Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» травня 2024 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Система захищеного електронного голосування»

Виконавець: студент ІІ курсу, групи КБм-21

_____ **Євгеній ПОНОМАРЕНКО**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Іван ПАРХОМЕНКО	
Нормоконтроль	Лариса МИРУТЕНКО	

Київ 2024

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» листопада 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-21 (група) Пономаренко Євгенію Володимировичу (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Система захищеного електронного голосування

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 15.11.2023 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	процес електронного голосування
Предмет досліджень	система безпечного електронного голосування
Мета	розробка системи електронного голосування, яка здатна забезпечити анонімність голосів з одночасною підзвітністю виборчого процесу загалом
Вихідні дані для проведення роботи	дослідження математичних моделей, розроблених алгоритмів, процедур, процесів, програмних рішень, бібліотек, стандартів, та

інших компонент, які можуть стати частиною або значно вплинути на розроблену систему електронного голосування

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна удосконалено раніше розроблені процедури електронного голосування та розроблено систему з їх використанням

Практична цінність можливість впровадження даної системи в Україні

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	17.11.2023 – 28.01.2024
Аналіз літературних джерел	29.01.2024 – 11.02.2024
Ознайомлення з існуючими системами електронного голосування в інших країнах	12.02.2024 – 25.02.2024
Розгляд існуючого законодавства, нормативно-правових актів, та інших підзаконних актів у сфері виборчого права та проведення виборів	26.02.2024 – 03.03.2024
Дослідження загроз, вразливостей та атак, що спрямовуються на системи голосування	04.03.2024 – 17.03.2024
Аналіз вже існуючих рекомендацій стосовно уникнення можливих загроз	18.03.2024 – 24.03.2024
Дослідження методів та алгоритмів, необхідних для створення безпечної системи електронного голосування	25.03.2024 – 14.04.2024
Розробка самої системи безпечного електронного голосування для використання в Україні	15.04.2024 – 28.04.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	29.04.2024 – 12.05.2024
Подача пакету документів на розгляд ЕК	13.05.2024 – 18.05.2024

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект	Зменшення видатків на проведення державного голосування
Соціальний ефект	Підвищення виборчої явки шляхом полегшення можливості голосування; представники влади будуть представлені більшою частиною населення

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Іван ПАРХОМЕНКО
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Євгеній ПОНОМАРЕНКО
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 17.11.2023 р.
Термін подання кваліфікаційної роботи до ЕК 17.05.2024 р.

РЕФЕРАТ

Пояснювальна записка містить 76 сторінок, 4 рисунки, список використаних джерел з 58 найменуваннями.

Об’єкт дослідження: процес електронного голосування

Мета кваліфікаційної роботи: розробка системи електронного голосування.

Методи дослідження: методи наукової абстракції, індукції та дедукції, аналізу, синтезу, структурування, алгоритмізація.

В роботі проведено аналіз існуючих систем голосування, у тому числі електронного голосування, у різних країнах.

Розроблено систему безпечного електронного голосування в Україні.

Практичне значення роботи полягає у створенні та розробці системи електронного голосування в Україні.

Результати здійснених у дипломній роботі досліджень можуть бути використані для впровадження електронного голосування в Україні.

Напрямки подальших досліджень полягають у нівелюванні та нейтралізації знайдених загроз та слабких місць розробленої системи безпечного електронного голосування в Україні.

Цю роботу було апробовано у наступному виданні:

Ponomarenko Y., Parkhomenko I. Challenges faced by electronic voting systems. VII Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS). 2024. С. 57–59.

Ключові слова: криптографія, інформаційні технології, голосування, електронне голосування, виборчий процес, вибори, демократія, безпека виборчого процесу, безпека виборів.

ЗМІСТ

РОЗДІЛ 1
ДОСЛІДЖЕННЯ ІСНУЮЧИХ СИСТЕМ ТРАДИЦІЙНОГО ГОЛОСУВАННЯ

Взаємодія є невід’ємною складовою людського життя та існування. Без взаємодії одне з одним люди можуть покладатися на свої фізичні та розумові здібності, використовувати лише ресурси, якими вона володіє та які вона може контролювати, і впливати лише на процеси, події, і рішення, які є для неї підвладними. Люди мають різні здібності, хист, та можливості, а також вирішують вкладати свої ресурси, час, енергію, увагу на покращення та набуття різних навичок. Це призводить до нерівності в можливостях, які мають різні люди, що в свою чергу призводить до того, що більш здатні можуть негативно впливати на менш здатних. Через наявність елементів, які вважають прийнятним використовувати свої навички у спосіб, що шкодить іншим, і через здатність таких елементів повністю вивести з балансу та контролю систему що не має встановленого процесу контролю та регулювання, анархічні системи не можуть існувати в широких масштабах. В свою чергу це призводить до необхідності наявності визначеної системи контролю та менеджменту ресурсів, прав та обов’язків учасників системи. Іншими словами, суспільство потребує правління.

