

МЕТОДИ ВИРІШЕННЯ ПРОБЛЕМИ ПРИМУСУ В ЕЛЕКТРОННИХ СИСТЕМАХ ГОЛОСУВАННЯ

У сучасних умовах стрімкого розвитку інформаційних технологій та збільшення кількості користувачів глобальної мережі Інтернет, впровадження електронної демократії є одним з ключових завдань для забезпечення соціального та економічного розвитку суспільства. Одним з інструментів електронної демократії є електронне голосування. Електронне голосування з'явилося як заміна паперовому, оскільки такий вид голосування може бути економічно вигідним, прозорим і неупередженим. Проте досвід використання електронного голосування у низці країн за останні три десятиліття свідчить про те, що впровадження таких систем було не надто успішним через недоліки безпеки та конфіденційності, які спостерігалися протягом тривалого часу. Однією з найбільших проблем систем голосування є загроза примусу, який змушує виборців змінити своє волевиявлення або взагалі утриматися від голосування проти їх волі. І, хоча на сьогоднішній день у багатьох системах електронного голосування впроваджено функціонал захисту від примусу, наслідками цього стають використання складних алгоритмів підрахунку, обтяження користувачів необхідністю зберігати матеріал криптографічного ключа та перекладання відповідальності на них введення в оману своїх примушувачів. Причиною цього є те, що в умовах електронного голосування важко контролювати, чи примушують виборця голосувати проти його волі. Тому створення електронної системи голосування, яка могла б забезпечити стійкість до примусу, прозорість та надійний захист, є справжнім викликом для багатьох науковців та інженерів. Через це було запропоновано декілька методів, які спрямовані на вирішення цієї проблеми. Однак більшість із запропонованих методів залишаються в основному теоретичними. Метою даної статті є аналіз цих методів вирішення проблеми примусу, а також визначення рівня стійкості до примусу, який вони забезпечують.

Ключові слова: електронна демократія, електронне голосування, таємне електронне голосування у мережі Інтернет, стійкість до примусу в системах електронного голосування, довіра громадян до систем електронного голосування.

Вступ. Голосування грає важливу роль в побудові демократичного суспільства. Електронне голосування - це нова концепція онлайн-виборів, заснована на криптографії. Система підтримує повнофункціональне онлайн-голосування на будь-яких пристроях, а результати опитування будуть розраховуватися автоматично і анонімно. У порівнянні з традиційним голосуванням, електронне голосування - це більш економічна, прозоріша і неупереджена система.

Однією з основних вимог демократичних виборів є те, що виборець повинен мати можливість вільно висловлювати свої справжні уподобання, тобто без примусу. Можна виділити такі основні вимоги до голосування:

- Конфіденційність гарантує, що ніхто не може дізнатися, як голосував виборець.
- Безпримусовість гарантує, що виборець матиме можливість голосувати, відображаючи свої справжні уподобання, навіть якщо він знаходиться під наглядом примушувача протягом періоду голосування. Також безпримусовість означає що примушувач не зможе примусити виборця утримуватися від виборів або віддати невалідний голос, а також віддати валідний голос, якщо він отримає доступ до облікових даних виборця [1].
- Відсутність відображення результату голосування (квитанції) гарантує, що зловмисник не зможе отримати доказів результату голосу, що робить примус по суті неефективним.

Методи вирішення проблеми примусу. Багато факторів можуть мати вплив на загрозу примусу: тип виборів, властивості протоколу голосування, характеристики системи та середовища голосування, обізнаність виборців, можливості нападника тощо.

Як правило, протоколи голосування, спрямовані на певну форму опору примусу, повинні йти на компроміс між різними цілями. Нижче описано деякі протоколи голосування, стійкі до примусу, їх переваги та недоліки, зручність використання та застосування на практиці.

