Аналітична записка
Інтернет-голосування: виклики та рішення

Вступ

Цифрові технології надають громадськості численні більш доступні, об'єднавчі та швидкі можливості для е-активізму. Однак, вони мають свою ціну. Інтернет-доступ до порталів е-участі робить їх більш вразливими до спотворень зсередини та зламу ззовні, а онлайн-медіа роблять громадську думку більш сприйнятливою до маніпуляції. Ці проблеми особливо актуальні для електронного голосування як головного методу прийняття рішень у політиці ери Інтернету, електронному врядуванні та цифровій демократії. Проте, завдяки низці рішень щодо архітектури, законодавства, процедур та обізнаності громадян, ризики е-голосування можливо знизити.

Таким чином, мета цієї праці – виявити, структурувати та зменшити ризики електронного голосування завдяки пропонованим практичним рішенням. У контексті ширшої виборчої реформи, вже після проведення аналізу витрат і вигод та прийняття рішення щодо запровадження інтернет-голосування, ця аналітична записка може допомогти передбачити імовірні ризики та спростувати необґрунтовані заперечення. На відміну від більшості публікацій, які або зосереджуються на окремих ризиках або описують належне інтернет-голосування, ця аналітична розвідка розглядає численні виклики та знаходить відповіді на них. Вона буде корисною для держ-службовців, політиків, громадських активістів та пересічних громадян для запобігання, виявлення та зменшення зловживань і-голосуванням, захисту е-демократії від спотворень та зміцнення ефективного врядування.

Серед усіх різновидів електронного голосування (е-голосування), таких, як голосування із використанням машини для голосування на дільниці чи віддаленого електронного голосування із використанням будки для голосування поза дільницею, у цій розвідці розглядається саме дистанційне інтернет-голосування. У цьому тексті інтернет-голосування (і-голосування) – це голосування із застосуванням комп'ютерних та інтернет-технологій принаймні для голосування та підрахунку голосів. У цьому сенсі воно співпадає із мобільним та онлайн-голосуванням.

Як універсальний інструмент е-участі, і-голосування розглядається щодо цілого спектру форм е-демократії: дорадчих онлайн-опитувань громадської думки, обов'язкових до виконання е-голосувань щодо публічної політики, проєктів бюджету участі, е-плебісцитів, е-референдумів, е-виборів (і-виборів, онлайн-виборів) тощо. Так і-голосування може сприяти представницькій, прямій, учасницькій, ліквідній та іншим видам демократії.

Це дослідження ґрунтується на розгляді наявних наукових та прикладних студій та аналізі вторинних даних щодо статистики і-голосування. Висновки базуються на прикладах рівня країн та громад, і тому їх можливо застосовувати до широкого спектру проєктів дистанційного і-голосування за різних політичних обставин.

Далі у тексті представлено часову послідовність найбільших викликів і-голосуванню, рекомендовано рішення, детальніше проаналізовано типові проблеми і-голосування та зроблено висновки. Також наведено лаконічний огляд країн проведених, але скасованих, скасованих, але розглянутих, чинних та потенційних і-виборів.

Автор: Дмитро Хуткий, радник із полісі та адвокації Європейського альянсу цифрового розвитку.

Рецензенти: Деніел Іннераріти, професор Школи транснаціонального врядування Інституту європейського університету, Італія; Роберт Кріммер, професор е-врядування Талліннського технічного університету «ТалТек», Естонія.

Подяка: це розвідка була виконана у межах прикладної дослідницької програми «Лідери публічної політики» у Школі транснаціонального врядування Інституту європейського університету.

Видавець: Європейський альянс цифрового розвитку, м. Брюссель, Бельгія, серпень 2020 року.

Ключові пункти

	Ризики	Рішення
1.	**Тенденційна постановка питання:** спотворення тексту бюлетеня для і-голосування для опитування, плебісциту, референдуму чи виборів; тенденційна постановка питання у мас-медіа	**Нейтральна постановка питання:** забезпечується рецензуванням комісією, завчасною публікацією, обговоренням та виправленням тексту бюлетеня; також дискусії сприяє вільний доступ до інтернету
2.	**Упереджена поляризація:** ефект попереднього вибору та схильність до підтвердження призводять до групової поляризації та створюють інформаційні бульбашки і спотворену соціальну реальність	**Цілеспрямоване об'єднання:** сприяння створенню оточення, яке підтримує розмаїття поглядів, критичне сприйняття інформації та інтелектуальну дискусію
3.	**Маніпулювання громадською думкою:** приховане мікротаргетування учасників голосування персоналізованими повідомленнями за допомогою великих даних, ботів та проплачених дописувачів	**Регламентація діяльності онлайн-медіа:** комплекс законодавчих, виконавчих та громадських заходів із накладення обмежень, забезпечення оприлюднення та виконання правил
4.	**Технічна несправність системи:** технічні несправності обладнання чи програмного забезпечення системи для голосування, а також людські помилки у користуванні системою	**Надійне функціонування системи:** тестування системи, навчання адміністраторів і-голосування, планування технічних і організаційних заходів у разі надзвичайних ситуацій
5.	**Зловмисне хакерство:** проблеми із кібербезпекою, пов'язані зі зламом системи і-голосування вітчизняними або іноземними урядовими або неурядовими суб'єктами	**Кібербезпека та доброчесність:** оцінювання та сертифікація системи, стратегія із кібербезпеки, тестування системи, змагання із виявлення помилок, навчання персоналу та освітня кампанія
6.	**Ексклюзія:** проблеми щодо правоздатності певних соціальних груп та проблеми доступності, обумовлені цифровою нерівністю	**Інклюзія:** гарантування права на голосування усім правоздатним громадянам, додавання і-голосування як альтернативи до звичайного
7.	**Неточні реєстри виборців:** недостовірні реєстри виборців можуть зловживатися для недопущення певних людей до голосування та використання підроблених документів для вкидання бюлетенів	**Точні реєстри виборців:** стандартні технічні та організаційні заходи у поєднанні із технологіями розподілених реєстрів, зокрема, такими, як блокчейн
8.	**Хибна ідентифікація:** ризик, що деякі люди із правом голосу будуть недопущені до голосування, а якісь шахраї проголосують, не маючи на те права	**Надійна ідентифікація:** запровадження декількох етапів надійної ідентифікації, поєднання яких мінімізує ризики хибної ідентифікації
9.	**Тиск на виборців, оприлюднення та купівля голосів:** проблеми добровільного або примусового оприлюднення голосів, груповий тиск, примус до голосування та купівля голосів	**Таємниця, свобода і доброчесність голосування:** технічні та організаційні механізми, можливість переголосування, підвищення обізнаності, звітування про порушення та правозастосування
10.	**Буденність голосування та абсентеїзм:** зменшення символічної цінності акту голосування призводить до менш масового та об'єднавчого голосування	**Свідоме голосування на основі цінностей:** цифрові технології сприяють активізму і новим традиціям, а громадянська освіта мотивує голосувати
11.	**Спотворене збереження та підрахунок голосів:** результати і-голосування можуть бути спотворені під час запису, зберігання та підрахунку	**Верифіковність і підзвітність:** наскрізна перевірка, технології розподілених реєстрів, система «Prêt à Voter», тестування системи, аудит і підзвітність
12.	**Дискредитація виборчої кампанії:** маніпуляції із голосуванням можуть знизити рівень довіри до інститутів демократії та поставити під сумнів легітимність результатів голосування	**Легітимність і довіра:** завчасне та збалансоване фахове обговорення задуму і-голосування у поєднанні із прозорою комунікацією процесу для широкої громадськості

1. Тенденційна чи нейтральна постановка питання?

Вже на найперших етапах підготовки і-голосування може бути проблематичним формулювання його теми. Здебільшого це стосується дорадчих опитувань громадської думки або обов'язкових до виконання плебісцитів чи референдумів, але також може мати стосунок і до виборів. У рекомендаціях Ради Європи щодо е-голосування чітко прописано: «Уся офіційна інформація має бути представлена рівною мірою, у межах та поза каналами для голосування… Електронний бюлетень, який використовується для е-голосування, не має містити інформації щодо варіантів голосування, окрім тих, які передбачені законом… Якщо інформація про варіанти голосування доступна на місці для е-голосування, вона має бути представлена справедливим чином»[1].

У найгіршому разі спотворений текст бюлетеня для і-голосування: а) порушуватиме встановлений законом (випадковий) порядок шляхом розміщення імені певного привілейованого кандидата на виборну посаду або назви певної партії нагорі списку чи б) розміщуватиме імена конкурентів до привілейованого кандидата внизу списку, в) приховуватиме імена конкурентів серед подібних за звучанням «технічних» кандидатів чи навіть г) міститиме текстову чи візуальну політичну рекламу на користь привілейованого кандидата. Цьому можливо запобігти шляхом попереднього розгляду бюлетеня комісією зі збалансованим складом учасників – або сформованим випадковим чином серед громадян (із застосуванням механізмів рендомократії, тобто демократії жеребкування) або обраних із широкого кола громадських організацій та політичних партій. Додатковим запобіжним заходом може слугувати завчасна публікація тексту бюлетеня, яка надасть достатньо часу для того, щоб виправити будь-які невідповідності.

Маніпулятивний бюлетень для і-голосування для опитування громадської думки, плебісциту чи референдуму може: а) містити двозначне або подвійне питання, яке заплутуватиме або вводитиме в оману учасника голосування чи б) складатися із підтасованої послідовності запитань із прихованими поглядами або почуттями – і цим спрямовувати голос у напрямку до бажаного варіанту. Цей ризик також можливо зменшити завдяки завчасній публікації, обговоренню та виправленню бюлетеня. У підсумку, механізми публічності, прозорості та громадського контролю можуть запобігти зловживанням і-голосування ще на етапі затвердження бюлетеня.

Менш явна маніпуляція може відбуватися у вигляді тенденційної постановки питання під час представлення у мас-медіа. Це особливо небезпечно за умов, коли найпопулярніші мас-медіа у країні або громаді контролюються окремою особою або групою олігархів. У такому разі рішенням є вільний доступ до інтернету, бо інтернет може надавати доступ до онлайн-медіа із низькою вартістю створення та різноманітним змістом.