1.1. Дослідження актуальності питання

Суспільство — це об’єднання людей, яке має певні географічні кордони, спільну законодавчу систему і певну національну (соціокультурну) ідентичність [1]. Для організації процесів, які мають на меті надання переваг, сервісів, послуг, інфраструктури, та інших потреб, впровадження яких надасть користь суспільству як такому та більшості його членів зокрема, прямо чи опосередковано, існує необхідність впровадження певної форми правління.

Одна з форм правління, яка існувала історично, але наразі не існує на рівні розвинених країн, це феодалізм. В такій формі правління рішення приймаються

одноосібно правителем суспільства. Право правління передається шляхом спадкування, що унеможливлює будь-яке представництво народу і його інтересів. Недоліком такої системи є покладання обов’язків правління на людину, яка практично не відчуває наслідків свого правління і здатна допускати значні помилки безперешкодно. Єдиним винятком є публічна страта, що відбувалася у результаті накопичення гніву суспільства понад межу, при якій люди вважають прийнятним виконувати вказівки влади. Це було невеликим, тому не надто дієвим важелем впливу суспільства над володарями влади, того такі системи у сучасному світі вважаються неприйнятними. За аналогією, авторитаризм, тоталітаризм, монархія, імперіалізм, та інші форми правління пов’язані з тими самими проблемами і через це мають схожі недоліки.

Іншою системою правління є демократія. Згідно [2, с. 227], демократія — це політичний режим, за якого єдиним легітимним джерелом влади у державі визнається її народ. Якщо правління народу відбувається прямо і рішення приймаються учасниками системи особисто, така система вважається прямою демократію. У разі, якщо рішення приймаються учасниками системи опосередковано, за участі осіб, які їх представляють, то таку систему називають непрямою або представницькою демократією.

1.2. Пряма демократія

Пряма демократія є непоганим рішенням для невеликих систем. Оскільки всі учасники системи можуть впливати на кожне рішення, і їх прийняття вимагає підтримку більшості, допоки більшість суспільства здатна приймати рішення в своїх інтересах, ця система здатна працювати. Але існує велика кількість проблем, які стають тільки гірше з набуттям кожного нового члена системи:

— Збільшення кількості осіб в системі збільшує час на підрахунок голосів, підвищує складність процесу підрахунку голосів, збільшує вірогідність помилки у разі використання ручних систем підрахунку, що загалом сповільнює систему та вимагає більше ресурсів (у тому числі грошових) для проведення голосування.

— У випадку, якщо присутність члена не є вимогою і рішення може бути прийняте більшістю виключно присутніх членів системи, існує ризик прийняття рішень виключно зацікавленою частиною суспільства.

— Різні люди мають різний ступінь зацікавленості в політичному процесі та різну кількість ресурсів (матеріальних, психологічних, розумових, тощо) які вони здатні вкладати в цю систему. Чим більше людей необхідно для прийняття рішення, тим більше людського ресурсу системи необхідно витрачати на ознайомлення зі специфікою проблеми, і тим більшою є вірогідність того, що учасники системи відмовляться витрачати цей ресурс і приймуть рішення без розуміння усіх його наслідків, що здатне призвести до негативних наслідків.

Для ефективного функціонування такої системи, її учасники фактично вимушені занурюватися в тонкощі кожного питання. Зі зростом кількості учасників, кількість питань, які потребують загального обговорення та рішення, також зростає, але при цьому зростає і кількість питань, які не стосуються напряму або не цікавлять кожного конкретно заданого учасника системи. Фактично, ефективність системи обмежується швидкістю найповільнішого учасника системи, якість рішень якого задовольняє мінімальний поріг творцями такої системи. Через це такі системи не можуть ефективно масштабуватися понад певний людський поріг. Для управління десятками, сотнями тисяч, або навіть мільйонами людей, постає необхідність використання непрямої (представницької) демократії.

1.3. Поняття голосування

Голосування — процес ухвалення рішення групою людей (зборами, електоратом), при якому загальна думка формується шляхом підрахунку голосів членів групи [3, с. 152]. В прямій демократії групою людей, яка формує загальну думку, згідно якій ухвалюються рішення, є всі члени суспільства. В представницькій демократії такою групою є обрані представники, які репрезентують суспільство опосередковано. Рішення одного обраного представника здатне репрезентувати інтереси десятків, сотень тисяч, або навіть мільйонів людей.

1.4. Представницька демократія

Представницька демократія вирішує багато проблем прямої демократії, але також має свій набір недоліків та проблем які потребують вирішення.

Важливим аспектом непрямої демократії є те, що, простіше кажучи, замість того, щоб усі люди в суспільстві приймали всі рішення щодо цього суспільства, люди делегують право приймати ці рішення тим, хто займає певні ролі чи посади. Потім люди погоджуються надати особі, яка обіймає або бере на себе цю роль або посаду, повноваження приймати рішення та керувати людьми в межах визначених обов'язків. У більшості випадків владні посади можна обіймати лише протягом певного періоду часу, і вибори визначають, чи та сама особа продовжує працювати на посаді. Зазвичай інтерес людини при владі полягає в тому, щоб залишатися при владі до тих пір, поки це дозволяють правила і закони суспільства. Іншими словами, щоб утриматися при владі, їм потрібно постійно заспокоювати населення, щоб їх не замінили.