Метод фальшивих облікових даних. Протоколи JCJ та Civitas. Початком дослідження проблеми примусу в системах електронного голосування можна вважати 2002 рік випуском статті А. Джулза, Д. Каталано та М. Якобссона [2]. В цій статті вони дали визначення опору примусу та запропонували перше рішення, яке його задовольняло та пізніше стало відоме як протокол JCJ. Це рішення передбачає використання фальшивих облікових даних, які виборці можуть використовувати під примусом, але примушувач не зможе відрізнити від справжніх.

У 2008 році протокол JCJ був покращений М. Кларксоном, С. Чонгом та Е. Майерсом шляхом введення розподіленої децентралізованої моделі довіри і поліпшення продуктивності. Покращений протокол отримав назву Civitas [3].



Рисунок 1 – Архітектура протоколу Civitas

Ні один з цих двох протоколів не визначає, як саме виборцю слід обрати відповідні облікові дані. С. Нейманн і М. Волкамер відзначили у своїй статті 2012 року [4], що ця дія є нетривіальною та може призвести до проблем як у використанні, так і у безпеці, якщо вона буде реалізована недбало. Вони запропонували реалізацію Civitas на основі смарт-карт і зчитувачів з PIN-кодами. Вибір між фальшивими та справжніми обліковими даними буде здійснено шляхом введення в зчитувач справжнього або підробленого PIN-коду.

По суті, пропозиція Нейманна та Волкамера інкапсулює всі важливі операції на стороні виборців у спеціальне обладнання, якому потрібно довіряти. Хоча в принципі такий підхід може зробити обробку облікових даних більш безпечною, він насправді не наближає нас до практичної реалізації. В принципі, сучасні смарт-карти мають достатню продуктивність, необхідну для реалізації таких функцій. Однак продуктивність - не єдине вузьке місце в практичному застосуванні. Програмне забезпечення, що реалізує функціональність протоколу, має якось потрапити на картки.

Також в рамках процедури реєстрації протокол також залежить від наявності анонімних каналів. Як варіант, автори пропонують використовувати мережу Тог як анонімний канал зв'язку.

Ще один різновид протоколу JCJ розробили Р. Арауйо та співавт. у своїй праці [5] у 2010 р. Вони запровадили коротші облікові дані та формально доказали стійкість до примусу, хоча їхній доказ спирався на нестандартний теоретико-числовий метод. У 2018 році А. Нето та співавт. [6] провели дослідження зручності використання для системи CIVIS, що є реалізацією протоколу, запропонованого Арауйо та співавт. та показали, що більше 90% учасників тесту не розуміють як працює функціонал подання підроблених голосів. Крім того їм був

незрозумілий результат, чи їх поданий голос був справжнім чи підробленим. Це вводить під сумнів всю концепцію використання підроблених облікових даних.

Метод повторного голосування. Естонська система електронного голосування. Повторне голосування - це метод, який надає виборцю можливість змінити свій голос у разі, якщо його примусили під час перших спроб. Найбільш популярним прикладом системи, заснованої на повторному голосуванні, є естонська система голосування, де це єдиний застосований захід проти примусу [7].

Найбільша проблема такого методу є те, що виборець може бути під примусом до кінця періоду голосування для того, щоб особа, яка примушує виборця, запевнилась що не було повторного голосування. Щоб уникнути цієї загрози, Естонія вирішила припинити подання голосів через Інтернет за дві години до закриття виборчих дільниць в останній день періоду голосування. Обґрунтування полягає в тому, що якщо виборець під примусом, у нього ще є час, щоб подати свій голос на папері, і голосування на папері скасовує електронне голосування. Однак, якщо виборець проживає далеко від будь-якої виборчої дільниці, він не може проголосувати без примусу. Вся система діє за умови, що частка таких подій є незначною.

Крім того, функція повторного голосування може вплинути на цілісність голосування, оскільки зловмисник може використовувати його для перезапису попереднього голосування.

Перевагою даного підходу є те, що можливість повторного голосування не потребує додаткових налаштувань на стороні клієнта, а також що цей процес легко зрозуміти для пересічного виборця.