2. Упереджена поляризація чи цілеспрямоване об'єднання?

Сфера громадської думки містить численні виклики: інформаційні бульбашки, ефект попереднього вибору, групову поляризацію, фейкові новини та викривлену соціальна реальність. Першопочаткова проблема є такою: «світ соціальних медіа створює малі, дуже поляризовані групи осіб, які схильні вірити усьому, що вони чують, байдуже наскільки це далеко від реальності»[2]. Люди, які живуть усередині інформаційної бульбашки, не отримують новин, які ставили би під сумнів негнучкі погляди – їх власні та їхніх соціальних груп. Понад те, люди, які перебувають під впливом схильності до підтвердження, шукають лише таку інформацію, із якою вони вже згідні, а не незалежну перевірку такої інформації. Фальшиві новини використовують ефект попереднього вибору та схильність до підтвердження – як властиві інформаційним бульбашкам риси, що зазвичай поляризують соціальні групи[3]. Позаяк людям притаманні когнітивні упередження і вони схильні об'єднуватися у соціальні групи, які поділяють спільні переконання, ці явища вже є частиною традиційної політики і через це не є проблемою як такі. Але коли вони підсилюються в інтернет-просторі, то стають дійсно проблематичними.

За таких обставин ключовим рішенням є цілеспрямовано сприяти створенню такого оточення, яке заохочує розмаїття поглядів, критичний підхід до поданої інформації та інтелектуальну дискусію. По-перше, доречно

[1] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

[2] Hull, G. 2019. Social Media Is Not Good for Democracy. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 100-104. New York: Greenhaven Publishing.

[3] Hull, G. 2019. Social Media Is Not Good for Democracy. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 100-104. New York: Greenhaven Publishing.

плекати індивідуальну проактивність щодо пошуку альтернативної інформації, заохочувати критичну оцінку джерел та змісту інформації, та формувати звичку складати власну незалежну точку зору, яка спирається на декілька джерел та критичне осмислення. По-друге, резонно заохочувати та підтримувати культуру полемічної і водночас інтелігентної дискусії. Для цього вчені пропонують низку можливих змін до онлайн-форумів та чатів, веб-сайтів та блогів: модерацію, адміністрування, громадський контроль, підписання угоди користувача, де визнаються правила дискусії та наводяться рекомендації щодо деполяризації, аж до покарання у вигляді видалення у разі порушення норм обговорення у дусі неполяризації та співпраці[4]. Для виявлення можливих порушень ці дослідники пропонують застосовувати програмне забезпечення для когнітивного картографування, автоматичного аналізу текстів та аналізу настроїв – щоб висвітлити напрямок обговорення.

Такі втручання спираються на припущення, що орієнтовані на обговорення норми та практики здатні повернути тенденції до поляризації у зворотному напрямку та заохотити поінформоване формування поглядів, ґрунтовне обговорення та більш розмаїті мережі згоди. Із цією метою можливо застосувати такі заходи із деполяризації: 1) створювати безпечний простір для формування більш гнучкої та глобальної ідентичності; 2) просувати офлайнові соціальні взаємодії та структури, які підтримують правила щодо деполяризації і тим самим зменшують онлайн-поляризацію; 3) запроваджувати формати співпраці та переговорів для зменшення мови ворожнечі та збільшення мови примирення; 4) налагоджувати стосунки між людьми, які збентежені, але шукають миру, а не насильства, і цим створюють і підтримують норми деполяризації[5]. Таким чином, нормативні структури простору онлайн-дискусії підштовхуватимуть до висловлення різноманітних поглядів, участі в інтелектуальних та інтелігентних дискусіях та встановлення численних зв'язків між дискутантами, чим вибудують більш складну та взаємопов'язану мережу осіб зі схожими поглядами.

3. Маніпулювання громадською думкою чи регламентація діяльності онлайн-медіа?

Окрім незбалансованостей, які виникають на етапі її формування, громадська думка може бути цілеспрямовано спотворена засобами онлайн-медіа. Великі дані про користувачів надають достатньо інформації для мікротаргетування конкретних учасників голосування за допомогою персоналізованих повідомлень і такого впливу на їхню поведінку, який неможливий за допомогою традиційних мас-медіа. Наприклад, автоматичний аналіз статистики «вподобайок» користувачів Фейсбуку виявився здатним визначити їхні демографічні профілі та основні політичні переконання, які були використані для мікротаргетування конкретних виборців у Сполучених Штатах Америки[6].

Хоча політична реклама у традиційних засобах масової інформації є звичайною практикою виборчих кампаній, із точки зору доброчесності мікротаргетування є сумнівною технологією. Обсяг інформації, який застосовується для таргетування особи, перевищує обсяг, який використовують традиційні засоби масової інформації, а читачі чи глядачі не завжди знають, яку саме інформацію про себе вони надають. Також, повідомлення щодо певного політика, підлаштовані під конкретних виборців, можуть не узгоджуватися між собою або навіть суперечити один одному, чим ставлять під сумнів цілісність відповідної політичної програми. Тоді як повідомлення у традиційних засобах масової інформації можуть переглянути, перевірити та поставити під сумнів інші глядачі, рекламні повідомлення із технологією мікротаргетування складно відстежувати та порівнювати. Понад те, непрозорі алгоритми формування «чорної скриньки» стрічки новин, пошукові алгоритми та сегментація рекламних повідомлень не дають змоги контролюючим органам зрозуміти, яку рекламу показують кому і коли, хто платить за неї, скільки і коли[7]. Крім того, певне повідомлення може бути посилене у соціальних медіа

[4] van Dijk, J.A.G.M., Hacker, K.L, & Mollov, B. 2018. Digital Media and Networking: Opportunities and Constraints for Depolarizing Political Discourse. In: van Dijk, J.A.G.M., Hacker, K.L. *Internet and Democracy in the Network Society*. Pp. 108-130. New York: Routledge.

[5] van Dijk, J.A.G.M., Hacker, K.L, & Mollov, B. 2018. Digital Media and Networking: Opportunities and Constraints for Depolarizing Political Discourse. In: van Dijk, J.A.G.M., Hacker, K.L. *Internet and Democracy in the Network Society*. Pp. 108-130. New York: Routledge.

[6] Hull, G. 2019. Social Media Is Not Good for Democracy. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 100-104. New York: Greenhaven Publishing.

[7] Howard, A., & Wonderlich, J. 2019. Social Media Sites Should Have to Disclose Political Advertising Files. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 105-112. New York: Greenhaven Publishing.

(які ще називають соціальними мережами) або численними повідомленнями (напів)автоматичних ботів із підроблених облікових записів або дуже помітними повідомленнями від таємно проплачених дописувачів. Хоча деякі автори можуть щиро підтримувати певного кандидата, проблеми виникають тоді, коли така діяльність організовується або фінансується таємно. Це створює оманливе враження щирої незалежної підтримки політика або партії, хоча насправді це не так.

Ці виклики потребують комплексних законодавчих, виконавчих та громадських заходів у відповідь. Органи державної влади можуть накласти обмеження, забезпечити оприлюднення та вдатися до примусових заходів у цій сфері: замовники, такі як політичні партії, та надавачі послуг, такі як Фейсбук, мають бути зобов'язані проактивно оприлюднювати вичерпну інформацію про політичну рекламу у машиночитному відкритому форматі онлайн, у відкритому доступі для громадськості та виборчих комісій[8]. Фінансування політичної підтримки має бути явно зазначено самими дописувачами, відстежуватися надавачами послуг соціальних медіа та каратися у випадках, коли така політична підтримка приховується. Наприклад, Фейсбук вже виявляє та вилучає облікові записи користувачів, які демонструють ознаки скоординованої оманливої поведінки. Ба більше, державні заходи мають доповнюватися активною громадською позицією акціонерів онлайн-медіа, висвітленням у мас-медіа, аналітичними записками із цього питання, а також тиском громадськості[9].

4. Технічна несправність системи чи надійне функціонування системи?

Зазвичай застереження щодо голосування із використанням цифрових технологій стосуються технічних проблем функціонування системи голосування, пов'язаних із обладнанням або програмним забезпеченням. Це може бути неправильний код, який призводить до помилок під час голосування або підрахунку голосів, перевантаження системи чи збій у роботі обладнання. У найгіршому разі невеликі помилки під час запуску та налаштування інтернет-додатків можуть повністю скомпрометувати голосування[10]. Справді, такі ризики дійсно існують, позаяк цифрові системи для голосування є централізованими. Тим не менше, їх можливо зменшити за допомогою тестувань із максимальним навантаженням та перевіркою на різноманітні ризики.

Із цим також пов'язана проблема, яку можливо віднести до людського фактору. Адже «неналежно підготовлені адміністратори виборів можуть ненавмисно припускатися помилок, які швидко підірвуть довіру громадськості»[11]. Варто відмітити, що ця проблема не є специфічно притаманною виключно електронному голосуванню, але може трапитися під час будь-якого голосування. Щоб запобігти помилкам у взаємодії між людиною та комп'ютером під час е-голосування, виборчі комісії мають розуміти та довіряти технологіям для голосування, що забезпечується ретельним оцінюванням та ефективним навчанням[12]. Автори огляду також радять переконатися, що зовнішні надавачі послуг, приватні та державні, дотримуються законів і вимог, що забезпечується оцінкою ризиків стосовно можливих зв'язків та залежностей зовнішніх надавачів послуг.

Також у цьому плані дуже доречні рекомендації Ради Європи. Зокрема, вони підкреслюють важливість технічних та організаційних заходів щодо збереження даних навіть у разі аварії в роботі системи, регулярних перевірок роботи системи та наявності користувачів, збереження обладнання для е-голосування у надійному місці, створення резервних копій, наявності плану аварійного відновлення, інструкції, як діяти у надзвичайній ситуації, процедури встановлення оновлень та виправлень у систему, а також безпечного поводження із зашифрованими даними.[13]

---

[8] Howard, A., & Wonderlich, J. 2019. Social Media Sites Should Have to Disclose Political Advertising Files. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 105-112. New York: Greenhaven Publishing.

