voting records, and party affiliations. *L2-data*. URL: <https://www.l2-data.com/>

19. U.S. Federal Elections: The Insider Threat. (2024). *United States Election Assistance Commission*. URL: https://www.eac.gov/sites/default/files/2024-06/2024_General_Elections_Insider_Threat.pdf

20. Potential Cybersecurity Threats to the 2024 U.S. Election: Voter Database Leaks. *Constella AI*. 2024. URL: <https://constella.ai/2024-u-s-election-voter-database-leaks/>

21. Islam N., Kim S., Pirooz M., and Shvetsov S. (2024). Cyber Threats to Canadian Federal Election: Emerging Threats, Assessment, and Mitigation Strategies. *Computer Science. Cryptography and Security Arxiv*. Cornell University. DOI: 10.48550/arXiv.2410.05560

22. Watts C. (2024). As the U.S. election nears, Russia, Iran and China step up influence efforts. *Microsoft Threat Analysis Center*. Microsoft. URL: <https://blogs.microsoft.com/on-the-issues/2024/10/23/as-the-u-s-election-nears-russia-iran-and-china-step-up-influence-efforts/>

23. The First Major Cyberattack of the 2024 Election. (2024). *The New York Times*. URL: <https://www.nytimes.com/2024/08/27/podcasts/the-daily/hacking-2024-election.html?>

24. 2024 US Election: Top Cyber Threats & Organizational Impacts. (2024). *ReliaQuest*. URL: <https://reliaquest.com/blog/2024-us-election-top-cyber-threats-organizational-impacts/>
25. Lindemulder G. (2024). What are advanced persistent threats? *IBM*. URL: <https://www.ibm.com/think/topics/advanced-persistent-threats>
26. Groups register. *MITRE ATT&CK*. URL: <https://attack.mitre.org/groups/>
27. Russian hacker group attacks Romanian government websites on election day. (2025). *Politico*. URL: <https://www.politico.eu/article/russia-hacker-group-romania-election-day-constitutional-court-vote/>
28. Health Insurance Portability and Accountability Act (HIPAA). (1996). *US government Centers for Disease Control and Prevention*. URL: <https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html>
29. General Data Protection Regulation (GDPR). *Official Journal of the European Union*. European Union. 2018. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
30. Full democracy data. *Our World in Data*. 2023. URL: <https://ourworldindata.org/grapher/full-democracy-lexical>
31. Feldstein S. (2021). The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance. *Oxford University Press*. URL: <https://books.google.com.ua/books?id=W3QjEAAAQBAJ&lpg=PP1&lr&pg=PP1#v=onepage&q&f=false>
32. Discussion on Elections Online Voting. *CSPAN*. 2020. URL: https://archive.org/details/CSPAN_20201022_081100_Discussion_on_Elections_Online_Voting/
33. California Voter Foundation and Verified Voting Urge Veto of Assembly Bill 2159. *California Voter Foundation and Verified Voting*. 2024. URL: <https://verifiedvoting.org/wp-content/uploads/2024/09/CA-2159-veto-CVF-VV1.pdf>
34. Newman L.H. (2020). Voting App Flaws Could Have Let Hackers Manipulate Results. *Wired*. URL: <https://www.wired.com/story/voatz-voting-app-security-flaws/>
35. The arrival of e-voting and campaign technologies in Europe: Promise, perils and preparedness. *European Parliamentary Research Service*. European Parliament. 2024. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762321/EPRS_BRI\(2024\)762321_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762321/EPRS_BRI(2024)762321_EN.pdf)
36. Study on E-Voting practices in the EU. *European Commission*, B-1049 Brussels. JUST/2021/OP/0002. 2023. URL: https://commission.europa.eu/document/download/23076478-987e-4dea-b9ef-df5e0dfd6cd2_en?filename=DG_JUST_EVoting_Report_pdf.pdf
37. Electronic Privacy Directive (e-PD). Directive 2002/58/EC of the European Parliament and of the Council. *Official Journal of the European Communities* European Union. 2002. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058>
38. Digital Services Act. (DSA). Regulation (EU) 2022/2065 of the European parliament and of the council. *Official Journal of the European Union*. European Union. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>
39. Transparency and targeting of political advertising (TTPA). Regulation (EU) 2024/900 of the European parliament and of the council. *Official Journal of the European Union*. European Union. 2024. 2024/900. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400900
40. Artificial intelligence act (AIA). Regulation (EU) 2024/1689. *European Parliamentary Research Service*. European Parliament. 2024. 2024/1689. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)
41. Pereira L. (2023). Why does the Netherlands still not have electronic voting? *Dutch Review*. URL: <https://dutchreview.com/news/why-netherlands-no-electronic-voting/>
42. Sebes E. J. (2013). Electronic Voting Banned in Germany. *OSET Institute*. URL: <https://www.osetinstitute.org/blog/electronic-voting-banned-in-germany>
43. Re-evaluation of the Use of Electronic Voting in the Netherlands. *NDI*. 2013. URL: <https://www.ndi.org/e-voting-guide/examples/re-evaluation-of-e-voting-netherlands>
44. The arrival of e-voting and campaign technologies in Europe: Promise, perils and preparedness. *European Parliamentary Research Service*. European Parliament. 2024. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762321/EPRS_BRI\(2024\)762321_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762321/EPRS_BRI(2024)762321_EN.pdf)
45. Lithuanian government seeks to introduce online voting this year. *The Baltic Times*. 2013. URL: https://www.baltictimes.com/lithuanian_government_seeks_to_introduce_online_voting_this_year/
46. South Korea to develop blockchain voting system. *The Voting News and Verified Voting*. 2018 URL: <https://thevotingnews.com/%e2%80%8bsouth-korea-to-develop-blockchain-voting-system-zdnet/>

Mykhailichenko S. Digitalization of the electoral process: reality conditions, perspectives, threats.

The role of modern digital technologies in electoral procedures of democracies is experiencing exponential growth, bringing both positive and negative changes. On one perspective, these transformations optimize efficiency and transparency of such procedures, streamlining the electoral

processes efficiency. On the other perspective, they introduce security risks to political communication technologies, where democratic elections are the core component. The material of this article provides an in-depth analysis of the key threats posed by digitalization in electoral operations. It investigates how Big Data, Machine Learning, Artificial Intelligence, high-speed internet, and modern mobile technologies are redefining political communication and election security. To achieve a more detailed understanding of the problem, the article decomposes the electoral process into constituent sub-stages — the preparation phase, and the phase of voting itself along with and the vote-counting. Utilizing this approach enables to methodically classify threats into four key groups: information and cybersecurity threats, data manipulation threats, threats to technical and organizational safety, and institutional and regulatory threats. Employing case studies, event analysis, threats systematization, and comparative analysis, it considers empirical examples of cyberattacks and data manipulation. It also provides an overview of regulatory frameworks governing personal data protection and information security across various democracies. The article emphasizes the necessity for modern regulatory and technical solutions to the risks mitigation. Its findings possess practical applicability for government institutions which are oriented toward election security, safeguarding democratic processes and for analytical centers.

Keywords: psephology, digitalization, electoral process, information and communication technologies, mass media, big data, artificial intelligence, machine learning, cybersecurity, data manipulation, data protection, information security, political and juridical threats, national security, e-voting, digital infrastructure, cognitive functions, voter behaviour, democracy.