Метод перевірки права на голос. Група протоколів Helios. Перша версія протоколу Helios була описана в роботі Б. Адіди [8] та орієнтована на середовища з низькою вірогідністю примусу. У ході пізніших досліджень було розроблено кілька розширень, щоб посилити його опір примусу.

О. Кулик, В. Тігуе та В. Фолкамер розширили протокол Helios, щоб забезпечити приватну перевірку права на обрання, що означає що серед усіх поданих голосів до підрахунку включені лише голоси виборців, які мають право на голос, не показуючи, хто їх фактично подав [9]. Як побічний продукт, вони досягають відсутності отримання квитанції результату голосування в тому сенсі, що виборець не може довести, як він голосував, оскільки може непомітно переголосувати. Однак автори заявили, що протокол сприйнятливий до атаки рандомізації. Слідуючи ініціалам авторів, схема відома як KTV-Helios.

В оригінальній версії Helios виборці можуть представити випадковий рандомізований підпис голосу як квитанцію результату голосування для примушувача. Протокол BeleniosRF використовує повторно рандомізовані шифровані підписи, причому частина рандомізації відбувається на стороні серверу, який приймає голос, що не дає можливості виборцю надати будь яку квитанцію про результат голосування [10].

Широкі суспільно-правові дебати щодо конституційності повторного голосування відбувалися в Естонії, коли там було запроваджено голосування в Інтернеті. За кілька місяців до перших Інтернет виборів Президент Естонії подав до Верховного Суду положення про голосування в Інтернеті для перевірки конституційності повторного голосування, стверджуючи, що можливість зміни голосів в Інтернеті дає переваги Інтернет-виборцям у порівнянні з виборцями на папері. Рішення Верховного суду не підтримало цю точку зору, прийшовши до висновку, що просто технічна можливість подання повторних голосів не дає виборцям Інтернету жодної переваги [11].

Хоча результати подібної дискусії можуть бути різними, повторне голосування як простий у реалізації та відносно ефективний захід проти примусу є досить важливим для перегляду деяких законодавчих принципів.

Метод кільцевих підписів. Протокол Eos. С. Патачі та К. Шурманн запропонували протокол голосування Eos на основі умовно пов'язаних кільцевих підписів [12]. Всі виборці умовно зв'язуються між собою в кільце що дозволяє підписувати їх голоси анонімно. Eos використовує дві фази перемішування з метою розірвати зв'язок між виборцем і голосом,

роблячи майже неможливим для примушувача відстеження за голосом через таблицю результатів.

В Eos є дві основні заходи боротьби з примусом. По-перше, виборець може використовувати підсвідому підказку під час підготовки зашифрованого голосу. На практиці така підказка реалізується шляхом пред'явлення справжнього або псевдо-PIN-коду спеціальному апаратному пристрою для голосування або примушувачеві, який контролює цей пристрій.

По-друге, якщо активно примушуваний виборець проголосував, використовуючи дійсний PIN-код, він може пізніше проголосувати повторно, щоб оновити результати голосування. Однак в цьому випадку публічна дошка оголошень буде містити кілька зашифрованих голосів, відданих одним і тим же псевдоідентифікатором, який може бути відомий примушувачеві. В цьому випадку виборцю, можливо, доведеться збрехати примушувачеві, що він був останнім, хто віддав свій голос.

Протокол робить кілька нетривіальних припущень. По-перше, щоб позбутися від побічних каналів при передачі голосів, підписаних кільцево, необхідно використовувати анонімні канали, але на практиці це досить складно.

По-друге, для реалізації операцій на стороні клієнта будуть потрібні спеціальні апаратні токени. У статті пропонується використовувати в цій ролі апаратні гаманці, призначені для зберігання ключів криптовалют.



Рисунок 2 – Апаратний гаманець для криптовалют Trezor

Можливо, таке обладнання можна перепрограмувати, але поширення обладнання або закритих ключів серед виборців - завдання нетривіальне.