[9] Howard, A., & Wonderlich, J. 2019. Social Media Sites Should Have to Disclose Political Advertising Files. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 105-112. New York: Greenhaven Publishing.

[10] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.

[11] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.

[12] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.

[13] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

5. Зловмисне хакерство чи кібербезпека та доброчесність?

Імовірно, найбільше занепокоєння стосовно і-голосування викликають ризики щодо кібербезпеки. Джерело хакерських загроз може знаходитися у суспільстві, де відбувається і-голосування, всередині уповноважених органів організації і-голосування, а може походити і від кіберзлочинців з іншої країни чи від вороже налаштованої іноземної держави. Стосовно нападів зсередини самого суспільства, варто відмітити, що дистанційне офлайн-голосування має подібні ризики: наприклад, як у випадку заочного голосування, голосування поштою, під час підрахунку голосів тощо. Завдяки використанню серверів, підключених до мережі інтернет для забезпечення голосування онлайн, і-голосування справді більш вразливе до атак з-за кордону – як індивідуальних, так і режисованих іноземною державою. Так «уряди, які готові вкладати величезні ресурси у напад на будь-яку інтернет-платформу, можуть спрямувати такі ресурси на інтернет-голосування для того, аби змінити результати виборів або підважити довіру громадськості до результатів виборів»[14]. Подібно до протидії впливам на голосування у випадках дистанційного офлайн-голосування, зменшити ризики щодо кібербезпеки онлайн-голосування можливо завдяки розробці кращих механізмів безпеки. До початку і-голосування технічна система має пройти оцінювання та сертифікацію. Рада Європи рекомендує: «незалежний та компетентний орган має оцінити відповідність системи е-голосування та будь-якої складової інформаційно-комунікаційної технології (ІКТ) технічним вимогам» у вигляді офіційної сертифікації або іншого належного контролю[15].

Систему і-голосування можливо зламати різними способами. Наприклад: «будь-хто може спробувати підробити (*зловмисне кодування*) або посадові особи можуть ненавмисно допустити чиєсь втручання у процес голосування (*троянські атаки*)»[16]. В одному аналізі випадку «дослідники показали, що зловмисник може скористатися вразливими сторонами Австралійської системи «iVote» і вставити код для викрадення голосів… зокрема, поставити під загрозу незахищені точки доступ до вай-фай, підробити кеш ISP DNS, вчинити атаку на вразливі роутери та викрасти префікси BGP»[17]. Також вони повідомили, що наступного дня виборча комісія змінила налаштування серверу системи «iVote». В іншому красномовному прикладі «протягом тестування і-голосування до Вашингтону, Округу Колумбія, команда тестувальників провела декілька атак і продемонструвала, що злочинці можуть викрасти секрети, змінити минулі голоси, змінити майбутні голоси, поставити під загрозу таємницю голосування та створити відстрочений ефект прихованості»[18]. Повідомляється, що ретроспективно ці вразливості полагодити доволі просто. Таким чином, деякі системні проблеми є технічними і можуть бути вирішені. Для цього можливо запросити (за винагороду) етичних «білих» хакерів (які знаходять слабкі сторони у безпеці з метою виправити їх та недопустити зловживання лиходіями), щоб випробувати систему на міцність, виявити її вразливі сторони та допомогти вдосконалити її кібербезпеку.

Також можливо запровадити декілька рішень на рівні системної архітектури. У цьому плані Концепція кібербезпеки Національного інституту стандартів і технологій (НІСТ) пропонує декілька рекомендацій, спрямованих на зменшення ризиків зламу: проводити ретельне моделювання загроз, розробити план управління ризиками та стратегію кібербезпеки, застосувати криптографічний захист (для даних, які передаються та даних, які зберігаються), вдосконалити методи шифрування голосування, використовувати спеціально розроблене та надійне обладнання (наприклад, електронну ID-картку), застосовувати перевірку безпеки кінцевої точки (аби підтвердити, що елемент програмного забезпечення е-голосування не був змінений), попередньо налаштоване середовище завантаження або технологію віртуалізації (щоб перервати дію шкідливого програмного забезпечення) та додаткові канали комунікації (такі, як естонський QR-код, який

[14] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.

[15] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

[16] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[17] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.

[18] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.

дає можливість учаснику голосування перевірити свій голос із іншого пристрою)[19]. Хорошим зразком кібербезпеки є естонська система і-голосування, яка використовує захищену ID-картку та можливість перевірки власного голосу. Дослідники стверджують: «немає жодних доказів того, що естонське інтернет-голосування було поставлено під загрозу»[20]. Також, узгоджена, але децентралізована система і-голосування є вдалим рішенням для управління ремонтно-відновлювальних робіт у разі часткової несправності системи або нападу[21].

Крім того, нападник може розшифрувати та опублікувати конфіденційну інформацію, як от, про виборців, чим поставити виборчі комісії перед дилемою скасування виборів або оголошення їх такими, що відбулися, але зіткнутися із розголошенням конфіденційних даних в інтернеті. Тим не менше, навіть цей ризик можливо зменшити. Зокрема: 1) підсумки можуть бути оголошені для підмножин виборців у такий спосіб, щоб кількість голосів за кожного кандидата була достатньо великою, або приховати закодовану інформацію у статистичному шумі, забезпеченому голосами чесних виборців; 2) статистичні дані про недійсні голоси мають бути зведені до мінімуму та оприлюднені в узагальненій формі, а не з точністю до виборчої дільниці чи невеликого виборчого округу; 3) подальші докладні статистичні дані та інформація мають вважатися таємними[22].

Окрім технічних вразливостей, систему і-голосування може поставити під загрозу людський фактор. Так, системні адміністратори, які мають доступ до серверів та програмного забезпечення для голосування, можуть навмисно чи випадково відкрити шлях для атаки через використання заражених USB-карт флеш-пам'яті або через зниження рівня захисту систем[23]. Щоби запобігти таким випадкам, рекомендується проводити ретельне навчання персоналу, який організовує голосування.

Навіть якщо забезпечено найвищий рівень кібербезпеки на рівні центральної системи і-голосування, залишається проблематичною кібербезпека власних пристроїв, які використовуються для і-голосування. За деякими оцінками, «багато персональних комп'ютерів чи мобільних пристроїв, які використовуються для онлайн-голосування, є слабко захищеними»[24]. Із технічної точки зору, нападники можуть запускати атаки типу «відмови в обслуговуванні», які мають на меті зірвати вибори, намагатися переадресувати виборців на підроблені сайти для голосування та організувати масштабні атаки на пристрої користувачів-виборців, можливо, із застосуванням заражень за допомогою попередньо створеної мережі ботів[25]. Ці загрози вважаються одними із найскладніших та найменш розв'язаних проблем інтернет-безпеки. Проте, ретельне тестування системи із максимальним навантаженням та від різноманітних кібератак може зменшити ці ризики.

Нападник також може застосувати зворотне баєсівське зараження для спотворення програмного забезпечення виборців. Це можливо вчинити за допомогою атаки типу «відмови в обслуговуванні» на спам-фільтри виборців – потай навчити спам-фільтр виборця шляхом надсилання листів зі спам-повідомленнями, майстерно насиченими ключовими словами зі справжніх листів від системи для голосування, через що спам-фільтри будуть непомітно відсіювати листи від системи для голосування[26]. Однак, автори дослідження припускають, що користувачі можуть зменшити вплив зворотнього баєсівського зараження – додати електронні адреси виборчих комісій до білого списку і в такий спосіб запобігти відсіюванню листів, а посадові особи, уповноважені проводити вибори, можуть зменшити наслідки нападу – використати паралельні канали

[19] The National Institute of Standards and Technology. 2011. *The Security Considerations for Remote Electronic UOCAVA Voting*.
[20] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.
[21] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.
[22] Wikström, D., Barrat, J., Heiberg, S., & Krimmer, R. 2017. How Could Snowden Attack an Election? In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017.* Pp. 280-291. Cham, Switzerland: Springer.
[23] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.
[24] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.
[25] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.
[26] Jonker, H., Mauw, S., & Schmitz, T. 2017. Reverse Bayesian Poisoning: How to Use Spam Filters to Manipulate Online Elections. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017.* Pp. 183-197. Cham, Switzerland: Springer.

комунікації (до прикладу, розіслати смс-повідомлення) для оповіщення користувачів про те, що реєстраційні дані надіслані.

На учасників голосування можуть бути вчинені персональні хакерські атаки. Нападники можуть заразити комп'ютерним вірусом, викрасти або виманити реєстраційні дані, або вдатися до соціальної інженерії і в такий спосіб завадити виборцю проголосувати, змінити голос, відстежити характер голосування, використати реєстраційні дані виборця для отримання доступу та заподіяння шкоди системі для голосування, змінити результати виборів або зашкодити достовірності результатів виборів[27]. Вірогідно, що такі маніпуляції не зачеплять великої кількості виборців. У будь-якому разі, ці ризики мають бути враховані. Однією із причин того, що виборці є дуже вразливими, є така: «хоча через втрату грошей вони імовірно помітять, що щось не так у їхньому онлайн-банкінгу, анонімність процесу голосування призводить до того, що майже неможливо помітити те, що їхні голоси були змінені»[28]. Проте, це застереження стосується лише таких систем і-голосування, у яких учасники голосування не можуть у будь-який момент перевірити свої голоси. У деяких ІТ-рішеннях вони таки наділені такою можливістю. У цілому, зважаючи на широкий спектр маніпулятивних впливів, спрямованих на учасників голосування, доцільно проводити кампанії із громадянської освіти, які би привертали увагу до ризиків і-голосування та пояснювали, як голосувати безпечно, радили користуватися сучасним антивірусним програмним забезпеченням, ігнорувати листи із виманюванням даних, перевіряти свої голоси тощо.

6. Ексклюзія чи інклюзія?