Оскільки вибір відбуватиметься шляхом введення реального або псевдо-PIN, ми також маємо всі звичайні проблеми управління псевдо-PIN. Якщо користувач введе неправильний PIN, пристрій не зможе дати ніякої зворотної зв'язки, і спокійно відправить голос, який виборець не збирався віддавати (наприклад, в сценарії, коли виборець хотів використовувати псевдо-PIN, але випадково використав справжній).

Метод “паролів паніки”. Протокол Selections. Дж. Кларк і У. Хенгартнер в 2008 році [13] запропонували особливу форму підроблених облікових даних, названих “паролями паніки”. Суть панічних паролів полягає в тому, що користувач може вибрати істинний пароль разом з набором альтернативних, які можуть бути використані для прихованого оповіщення системи про те, що користувач знаходиться в ненормальних обставин, наприклад, примус.

Останнє є важливим сценарієм загрози в разі віддаленого голосування, тому ті ж автори побудували схему голосування, стійку до примусу, під назвою Selections на основі своєї основної ідеї [14].

На жаль, змусити запам'ятовані людиною паролі працювати в якості підроблених облікових даних проблематично.

По-перше, необхідний складний процес реєстрації. Звичайно, він повинен відбуватися в контрольованому середовищі без примусу, але це стандартне припущення. У контрольованій реєстраційній кабінці все одно потрібно комп'ютер з доступом в Інтернет, щоб роздрукувати бюлетень виборця. Це передбачено в якості контрзаходу.

Єдиний спосіб, яким примушувач може домогтися цього, - обшукати речі виборця і пройти разом з ним до дверей реєстраційної кабінки.

У процесі реєстрації раніше обрані і зашифровані паролі паніки повторно рандомізують. Виборець вибирає один з повторно рандомізованих шифрів, який публікується в державному реєстрі. У протоколі передбачається, що виборець видаляє випадковість, використану для повторної рандомізації, і не записує її. Побудова властивостей безпеки на припущенні, що деяке значення буде видалено, завжди сумнівно. Можуть існувати побічні канали, якими примушувач змусить виборця користуватись для запису або передачі значення. Якщо примушувач брав участь в створенні бюлетеня виборця і має до нього доступ, то повторно зашифрований пароль паніки в публічному списку може бути зіставлений з зашифрованим словом паніки на бюлетені. Таким чином, випадковість дає можливість довести достовірність пароля, переданого примушувачеві.

Крім того, Selections страждає від типових проблем систем, заснованих на паролі. Ідея [14] полягає в тому, щоб пройти складний процес реєстрації один раз, а потім використовувати облікові дані протягом декількох заходів. Однак вибори, як правило, проходять лише раз в кілька років, і багато виборців, швидше за все, за цей час забудуть свої паролі, незалежно від того, наскільки хороший пароль використовується. Щоб вирішити цю проблему, люди зазвичай записують паролі, що збільшує ризик примусовості.

Висновки. Розробка протоколу електронного голосування, який відповідав би всім вимогам безпеки є досить складною задачею. З одного боку, хотілося б, щоб протокол був захищений від всіх атак, але за це доводиться платити підвищеною складністю технічної реалізації та користування цим протоколом.

У даній роботі розглядаються властивості стійкості до примусу різних протоколів голосування. В ході дослідження було описано п'ять методів вирішення проблеми примусу в електронному голосуванні, деякі з яких (наприклад можливість повторного голосування) достатньо прості в реалізації. У той же час, вимоги щодо організації анонімних каналів чи створення спеціалізованого обладнання легко записати на папері, але досить складно реалізувати.

Метод з використанням фальшивих облікових даних - один з найстаріших методів досягнення доведених властивостей стійкості до примусу, але деякі дослідження, як, наприклад, стаття А. Нето та співвавт. [6], показують, що для більшості користувачів даний метод викликає труднощі у розумінні як правильно користуватись цими обліковими даними. Це ставить під сумнів всю ідею використання підроблених облікових даних. В цілому, бракує досліджень зручності використання, які були б присвячені аспектам стійкості протоколів голосування до примусу.