Одним із джерел занепокоєння щодо і-голосування є питання інклюзії. Зважаючи на складність публічної політики та розмаїття суспільства, критично важливо гарантувати ефективність, плюралізм та справедливість механізмів непрямої або представницької демократії[29]. Якщо поміркувати, і-голосування є викликом для права участі у голосуванні на загальних виборах та викликає суперечки щодо того, хто має мати право голосу, позаяк багато країн обмежують можливість голосування на загальних виборах колом громадян, які проживають у країні (або з принципових або практичних міркувань – організації голосування громадян, які проживають за кордоном)[30]. Однак, у таких випадках і-голосування має потенціал до скасування обмежень та розширення прав і можливостей. По-перше, принцип загального виборчого права гарантує право голосу усім правоздатним громадянам. По-друге, дистанційне інтернет-голосування як вибірковий варіант на додачу до традиційного офлайн-голосування на виборчій дільниці здатне розширити базу виборців. Завдяки цьому запровадження і-голосування може спровокувати дискусію щодо того, хто має право голосу, привести до змін у законодавстві та надати право голосу деяким соціальним групам, виключеним із політичного процесу, наприклад, емігрантам, і цим самим збільшити інклюзивність опитувань громадської думки, консультацій, референдумів та виборів.

Більш суперечливим є питання надання права голосу на основі заслуг. Існує погляд, що для ефективних та справедливих демократичних рішень не завжди бажано збільшувати участь у виборах, якщо це розмиває межі між групами виборців із ґрунтовними (більш сталими та заснованими на співпраці) уподобаннями та іншими виборцями (до прикладу, невимушене і-голосування з дому у кінцевому підсумку не обов'язково є бажаним)[31]. Але таке ставлення суперечить принципам рівності прав та рівності голосів і схильне дискримінувати людей, які хочуть голосувати онлайн – тому воно має бути відхилене із ціннісних міркувань. Твердження, наведене за посиланням також є хибним, тому що обговорення та співпраця онлайн не відбуваються «без зусиль», але часом потребують стільки ж або навіть більше енергії та часу, ніж офлайн. Окрім того, миттєва зміна поглядів може бути логічною, якщо вона спирається на якусь нову інформацію про можливу публічну політику, виборну особу або

[27] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.
[28] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[29] Innerarity, D. 2019. *Politics in the Times of Indignation: The Crisis of Representative Democracy*. London: Bloomsbury Academic.
[30] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[31] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

партію. Навіть якщо зміна настроїв є не раціональною, а емоційною, виборець має на це право. Саме публічні особи та політики мають доносити найбільш доречну, точну та переконливу інформацію про себе до виборців.

До попереднього питання є близькою проблема цифрової нерівності. Викликає занепокоєння те, що «інтернет-голосування може надати політичні права заможним і зробити процес голосування легшим для них, але не допомогти незаможним»[32]. Але поєднання онлайн- і офлайн-форматів як альтернативних насправді зменшує нерівність, позаяк виборець може вільно обрати найзручніший та найбажаніший спосіб голосування. Крім того, наявний перелік заходів, які можуть полегшити використання і-голосування. Зокрема, Рада Європи рекомендує забезпечити, що: 1) інтерфейс системи для голосування легкий для розуміння та використання усіма учасниками голосування; 2) варіанти для голосування на будь-якому клієнтському пристрої підлаштовані під пересічного виборця, який не володіє спеціалізованими навичками користування комп'ютером; 3) учасники голосування залучені до розробки систем е-голосування; 4) нові ІТ-продукти сумісні з попередніми версіями; 5) система е-голосування доступна для осіб з обмеженими можливостями та особливими потребами; 6) на вимогу виборці забезпечені спеціальними інтерфейсами або іншими рівнозначними ресурсами; 7) інтерфейси для і-голосування якомога повніше відповідають приписам, викладеним в Ініціативі інтернет-доступності[33]. Також, наприклад, у європейських країнах, цифрова нерівність зменшується у руслі збільшення цифрової грамотності та поширення використання інтернет-технологій[34].

7. Неточні чи точні реєстри виборців?

Об'єктом маніпуляції також можуть бути реєстри виборців. Проблема може полягати в тому, що посадові особи, уповноважені проводити вибори, які мають найвищі рівні доступу із можливістю додавати до реєстру виборців громадян із правом голосу, вилучати виборців без права голосу, змінювати зразки бюлетенів, визначати час і дату голосування, встановлювати правила проведення виборів та оформлювати виборчі протоколи, можуть зловмисно поставити систему під загрозу або ненавмисно стати співучасниками нападу через використання зараженого пристрою[35]. За таких обставин спотворені реєстри виборців можуть бути використані для того, щоб завадити певним людям голосувати (наприклад, якщо їхні політичні уподобання зрозумілі з їхніх дописів у соціальних медіа) та для голосування за «мертвих душ» (щоб незаконно проголосувати за певну публічну політику, політика або партію).

Ці ризики можливо врахувати та запобігти ним. Згідно із рекомендаціями Ради Європи: «Потрібно забезпечити достовірність, доступність та цілісність реєстрів виборців та списків кандидатів. Необхідно встановлювати справжність джерела даних. Потрібно дотримуватися положень про захист даних»[36]. Для цього існують стандартні технічні та організаційні рішення. Зокрема, автоматизація та комп'ютеризація завдань посадових осіб, уповноважених проводити вибори, має відбуватися відповідно до низки протоколів, які мають запобігти прихованим атакам на систему, забезпечуватися необхідним рівнем профілів для входу до системи, паролів та аудитом, а також супроводжуватися навчальними програмами та просвітницькими кампаніями щодо ризиків кібербезпеки[37].

А на рівні системної архітектури можливо застосувати технології розподілених реєстрів (до прикладу, блокчейн). Завдяки своїй особливій структурі вони встановлюють рівноправну мережу та набір консенсусних

[32] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[33] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[34] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.
[35] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.
[36] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[37] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.

алгоритмів для копіювання, спільного використання та синхронізації узгоджених наборів цифрових даних. Реєстр виборців, до якого застосовується така технологія, значно складніше змінити, хоча для цього потрібно розподілити доступ до нього між кількома суб'єктами (державними установами) та ознайомити системних адміністраторів із цією непростою технологією. Окрім того, така система може перевантажуватися великою кількістю записів і запитів, тому вона потребує ретельного тестування із максимальним навантаженням.

8. Хибна чи надійна ідентифікація?

У неконтрольованому середовищі дистанційного інтернет-голосування існує ризик того, що деякі справжні виборці, наділені правом голосу, не будуть допущені до голосування, тоді як деякі несправжні виборці (напів- або повністю автоматизовані боти або реальні особи, які зловживають вкраденими або підробленими реєстраційними даними) проголосують, хоча вони не мають на те права. У цьому плані може непокоїти такий момент: «буде складно, якщо не взагалі неможливо, переконатися в тому, що конкретний голос був відданий особою, яка мала право голосу, а не порушником»[38]. За найгіршого сценарію, вирішальна кількість таких хибно ідентифікованих учасників голосування може під час електронної консультації-опитування чи обов'язкового до виконання е-референдуму штучно «розігнати» певну публічну політику або під час е-виборів обрати привілейовану особу на державну посаду.

Від цього можливо захиститися завдяки запровадженню кількох етапів надійної ідентифікації, поєднання яких мінімізує ризики хибної ідентифікації. До прикладу, резиденти Естонії володіють засобами цифрової ідентифікації і для них «комбінація «матеріального» маркера (посвідчення особи) і «нематеріального» маркера (PIN-коду) гарантує надійну перевірку того, що особа, яка увійшла у систему, дійсно є відповідною особою»[39]. Гіпотетично, особа може продати свої засоби цифрової ідентифікації. Але це було би подібно до передачі комусь власного паспорту, за яким хтось може оформити банківський кредит або зареєструвати бізнес. Такі ризики є зависокими, щоб до них вдаватися. І навіть для таких випадків зловживання засобами цифрової ідентифікації розроблені запобіжні заходи. Від учасника голосування можуть вимагати зробити цифрове фото навпроти камери безпосередньо перед процесом голосування – таке фото порівнюватиметься з еталонною фотографією виборця, зробленою для посвідчувальних документів про особу, виданих уповноваженими державними органами. Такі аргументи на користь суворішої ідентифікації «часто позиціонуються як компроміс між доступністю процедури голосування для виборців та необхідністю більшого захисту від шахрайства у процесі голосування»[40].

9. Тиск на виборців, оприлюднення та купівля голосів чи таємниця, свобода і доброчесність голосування?

Дистанційне інтернет-голосування є викликом для забезпечення таємниці голосування. Дослідники припускають, що і-голосування несе потенційну загрозу принципу таємного голосування[41]. Тим не менше, розроблені численні технологічні та організаційні механізми, які забезпечують таємницю голосу, відданого через інтернет (і-голосу). Відповідно до рекомендацій Ради Європи, е-голосування: 1) має забезпечити таємницю волевиявлення на усіх етапах процесу голосування; 2) дані реєстру виборців мають бути чітко відокремлені від власне складових для голосування; 3) система е-голосування та будь-яка уповноважена сторона мають захистити дані автентифікації таким чином, щоб несанкціоновані сторони не могли зловжити, перехопити, змінити чи в інший спосіб дізнатися про ці дані; 4) система е-голосування не повинна надавати виборцю підтвердження змісту відданого голосу, яким би могли скористатися треті особи; 5) виборець має бути поінформований про можливі ризики щодо таємності дистанційного е-голосування та рекомендованих

[38] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[39] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[40] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[41] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.