ЛІТЕРАТУРА:

1. Juels, A., Catalano, D., Jakobsson, M. Coercion-resistant electronic elections. *Proceedings of WPES 2005*. ACM 2005. pp. 61–70.
2. Juels, A., Catalano, D., Jakobsson, M. Coercion-Resistant Electronic Elections. *Cryptology ePrint Archive, Report 2002/165* 2002. [Електронний ресурс]. Режим доступу: <https://eprint.iacr.org/2002/165>.
3. Clarkson, M.R., Chong, S., Myers, A.C. Civitas: Toward a Secure Voting System. *2008 IEEE Symposium on Security and Privacy (S&P 2008)*. IEEE Computer Society 2008. pp. 354–368.
4. Neumann, S., Volkamer, M. Civitas and the Real World: Problems and Solutions from a Practical Point of View. *ARES 2012*. IEEE 2012. pp. 180–185.
5. Araújo, R., Rajeb, N.B., Robbana, R., Traoré, J., Youssfi, S. Towards practical and secure coercion-resistant electronic elections. *CANS 2010, Proceedings. LNCS*. Springer 2010. vol. 6467. pp. 278–297.

6. Neto, A.S., Leite, M., Araújo, R., Mota, M.P., Neto, N.C.S., Traoré, J. Usability Considerations For Coercion-Resistant Election Systems. *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems*. IHC 2018. pp. 40:1– 40:10.
7. Madise, Ü., Martens, T. E-voting in Estonia 2005. The first Practice of Country - wide binding Internet Voting in the World. Krimmer, R. (ed.) *Electronic Voting 2006*. GI 2006. vol. 86, pp. 15–26.
8. Adida, B. Helios: Web-based Open-Audit Voting. *Proceedings of the 17th USENIX Security Symposium*. USENIX Association 2008. pp. 335–348.
9. Kulyk, O., Teague, V., Volkamer, M. Extending Helios Towards Private Eligibility Verifiability. *VoteID 2015, Proceedings. LNCS*. Springer 2015. vol. 9269. pp. 57–73.
10. Chaidos, P., Cortier, V., Fuchsbaauer, G., Galindo, D. BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme. *Proceedings of 2016 ACM CCS*. ACM, New York, NY, USA 2016. pp. 1614–1625.
11. Madise, Ü., Vinkel, P. Internet voting in Estonia: from constitutional debate to evaluation of experience over six elections. *Regulating eTechnologies in the European Union. Normative Realities and Trends*. Springer 2014. pp. 53–72.
12. Patachi, S., Schürmann, C. Eos a universal verifiable and coercion resistant voting protocol. *E-Vote-ID 2017, Proceedings. LNCS*. Springer 2017. vol. 10615. pp. 210–227.
13. Clark, J., Hengartner, U. Panic Passwords: Authenticating under Duress. HotSec'08, Proceedings. [Электронный ресурс] USENIX Association 2008. Режим доступа: http://www.usenix.org/events/hotsec08/tech/full_papers/clark/clark.pdf.
14. Clark, J., Hengartner, U. Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance. Danezis, G. (ed.) *FC 2011, Revised Selected Papers. LNCS*. Springer 2011. vol. 7035. pp. 47–61.

REFERENCES:

1. Juels, A., Catalano, D. and Jakobsson, M. (2005), “Coercion-resistant electronic elections”, *Proceedings of WPES 2005*, ACM, pp. 61–70.
2. Juels, A., Catalano, D. and Jakobsson, M. (2002), “Coercion-Resistant Electronic Elections”, *Cryptology ePrint Archive*, Report 2002/165, <https://eprint.iacr.org/2002/165> (accessed 23 October 2021).
3. Clarkson, M.R., Chong, S. and Myers, A.C. (2008), “Civitas: Toward a Secure Voting System”, 2008 IEEE Symposium on Security and Privacy (S&P 2008), IEEE Computer Society, pp. 354–368.
4. Neumann, S. and Volkamer, M. (2012), “Civitas and the Real World: Problems and Solutions from a Practical Point of View”, *ARES 2012*, IEEE, pp. 180–185.
5. Araújo, R., Rajeb, N.B., Robbana, R., Traoré, J. and Youssfi, S. (2010), “Towards practical and secure coercion-resistant electronic elections”, *CANS 2010, Proceedings. LNCS*, Springer, vol. 6467, pp. 278–297.
6. Neto, A.S., Leite, M., Araújo, R., Mota, M.P., Neto, N.C.S. and Traoré, J. (2018), “Usability Considerations For Coercion-Resistant Election Systems”, *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems*, IHC 2018, pp. 40:1– 40:10.
7. Madise, Ü. and Martens, T. (2006), “E-voting in Estonia 2005. The first Practice of Country - wide binding Internet Voting in the World”, Krimmer, R. (ed.) *Electronic Voting 2006*, GI, vol. 86, - pp. 15–26.
8. Adida, B (2008), “Helios: Web-based Open-Audit Voting”, *Proceedings of the 17th USENIX Security Symposium*, USENIX Association, pp. 335–348.
9. Kulyk, O., Teague, V. and Volkamer, M (2015), “Extending Helios Towards Private Eligibility Verifiability”, *VoteID 2015, Proceedings. LNCS*, Springer, vol. 9269, pp. 57–73.
10. Chaidos, P., Cortier, V., Fuchsbaauer, G. and Galindo, D. (2016), “BeleniosRF: A Non-Interactive Receipt-Free Electronic Voting Scheme”, *Proceedings of 2016 ACM CCS*, ACM, New York, NY, USA, pp. 1614–1625.
11. Madise, Ü. and Vinkel, P (2014), “Internet voting in Estonia: from constitutional debate to evaluation of experience over six elections”, *Regulating eTechnologies in the European Union. Normative Realities and Trends*, Springer, pp. 53–72.
12. Patachi, S. and Schürmann, C (2017), “Eos a universal verifiable and coercion resistant voting protocol”. *E-Vote-ID 2017, Proceedings. LNCS*, Springer, vol. 10615, pp. 210–227.
13. Clark, J. and Hengartner, U. (2008), “Panic Passwords: Authenticating under Duress”, *HotSec'08, Proceedings. USENIX Association*, http://www.usenix.org/events/hotsec08/tech/full_papers/clark/clark.pdf (accessed 23 October 2021).
14. Clark, J. and Hengartner, U. (2011), “Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance”, Danezis, G. (ed.) *FC 2011, Revised Selected Papers. LNCS*, Springer, vol. 7035, pp. 47–61.

In today's condition of rapidly evolving information technologies and increasing number of users of the Internet, building e-democracy is one of the key tasks to ensure the social and economic progress of society. One of the tools of e-democracy is electronic voting. Electronic voting has emerged as a replacement for paper voting, as this type of voting can be cost-effective, transparent and objective. However, the experience of using electronic voting in several countries over the past three decades shows that the implementation of such systems has not been very successful due to long-standing security and privacy shortcomings. One of the biggest problems with voting systems is the threat of coercion, that can force voters to change their will or abstain from voting against their will. And although many e-voting systems today have coercion protection, the consequences are the use of heavyweight counting algorithms, burdening users with the need to store cryptographic key material, and shifting responsibility to mislead their enforcers. The reason for this is that in the conditions of electronic voting it is difficult to control whether the voter is forced to vote against his will. Therefore, the creation of an electronic voting system, which could provide coercion resistance, transparency and reliable protection, is a real challenge for many scientists and engineers. Therefore, several methods have been proposed to solve this problem. However, most of the proposed methods remain largely theoretical. The purpose of this article is to analyze these methods of solving the problem of coercion, as well as to determine the level of resistance to coercion that they provide.

Keywords: *e-democracy, e-voting, secret e-voting on the Internet, coercion resistance in e-voting systems, citizens' trust in e-voting systems.*