заходів щодо їх зменшення перед голосуванням; 6) виборець має бути поінформований щодо того, як видалити, де це можливо, сліди голосування з пристрою, на якому було здійснено дистанційне голосування; 7) процес е-голосування має бути організований так, щоб унеможливити реконструювати зв'язок між незапечатаним голосом і учасником голосування; 8) інформація про виборця має бути відокремлена від відданого голосу на заздалегідь визначеному етапі підрахунку голосів; 9) будь-яка розшифровка, яка необхідна для підрахунку голосів, має бути виконана якомога швидше після завершення часу, відведеного на голосування[42]. Незважаючи на ці заходи, учасники голосування можуть ненавмисно порушити таємницю голосування і сфотографувати заповнені бюлетені. Але це може трапитися як під час офлайн-, так і онлайн-голосування. У цьому відношенні висловлюється так застереження: «країни мають стояти на сторожі того, щоб виборці не відсилали селфі з кабінок для голосування»[43]. Тож правові обмеження, які застосовуються на практиці та ілюструються показовими прикладами, мають припинити такі дії.

Технічна складність ІТ-рішень наражається на певну критику. Наприклад, розглядається така ситуація: якщо виборцю заздалегідь надати можливість обрати код, який позначатиме варіант вибору (коли голос «А» означає «Б»), відомий тільки виборцю, така схема зазнає краху у складних виборчих системах і, що найпростіше, виборець може не згадати код під час голосування[44]. Однак, виборець так само може забути номер у списку або переплутати ім'я кандидата чи назву публічної політики, якщо бюлетень містить подібні до справжнього «технічні» варіанти. Ризики, пов'язані із запам'ятовуванням, видаються подібними в онлайн- і офлайн-голосуванні і в будь-якому разі мають бути розглянуті та зменшені. І офлайн-вибори можуть мати технічні збої, проте вони проводяться, незважаючи на висловлені занепокоєння, – із ціннісних міркувань підтримки демократії.

Виклик забезпечення таємниці е-голосування пов'язаний із додатковими ризиками. Позаяк неможливо гарантувати те, що ніхто не спостерігає за виборцями, які голосують, це відкриває скриньку Пандори із примусом виборців[45]. Хоча ця проблема має своє рішення. Щоби протидіяти виклику, що примушувач може стояти поруч із виборцем під час голосування, Сполучені Штати Америки дозволяють виборцю голосувати декілька разів і враховують лише останній голос[46]. Справді, право змінювати свій голос необмежену кількість разів до завершення періоду голосування допомагає уникнути безпосередньої небезпеки виборцю, оскільки можливо проголосувати, як наказано, а потім змінити свій голос. Проти цього висловлюють таке заперечення: «це не вирішує проблеми, тому що тиск із метою змінити голос може вплинути на виборця в останню хвилину до завершення голосування»[47]. Однак, намір масово спотворити і-голосування вимагатиме забагато «смотрящих» наглядачів, які мають знаходитися поруч із виборцями наприкінці періоду і-голосування, що робить цей спосіб тиску нереалістичним у великих масштабах.

Понад те, органи управління виборами можуть приготувати запасний варіант офлайн-голосування на виборчій дільниці. Завдяки цьому особа матиме змогу проголосувати офлайн навіть після періоду онлайн-голосування. На противагу цим заходам висувається аргумент, що можливість зміни голосу у контрольованому середовищі, такому, як виборча дільниця, не вирішує питання вразливості доброчесності процесу, позаяк «людина під примусом може бути занадто налякана, щоб іти до виборчої дільниці[48]. Хоча особа може бути налякана і сфотографувати свій бюлетень також і на офлайн-виборах. Далі наводяться такі приклади: «Вивчення випадків в історії Сполучених Штатах Америки, коли голосування проходило відкрито, виявило, що виборці часто були

---

[42] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

[43] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[44] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[45] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.

[46] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[47] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[48] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

об'єктами переслідування та навіть викрадення чи вбивства, якщо вони не голосували відповідно до вимог примушувачів. Навіть за відсутності явного примусу виборці могли взагалі утримуватися від голосування, щоб уникнути переслідування за висловлення власних поглядів»[49]. Щоб захистити від цього виборців, має бути «гаряча» телефонна лінія для повідомлення про такі випадки та професійна правоохоронна система, здатна їх вирішити. Зі стратегічного погляду, в одному моделюванні було продемонстровано, що в інтересах суспільства – не пристосовуватися до очікуваної стратегії агресора, але відкрито оголосити власну публічну політику протидії примусу, і тоді раціональний агресор буде змушений утриматися від примусу[50].

Навіть якщо особа, що голосує, має право голосу та безпосередня загроза відсутня, така особа може не мати щирого наміру голосувати саме так. Виборці можуть відчувати тиск щодо відповідності очікуванням однолітків, можуть вчиняти так, тому що один голос зазвичай не визначає результати виборів, можуть бути об'єктами тиску родини або племені – і такий тиск не був би ефективним за умов таємного голосування на виборчій дільниці[51]. Однак, якщо люди обговорюють свій вибір до початку голосування, тиск із боку однолітків, сім'ї або племені може мати місце і під час офлайн-виборів. Ці ризики існують незалежно від використаної технології голосування та можуть бути зменшені завдяки заохоченню відкритої та інтелектуальної публічної дискусії. Насправді, технологія мобільного і-голосування ускладнює постійний тиск, позаяк особа може знайти час та місце, коли і де нікого немає, і проголосувати через інтернет наодинці.

Навіть якщо немає зовнішнього тиску, може відбуватися підкуп виборців. Щодо цього наводиться така інформація: «Втрата таємності може призвести до підкупу та ринку голосів. Ми маємо докази і зі Сполучених Штатів Америки і з Великої Британії, що підкуп голосів стає непривабливим лише тоді, коли немає зовнішнього механізму, який би гарантував, що голос і справді був відданий так, як заявив виборець»[52]. Це співвідноситься із попередніми рішеннями щодо можливості зміни голосу та голосування офлайн після голосування онлайн. Найкритичніше припущення полягає у тому, що наразі жодна технологія не може ефективно зменшити підкуп виборців[53]. Це складна соціально-політична проблема, яка може трапитися під час як офлайн-, так і онлайн-виборів і має вирішуватися підвищенням обізнаності у поєднанні із правоохоронними заходами.

10. Буденність голосування та абсентеїзм чи свідоме голосування на основі цінностей?

Подальша критика і-голосування ставить під сумнів його цінність для громадянської дії. Припускається, що інтернет-голосування може «вплинути на те, як людина голосує, перетворюючи цю дію радше на «вподобайку», ніж на свідомий акт громадянської участі» та «збільшити вагу, якої виборці надають особистим інтересам на відміну від громадських», знівелювати цінність та мотивацію «вважатися своїми сусідами, друзями, однолітками та родичами як активні та залучені громадяни» та навіть «призвести до зниження явки виборців попри переваги зручності та низької вартості»[54]. Проте, перед тим, як голосувати онлайн, люди можуть вкласти багато часу, уваги та сил у вивчення публічної політики, поставленої на голосування, або політиків у виборчому списку. Тоді акт голосування по інтернету матиме значну цінність. Ба більше, люди можуть публікувати фотографії поруч із пристроями для голосування або із зображенням повідомлення «проголосовано», зберігаючи таємницю голосування. Насправді, цифрові технології полегшують вияв громадянської дії. А наголос на власних чи спільних інтересах та схильність голосувати чи не голосувати є загальною мотивацією та гіпотетично не має залежати від технології голосування.

---

[49] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[50] Jamroga, W., & Tabatabaei, M. 2016. Preventing Coercion in E-Voting: Be Open and Commit. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 1-17. Cham, Switzerland: Springer.

[51] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[52] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[53] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.

[54] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

Інше занепокоєння висловлюється щодо символічної цінності процесу голосування. Із цього приводу наводяться такі міркування: «виконання голосування настільки ж несерйозно, як перемикання каналів на дивані, нівелює церемоніальну природу виборів», «вибори стають такими ж буденними, як натискання клавіш на пульті дистанційного керування, а не вирішальним моментом у житті спільноти або нації», виборці більше не «здійснюють свої права і обов'язки громадян шляхом виконання церемоніального зібрання зі своїми співгромадянами на виборчій дільниці» та їм бракує перетворення «зібрання окремих індивідів на суверенний народ»[55]. Хоча навпаки, і-голосування може породити нові традиції, такі, як повідомлення у соціальних медіа зі спільними хештегами, і в такий спосіб поєднати співгромадян. Ба більше, важливість голосування залежить не від відстані, а від цінностей. Їх можливо розвинути завдяки громадянській освіті та збільшення обізнаності.

11. Спотворене збереження та підрахунок голосів чи верифіковність і підзвітність?

Результати і-голосування можуть бути спотворені на етапах запису та підрахунку голосів. Тому Рада Європи встановила низку рекомендацій щодо забезпечення достовірності результатів е-голосування. Вони постановляють, що необхідно вжити заходів аби забезпечити, що: 1) рівно відповідну кількість голосів віддано від кожного виборця, збережено в електронній урні з бюлетенями та враховано у результатах виборів; 2) якщо виборець має право віддати електронний голос декілька разів, то враховується тільки останній голос; 3) якщо виборець має право проголосувати із використанням кількох способів голосування, тоді зараховується тільки один голос; 4) в усіх інших випадках – виборець не може віддати більше одного голосу; 5) в усіх випадках – виборця чітко інформують щодо наявних можливостей голосування та щодо правил підрахунку голосів[56].

Щоб забезпечити достовірні результати, у системах і-голосування запроваджують можливості перевірки. Зокрема, можливість наскрізної (E2E) перевірки означає: «виборці та потенційні зовнішні аудитори мають мати можливість перевірити чи оприлюднений результат виборів є точним, тобто, чи відповідає він голосам, відданим виборцями, навіть якщо пристрої для голосування та сервери мають помилки у програмуванні чи явно шкідливі»[57]. Автори наведеного дослідження далі уточнюють, що індивідуальна верифіковність досягається тоді, коли відправник може перевірити, чи повідомлення досягло призначення, але не може визначити, чи це так для інших виборців, тоді як універсальна верифіковність гарантує можливість публічної перевірки коректності підрахунку голосів. Перспективний підхід полягає у тому, що «система голосування із можливістю прикінцевої перевірки (E2EVV) викорінить фальсифікацію виборів завдяки наданню виборцям можливості перевірити не лише те, що їхні голоси були віддані належно, а також і те, що вони були коректно записні та підраховані»[58].

До прикладу, навіть естонська надійна система і-голосування може бути вразливою до нападів, націлених на результати виборів. Щоби проілюструвати такий випадок і підтвердити цю гіпотезу, було розроблене одне шкідливе програмне забезпечення, яке продемонструвало можливість змінити або заблокувати голос так, щоб виборець це не помітив. У відповідь на це були розроблені два передові механізми перевірки: 1) незалежний мобільний обчислювальний пристрій, який завантажує криптограму голосу із сервера зберігання даних та грубо зламує його за допомогою випадкового шифрування, отриманого з комп'ютера виборця за допомогою QR-коду; 2) програмне забезпечення, розміщене на сервері, яке генерує код підтвердження для виборця[59]. Такий протокол запроваджує вищий рівень безпеки, адже для зламу властивостей перевірки або конфіденційності потребує зловмисної співпраці принаймні двох сторін.

---

[55] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[56] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

[57] Küsters, R., & Müller, J. 2017. Cryptographic Security Analysis of E-voting Systems: Achievements, Misconceptions, and Limitations. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp. 21-41. Cham, Switzerland: Springer.

[58] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.

[59] Kubjas, I., Pikma, T., & Willemson, J. 2017. Estonian Voting Verification Mechanism Revisited Again. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp. 306-317. Cham, Switzerland: Springer.

Для забезпечення надійності зберігання даних про голосування та надійності підрахунку голосів також корисно застосувати передові технології е-голосування. Однією з них є блокчейн – відкритий розподілений реєстр, стійкий до змін даних завдяки криптографічному запису даних, який для зміни даних потребує погодження учасників рівнопорядкової мережі. Іншою системою голосування є «Prêt à Voter», яка застосовує упорядкований випадковим чином та зашифрований криптографічно список кандидатів. Вона водночас уможливлює миттєвий автоматичний підрахунок результатів виборів, дає можливість виборцю перевірити власний голос та захищає таємницю голосування. І блокчейн і «Prêt à Voter» є рішеннями, які «гарантують, що жодна сторона не матиме змоги контролювати, вилучати або змінювати дані й таким чином спотворювати результати голосування»[60]. Хоча залишаються ризики, пов'язані з тим, що технологія блокчейн не захищає інформацію під час її поширення в інтернеті, а також не забезпечує більшу стійкість серверів та інфраструктури до постійних загроз підвищеної складності (APT)[61]. Зважаючи на це, тестування системи і-голосування у меншому масштабі або для дорадчого голосування буде розважливим рішенням.

На додачу до запровадження кібербезпечної системи і-голосування та увімкнення функції наскрізної перевірки, доцільно, щоб органи управління виборами та громадянське суспільство проводили аудит за замовчуванням. Це обґрунтовується тим, що за складністю процедур і-голосуванням може заховатися спотворення даних про голосування. Так, моделювання австралійських і-виборів показало, що завдяки використанню маніпуляції на основі «MOV» та мінімізації змін першого вибору нападник із високим ступенем впевненості може уникнути автоматичного перерахунку та успішно змінити переможця виборів[62]. Тому автори дослідження наголошують на важливості ретельних аудитів виборів заради зменшення ризиків. В ідеалі, такі перевірки мають охоплювати увесь набір даних голосів. Зокрема, аудит у вигляді порівняння бюлетенів потребує незалежного підрахунку не тільки вибірки, а усіх електронних бюлетенів, – аби перевірити, чи електронна система виборів підвела підсумки точно[63].

Рада Європи встановила комплекс стандартів аудиту. Зокрема, відповідно до них: 1) система е-голосування підлягає аудиту; 2) система аудиту має бути відкритою та комплексною і оперативно повідомляти про потенційні проблеми та небезпеки; 3) система аудиту має фіксувати моменти часу, події та дії; 4) автоматизовані інструменти та процедури системи мають бути здатними до швидкого і точного аналізу даних та звітування про них, щоб у такий спосіб уможливити швидкі корегувальні дії; 5) система аудиту має надавати звіти, які можливо перевірити, про перехресну перевірку даних, напади на систему або мережу, виявлення та повідомлення про вторгнення, маніпулювання даними, шахрайство та спроби шахрайства; 6) система е-голосування має підтримувати надійні синхронізовані джерела часу; 7) точність джерела часу має бути достатньою для збереження часових міток для аудиту і даних спостережень, а також для дотримання часових обмежень реєстрації, номінації, голосування чи підрахунку; 8) висновки за підсумками аудиту мають бути враховані у майбутніх е-виборах[64].

Окрім можливості перевірки, система і-голосування повинна бути підзвітною. Підзвітність дає можливість не лише перевірити, чи гарантується бажана властивість, наприклад, що результати виборів правильні, а й забезпечити, що виявити порушників можливо[65]. Автори дослідження пояснюють, що підзвітність посилює стимули, щоб усі сторони дотримувалися своїх ролей, позаяк у разі порушень їх можливо виявити і тоді вони зазнають значних фінансових стягнень, правових покарань або репутаційних втрат.

---

[60] Хуткий Д. Е-голосування в Україні: досягнення, виклики та перспективи. *Огляд Україна Брюссель*. 2020. Квітень. С. 11-13.
[61] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.
[62] Blom, M., Stuckey, P.J., & Teague, V.J. 2019. Election Manipulation with Partial Information. In: Krimmer, R. et al (eds.) *Electronic Voting: Fourth International Joint Conference, E-Vote-ID 2019*. Pp. 32-49. Cham, Switzerland: Springer.
[63] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.
[64] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[65] Küsters, R., & Müller, J. 2017. Cryptographic Security Analysis of E-voting Systems: Achievements, Misconceptions, and Limitations. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp 21-41. Cham, Switzerland: Springer.

12. Дискредитація виборчої кампанії чи легітимність і довіра?

Незалежно від того, чи мали місце спроби зламу і-голосування, принципово важливо, щоби громада або суспільство погодилися, що процес і-голосування відбувся належним чином, і цим підтвердили його легітимність. Недостатньо, щоб вибори дійсно відповідали вимогам загального, рівного, вільного і таємного виборчого права, адже для існування демократії виборці мають вірити, що ці вимоги були виконані, і не повинні мати підстав сумніватися у тому, що голосування відбулося належним чином[66]. Це критично важливо для першого досвіду і-голосування. Позаяк перший негативний досвід – або неналежна реакція на виявлені вразливості – може налаштувати учасників виборів проти такої технології, після чого буде складно відновити довіру[67]. Зманіпульоване голосування може зашкодити не лише ставленню до певної виборчої технології, але й до демократії в цілому. Тому масштабне шахрайство на виборах здатне підважити довіру до демократії[68].

У цьому відношенні, регулярні заходи із прозорої комунікації життєво необхідні для підтримки довіри громадськості. Коли у 2017 році в естонській системі ID-карток була виявлена вразливість, центральні органи державної влади ухвалили публічну політику максимальної прозорості щодо впливу вразливості та заходів, вжитих для зменшення її впливу, – цьому сприяла суспільна довіра до влади та нечисленне населення[69].

Із цього приводу доречні наступні рекомендації: 1) уряди мають бути прозорі щодо усіх аспектів е-голосування; 2) органи, уповноважені проводити вибори, повинні оприлюднювати офіційний список програмного забезпечення, використаного для е-виборів; 3) публічний доступ до елементів системи е-голосування та інформації про них, зокрема, документації, вихідного коду та угод про нерозголошення, має бути забезпечений для залучених сторін та ширшої громадськості заздалегідь до початку виборів; 4) запровадження електронних технологій голосування має включати розробку комплексних, детальних, покрокових інструкцій включно із посібником щодо процедур; 5) складові системи е-голосування мають бути відкриті для перевірки та сертифікації; 6) системи е-голосування мають створювати надійні та достатньо деталізовані дані спостережень для проведення спостереження за виборами; 7) має існувати можливість надійно визначити час, коли певна подія створила дані спостереження; 8) слід дотримуватися достовірності, доступності та цілісності даних; 9) вітчизняні та міжнародні спостерігачі повинні мати доступ до усієї необхідної документації щодо процесу е-голосування, до тестування програмного забезпечення та обладнання, та до процесів оцінки і сертифікації[70].

Громадська думка населення є чутливою до постановки питання про формат голосування. До прикладу, у Сполучених Штатах Америки було виявлено такі закономірності: коли виборцям надати міркування про фальсифікації голосування, це схиляє їх до більшої підтримки паперових варіантів на противагу машинам для голосування із сенсорним екраном, і, навпаки, коли виборцям надати міркування щодо зручності, це схиляє їх віддавати перевагу е-голосуванню, а не паперовим варіантам; ознайомлення із міркуваннями щодо фальсифікації або зручності викликає статистично значущі відхилення від уподобань виборців щодо виборчих систем, із якими вони вже обізнані[71]. Тому обговорення варіантів паперового, стаціонарного електронного чи дистанційного інтернет-голосування має бути збалансованим і об'єктивним.

Ставлення політиків та фахівців, обізнаних щодо технології та публічної політики і-голосування, також важливе для встановлення довіри до інтернет-голосування. Зокрема, доречно залучати вчених, активістів та політиків на ранніх етапах розробки концепції і-голосування, уповноважувати експертів приймати рішення та чітко

---

[66] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[67] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.

[68] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.

[69] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.

[70] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

[71] Alvarez, R.M., Levin, I., & Li, Y. 2018. Fraud, Convenience, and E-voting: How Voting Experience Shapes Opinions about Voting Technology. *Journal of Information Technology & Politics, 15, 1*, 94-105, DOI: 10.1080/19331681.2018.1460288

зазначати, як саме їхні пропозиції були враховані. Протягом періоду голосування підвищити рівень довіри також може публікація відкритого коду програмного забезпечення і-голосування, оперативне оприлюднення результатів та відкритість до громадського аудиту. Також важливо роз'яснювати технічні, політичні та соціальні виміри і-голосування журналістам та лідерам громадської думки, ілюструвати лаконічною інфографікою та відео-прикладами. Переходу до і-голосування також може сприяти нейтральна підтримка політичних еліт[72].

Висновки

Виконаний аналіз доводить, що і-голосування має численні ризики, але їх можливо зменшити. Для кожного проблемного питання, виявленого дослідниками та практиками, вже розроблені декілька відповідних рішень. Тому, якщо вже вирішено запроваджувати і-голосування, далі потрібно ретельно зменшувати ризики.

Численні виклики пов'язані із технічними аспектами системи голосування (обладнанням та програмним забезпеченням): технічна несправність, злам, загроза реєстру виборців, хибна ідентифікація виборця, оприлюднення голосів, порушення у процесі збереження та підрахунку голосів. Проте, передові рішення щодо кібербезпеки та організаційні заходи мають бути достатніми для захисту системи і-голосування. Зважаючи на складність системи і-голосування, зусилля щодо її захисту та зламу можуть виглядати як нескінченна «гонка озброєнь». Тим не менше, залучення «білих» етичних хакерів для перевірки на міцність та вдосконалення системи має надати органам управління виборами додаткову перевагу. У будь-якому разі, деякі країни продемонстрували високий рівень надійності системи у польових умовах і-голосування.

Інші можливі зловживання стосуються певних «політичних» прийомів впливу на формат голосування, адміністраторів голосування та виборців. До них відносять: тенденційну постановку питання, упереджене обговорення в онлайн-медіа, ексклюзію виборців, тиск на виборців та підкуп виборців. Вони потребують комплексних запобіжних заходів щодо змін до законодавства, публічної прозорості, громадського контролю, правозастосування та публічної підзвітності. Позаяк уряди мають найвищі повноваження, посилені активним громадянським суспільством, разом вони достатньо сильні для втілення заходів із протидії зловживанням.

А деякі упередження та маніпуляції впливають на окремих виборців та на громадськість у цілому, будучи «соціальними». Це – групова поляризація, спотворення соціальної реальності, груповий тиск, буденність голосування, абсентеїзм та дискредитація кампанії. Ці виклики потребують свідомих завчасних заходів щодо створення об'єднавчого простору обговорення, запуску кампаній громадянської освіти, підвищення обізнаності та мобілізації до дії, доповнених фаховими обговореннями та прозорим спілкуванням із громадськістю. Імовірно, це найскладніша ділянка діяльності, оскільки вона залежить від зміни особистих ставлень та загальної громадської думки. Тим не менше, суспільні зміни таки відбуваються, хоча зазвичай і поступово.

Масштаб розповсюдження і-голосування можливо проілюструвати на прикладі його застосування для і-виборів посадових осіб. Позаяк офіційні і-вибори на виборні посади є обов'язковими для виконання, наділяють переможців владою та відкривають шлях до прямого впливу на політичну діяльність та публічну політику, вони мають «високі ставки». Від початку історично перших обов'язкових до виконання і-виборів 2003 року деякі країни випробували і-вибори і відмовилися від них, переважно через занепокоєння щодо кібербезпеки. І хоча ці випадки широко обговорювалися переважно у світлі виявлених проблем, деякі з цих країн насправді розглядають можливість повернення і-виборів. Понад те, кількість країн, які проводять і-вибори, хоч і невелика в абсолютних числах, є виразно більшою за кількість країн, які відмовилися від і-виборів. Ще більше країн розглядають можливість запровадити і-вибори у майбутньому, і їхня кількість зростає. Їхні уряди роблять висновки з уроків попередників, виконують дослідження, розробляють техніко-економічне обґрунтування, ухвалюють публічні політики на основі фактичних даних, тестують системи блокчейн і «Prêt à Voter», проводять пілотні експерименти та дискутують з експертами і громадськістю. І хоча це триває роками, зважаючи на довгострокові переваги збільшення інклюзивності, економії часу і коштів, та створення репутації, і-голосування – це справа, що вартує зусиль.

[72] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.

Додатки

Таблиця 1. Країни, які раніше використовували, але відмовилися від обов'язкового для виконання і-голосування на виборах посадових осіб (станом на травень 2020 року – 2)

Джерело: якщо не зазначено інакше – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Країна	Роки втілення	Масштаб і-голосування	Наділені правом і-голосу	Причини офіційного припинення
Нідерланди	2004 2004 2006[73]	Місцевий Європейський Союз Загально-державний	Виборці у певних округах (Рійнленд) Виборці за кордоном Виборці за кордоном	2008 рік: стурбованість щодо проблемних питань кібербезпеки, піднята громадськими активістами та перейнята урядом[74]
Норвегія	2011 2013	Місцевий Загально-державний	Виборці у певних округах (10 міських громад) Виборці у певних округах (10 міських громад)	2014 рік: стурбованість уряду щодо кібербезпеки та впливу на явку виборців[75]

Таблиця 2. Країни, які використовували, скасували, і розглядають можливість повернення обов'язкового для виконання і-голосування на виборах посадових осіб (станом на травень 2020 року – 2)

Джерело: якщо не зазначено інакше – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Країна	Роки втілення	Масштаб і-голосування	Наділені правом і-голосу	Стан справ
Швейцарія (втілення)[76]	2003–2018 2008–2018	Місцевий Загально-державний	Виборці у певних округах (до 13 кантонів) Виборці за кордоном (із певних округів – до 13 кантонів)	2019 рік: причина припинення – політична суперечка щодо питань кібербезпеки[78]
Швейцарія (тестування)[77]	2019	Загально-державний	Окремі групи виборців у певних округах Виборці за кордоном	2019 рік: ухвалене рішення про тестування системи і-голосування

[73] Caarls, S. 2010. *E-Voting Handbook: Key Steps in the Implementation of E-Enabled Elections*. Strasbourg: Council of Europe.
[74] Loeber, L. 2014. *E-voting in the Netherlands; past, current, future?* Conference Paper. October. URL: https://www.researchgate.net/publication/301547849_E-voting_in_the_Netherlands_past_current_future
[75] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.
[76] Germann, M., & Serdült, U. 2014. Internet Voting for Expatriates: The Swiss Case. *JeDEM: eJournal of eDemocracy and Open Government, 6, 2,* 197-215. DOI: https://doi.org/10.29379/jedem.v6i2.302
[77] Geiser, U. 2019. E-voting suffers another setback amid expat Swiss concerns. *SWI: Swissinfo.ch*. 27 June. URL: https://www.swissinfo.ch/eng/digital-democracy_e-voting-suffers-another-setback-amid-expat-swiss-concerns/45059918
[78] Geiser, U. 2019. E-voting suffers another setback amid expat Swiss concerns. *SWI: Swissinfo.ch*. 27 June. URL: https://www.swissinfo.ch/eng/digital-democracy_e-voting-suffers-another-setback-amid-expat-swiss-concerns/45059918

Країна	Роки втілення	Масштаб і-голосування	Наділені правом і-голосу	Стан справ
Франція (втілення)[79]	2012-2016	Загально-державний	Виборці за кордоном	2017 рік: причина припинення – стурбованість щодо кібербезпеки
Франція (тесту-вання)[80]	2020	Місцевий	Виборці за кордоном	2020 рік: проведені тестування платформи для дорадчого і-голосування

Таблиця 3. Країни, які наразі використовують обов'язкове для виконання і-голосування на виборах посадових осіб (станом на травень 2020 року – щонайменше 6)

Джерело: якщо не зазначено інакше – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Країна	Роки втілення	Масштаб і-голосування	Наділені правом і-голосу	Особливості
Вірменія[81]	2012, 2013 2017, 2018	Загально-державний Загально-державний	Дипломатичний персонал та їх родини, виборці за кордоном Дипломатичний персонал та їх родини, виборці за кордоном, військовослужбовці	Результати виборів зберігаються у файлах журналу, гіпотетично вразливих до зловживань
Австралія	2007[82] 2011–дотепер[83]	Загально-державний Місцевий	Військовослужбовці Виборці у певних округах (Новий Південний Уельс та Західна Австралія)	І-вибори продемонстрували: прийнятні витрати; бажаність (включно зі здатністю зберегти таємницю голосування) та явний вплив на поведінку виборців; впевненість у виборчій системі[84]
Канада	2003–дотепер[85]	Місцевий	Виборці у певних округах (Онтаріо та Нова Шотландія)	Кількість та вид реєстраційних даних (PIN-код, дата народження, питання безпеки, та попередня реєстрація за різними даними) варіюють;

[79] Leigh, T. 2017. France drops electronic voting for citizens abroad over cybersecurity fears. *Reuters*. 6 March. URL: https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233

[80] The French Ministry for Europe and Foreign Affairs. 2020. French citizens abroad – Approval of electronic voting for consular elections. 15 January. URL: https://www.diplomatie.gouv.fr/en/the-ministry-and-its-network/news/2020/article/french-citizens-abroad-approval-of-electronic-voting-for-consular-elections-15

[81] Manougian, H. 2020. Did You Know Armenia Allows Internet Voting? (But It's only for Some). *EVN Report*. 13 February. URL: https://www.evnreport.com/politics/did-you-know-armenia-allows-internet-voting-but-it-s-only-for-some

[82] Lundie, R. 2016. Electronic voting at federal elections. *Parliament of Australia.* URL: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/ElectronicVoting

[83] Goodman, N., & Smith, R. 2016. Internet Voting in Sub-national Elections: Policy Learning. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 164-177. Cham, Switzerland: Springer.

[84] Lundie, R. 2016. Electronic voting at federal elections. *Parliament of Australia.* URL: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/ElectronicVoting

[85] Government of Canada. 2017. Online Voting: A Path Forward for Federal Elections. January. URL: https://www.canada.ca/en/democratic-institutions/services/reports/online-voting-path-forward-federal-elections.html#toc21

Країна	Роки втілення	Масштаб і-голосування	Наділені правом і-голосу	Особливості
				повідомлення про технічні та безпекові питання є поодинокими; виборці мають позитивні враження[86]
Естонія	2009, 2014, 2019 2006, 2007, 2011, 2015, 2016, 2019 2005, 2009, 2013, 2017[87]	Європейський Союз Загально-державний Місцевий	Усі виборці	І-голосування проводиться протягом семи днів перед паперовим голосуванням у день виборів; застосовується перевірка, що голоси зараховані належно; і-голосування є політично нейтральним і не зміщує результати виборів; існує високий рівень впевненості та довіри до системи та процедур[88]
Панама	2014, 2018[89]	Загально-державний, місцевий	Виборці за кордоном	Щоби проголосувати, виборці мають надати дійсне посвідчення особи[90]
Сполучені Штати Америки	2016–дотепер	Загально-державний, місцевий	Виборці за кордоном, військовослужбовці, виборці у певних округах (понад 30 штатів)[91]	Технічні рішення залежать від штату; фахівці відмічають проблемні питання кібербезпеки[92]

Таблиця 4. Країни, які розглядають можливість запровадження обов'язкового для виконання і-голосування на виборах посадових осіб (станом на травень 2020 року – щонайменше 17)

Джерело: якщо не зазначено інакше – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Країна	Роки досліджень, тестувань чи розробки	Масштаб і-голосування	Наділені правом і-голосу	Стан справ
Австрія	2004	Загально-державний	Усі виборці	Виконане техніко-економічне обґрунтування[93]

[86] Goodman, N., & Smith, R. 2016. Internet Voting in Sub-national Elections: Policy Learning. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 164-177. Cham, Switzerland: Springer.
[87] Valisimed. 2020. Toimunud valimiste arhiiv. URL: https://www.valimised.ee/et/toimunud-valimiste-arhiiv
[88] Vinkel, P., & Krimmer, R. 2016. The How and Why to Internet Voting an Attempt to Explain E-Stonia. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 178-191. Cham, Switzerland: Springer.
[89] Tribunal Electoral. 2020. Elecciones Generales 1994-2019. URL: https://www.tribunal-electoral.gob.pa/eventos-electorales/elecciones-generales-1994-2019/
[90] Fierro, C.N. et. al. 2016. *Electoral Studies in Compared International Perspective. Voting from Abroad in 18 Latin American Countries*. México, Mexico: National Electoral Institute. URL: http://www.undp.org/content/dam/undp/library/Democratic%20Governance/Electoral%20Systems%20and%20Processes/Voting%20from%20Abroad%20in%2018%20Latin%20American%20Countries%20web%20version%20ENG.pdf
[91] Applegate, M., Chanussot, T., & Basysty, V. 2020. Considerations on Internet Voting: An Overview for Electoral Decision-Makers. Arlington, VA: IFES.
[92] Parks, M. 2019. In 2020, Some Americans Will Vote on Their Phones. Is That the Future? *NPR*. 7 November. URL: https://www.npr.org/2019/11/07/776403310/in-2020-some-americans-will-vote-on-their-phones-is-that-the-future?t=1588522064124
[93] Bundesministerium Inneres. 2020. Wahlen. Wahlrecht in Österreich, Überblick. URL: https://www.bmi.gv.at/412/start.aspx

Країна	Роки досліджень, тестувань чи розробки	Масштаб і-голосування	Наділені правом і-голосу	Стан справ
Гаїті	2017	Загально-державний	Усі виборці	Виконане техніко-економічне обґрунтування[94]
Ісландія	2014	Місцевий	Виборці у певних округах (Рейк'явік)	Виконане техніко-економічне обґрунтування[95]
Індія[96]	2010–2011	Місцевий	Виборці у певних округах	Проведене тестування обов'язкового до виконання і-голосування[97]
Фінляндія[98]	2016–2017	Загально-державний, місцевий	Усі виборці	Виконане техніко-економічне обґрунтування
Мексика	2012 2016	Місцевий Загально-державний, місцевий	Виборці за кордоном Виборці за кордоном	Проведене тестування обов'язкового до виконання і-голосування[99] Розроблені офіційні рекомендації[100]
Молдова	2016	Загально-державний	Усі виборці	Виконане техніко-економічне обґрунтування та розроблена дорожня карта[101]
Нова Зеландія[102]	2016, 2019	Місцевий	Виборці у певних округах	Започатковані тестування обов'язкового до виконання інтернет-голосування
Пакистан	2019	Загально-державний	Виборці за кордоном	Проведені тестування системи інтернет-голосування у невеликому масштабі[103]

[94] Chéry, P.M. 2017. *Analysis of the Feasibility of Electronic Voting in Haiti. Working paper.* 17 February. Copenhagen Consensus Center. URL: http://www.copenhagenconsensus.com/sites/default/files/electronic_voting_chery.pdf
[95] Island.is. 2020. Overview of the proposed solution. URL: https://vefur.island.is/media/pdf-skjol-a-island.is-2014/RegistersIceland-evoting.pdf
[96] Election Commission of India. 2020. Digital Inclusion for citizens in India for democracy. URL: https://eci.gov.in/divisions-of-eci/ict-apps/
[97] Scytl. 2020. State of Gujarat India. Internet voting for municipal elections. URL: https://www.parliament.uk/documents/speaker/digital-democracy/GUJARATINDIA.pdf
[98] Vaalit Val. 2020. Electronic voting in Finland. URL: https://vaalit.fi/en/electronic-voting1
[99] Munive, E.-Y. 2012. Mexican experience of e-voting. *Diplo Internet Governance Community.* 13 July. URL: http://www.diplointernetgovernance.org/profiles/blogs/mexican-experience-of-e-voting
[100] SEGOB. 2016. Acuerdo. *SEGOB*. 1 December. URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5463327&fecha=01/12/2016
[101] Republica Moldova. Comisa Electorala Centrala. 2016. *Feasibility study on Internet Voting for the Central Electoral Commission of the Republic of Moldova. Report and Preliminary Roadmap*. Chisinau, Moldova: Republica Moldova. Comisa Electorala Centrala. URL: https://www.undp.org/content/dam/moldova/docs/Publications/MD-IVOTE-FS-and-Roadmap_cleanENG.pdf
[102] Molineaux, J. 2019. *Solving and creating problems: Online voting in New Zealand*. January. Auckland, New Zealand: Auckland University of Technology. URL: https://thepolicyobservatory.aut.ac.nz/__data/assets/pdf_file/0003/302538/Solving-and-creating-problems-online-voting-in-New-Zealand.pdf
[103] Haq, H.B., McDermott, R., & Ali, S.T. 2019. *Pakistan's Internet Voting Experiment*. July. URL: https://www.researchgate.net/publication/334558559_Pakistan%27s_Internet_Voting_Experiment

Країна	Роки досліджень, тестувань чи розробки	Масштаб і-голосування	Наділені правом і-голосу	Стан справ
Португалія	2005	Загально-державний	Виборці за кордоном	Проведений дорадчий експеримент з і-голосування[104]
Росія[105]	2019	Місцевий	Виборці у певних округах (Москва)	Проведене тестування обов'язкового до виконання і-голосування із використанням системи приватного блокчейну
Сьєрра-Леоне	2018	Місцевий	Виборці у певних округах	Розпочата розробка системи і-голосування на основі системи блокчейн повного циклу[106]
Іспанія	2018 2003	Загально-державний Місцевий	Усі виборці Виборці за кордоном із певних округів (Каталонія)	Виконане техніко-економічне обґрунтування[107] Проведене тестування дорадчого і-голосування
Туреччина	2011	Загально-державний	Усі виборці	Виконане техніко-економічне обґрунтування включно з аналізом можливої системи і-голосування «Prêt à Voter»[108]
Україна	2018 2019	Загально-державний Загально-державний	Виборці за кордоном Виборці за кордоном	Проведений експеримент дорадчого і-голосування на основі системи блокчейн[109] Розпочата розробка відповідних нормативно-правових актів[110]
Об'єднані Арабські Емірати	2011	Загально-державний	Усі виборці	Проведене тестування дорадчої системи і-голосування[111]
Велика Британія	2002, 2003, 2007	Місцевий	Виборці у певних округах (6 окружних рад)[112]	Проведені тестування обов'язкового до виконання і-голосування[113]

[104] Comissão Nacional de Eleições. 2020. Voto electrónico. URL: http://www.cne.pt/content/voto-electronico
[105] Официальный сайт Мэра Москвы. Электронные выборы в Московскую городскую Думу. 2020. URL: https://www.mos.ru/city/projects/blockchain-vybory/
[106] E&T editorial staff. 2018. Blockchain technology deployed in Sierra Leonean election. *E&T*. 16 March. URL: https://eandt.theiet.org/content/articles/2018/03/blockchain-technology-deployed-in-sierra-leonean-election/
[107] Riera, A. & Cervelló, G. 2013. *Experimentation on Secure Internet Voting in Spain*. URL: https://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-10.pdf
[108] Adalier, O. et. al. 2011. A Case Study for Turkey: A Secure Paper-Based Electronic Voting System. *International Journal of eBusiness and eGovernment Studies, 3, 1*. URL: https://dergipark.org.tr/en/download/article-file/257068
[109] Suberg, W. 2018. Ukraine Electoral Commission Uses NEM Blockchain for Voting Trial. *Cointelegraph*. 8 August. URL: https://cointelegraph.com/news/ukraine-electoral-commission-uses-nem-blockchain-for-voting-trial
[110] Шишацкий, Е. & Юрасов, С. Большое интервью с Михаилом Федоровым. *Ліга.Tech*. 2019. 5 серпня. URL: https://tech.liga.net/technology/interview/didjital-strateg-zelenskogo-za-kajdym-reestrom-est-smotryaschiy-ot-kriminala
[111] ICA. 2020. E-Voting UAE: A Case Study. URL: https://www.ica.gov.ae/userfiles/EVoting_UAE_%20A%20Case%20Study.pdf
[112] Barry, C. et. at. 2002. *eVolution not revolution. Electronic Voting Status Report 2*. September. URL: https://www.vec.vic.gov.au/files/RP-EvolutionNotRevolution.pdf
[113] Kobie, N. 2015. Why electronic voting isn't secure – but may be safe enough. *The Guardian*. 30 March. URL: https://www.theguardian.com/technology/2015/mar/30/why-electronic-voting-is-not-secure