Переваги представницької демократії включають в себе:

— Обрані представники влади отримують заробітну платню та підтримку суспільства, що здатне виключити потребу обранців відволікатися від своєї основної функції — прийняття рішень — і не витрачати час на іншу роботу або бізнес.

— Обранці здатні приділяти більше часу і ресурсів на аналіз проблеми та прийняття рішень, а також мають доступ до кращої інформаційної та ресурсної бази, здатні використовувати державні механізми та інститути для підвищення ефективності збору даних та аналізу можливих наслідків прийняття рішень.

— Концентрація відповідальності звільняє тих, кого представляє обрана особа, від необхідності самостійно аналізувати та приймати державні рішення, що підвищує ефективність електорату в інших сферах їхнього життя та дозволяє їм приділяти більше часу на власні потреби без значної втрати політичного впливу або свідомості.

З недоліків представницької демократії в порівнянні з прямою можливо виділити наступні пункти:

— У випадку обрання корумпованих, некомпетентних представників, або таких, що не представляють інтереси тих, що обрали дану людину на представницький пост, негативні наслідки такого рішення на порядки перевищують негативні наслідки поганого впливу однієї людини в прямій демократії. В найгірших випадках достатньо всього декількох несправних елементів для того, аби кардинально вплинути на усю законодавчу систему загалом.

— Оскільки представники обираються всенародним голосуванням, у разі низької свідомості електорату, представники можуть обиратися не за принципом компетентності, а за принципом популізму, популярності, та порожніх обіцянок. В такій системі існує великий ризик того, що перемагають не найбільш здатні правити, а найбільш здатні продати себе публіці як людина, яка здатна правити.

— Попередня проблема посилюється тим, що суспільну думку формує публічне медіа, яке в капіталістичній системі може мати редакційний вплив ззовні шляхом підкупу. Таким чином, деякі політичні представники здатні де-факто "купити" свій шлях в політичну кар’єру. Ті, що схильні використовувати цей шлях та мають достатню кількість грошей для політичної реклами зазвичай не схильні до прийняття рішень в інтересах спільноти, яка обрала такого кандидата, або суспільства в цілому.

— Оскільки представники влади обираються на обмежений строк, великі за обсягом та часом політичні, економічні, соціальні, та інші всенародні програми, які мають на меті довгострокові вкладення задля довгострокових результатів, стикаються з проблемою того, що такі програми можуть бути відкликані новою владою, яка проти використання суспільних ресурсів в таких цілях. Оскільки інтереси обранців бути переобраними заради продовження своєї політичної кар’єри можуть суперечити довгостроковим інтересам суспільства, необхідно створення окремих агенцій, які будуть управляти подібними довгостроковими проєктами, з частковою ізоляцією таких агенцій від швидкоплинних змін тієї чи іншої ітерації влади.

— Як було зазначено вище, інтереси можновладців не завжди співпадають з інтересами суспільства. По-перше, можновладці мають свої власні персональні інтереси (наприклад, прибутку, ідеології, тощо), яким вони можуть бути здатні надати перевагу в порівнянні з інтересами суспільства. Оскільки обрані представники влади мають можливість використовувати свою владу як завгодно, спокуса зловмисного її використання завжди існуватиме серед обранців. По-друге, оскільки людям власно придавати більшого значення нещодавнім подіям в порівнянні з історичними подіями, можновладці часто використовують тактику відкладання суспільно популярних рішень до початку виборчої кампанії, аби пам’ять про такі рішення була більш свіжою в головах виборців.

Нинішня система непрямої демократії працює через процес, який називається виборами. Зазвичай вибори складаються з наступних процесів. Встановлюється певний часовий проміжок (зазвичай один день, але може бути довшим), і люди збираються у визначеному місці, щоб проголосувати за одного з багатьох кандидатів. Особа може віддати лише один голос (це також має місце в передостанніх системах голосування, навіть якщо бюлетень містить голоси за кількох кандидатів). Коли вони прибувають на виборчу дільницю, вони повинні бути зареєстровані для голосування, і держава повинна переконатися, що ця особа не має права голосу. Оскільки ті, хто виконує свої обов’язки від імені держави, також є людьми зі своїми власними планами та інтересами, важливо, щоб за виборами спостерігали люди з різними політичними поглядами та економічним, соціальним та іншим походженням, щоб забезпечити відсутність широкого та систематичного впливу, який міг би спотворити результати виборів від справжнього волевиявлення народу. Це важливо. Усі голоси підраховуються та перевіряються після їх подачі. Результати голосування перевіряються, збираються в центральному місці, узагальнюються та стають доступними для всіх.

Головний виклик будь-якої виборчої системи полягає в тому, що вона має задовольняти дві, здавалося б, суперечливі потреби: анонімність голосування та підзвітність усього процесу. Анонімність голосування важлива для запобігання дискримінації людей на основі того, як вони голосують, таким чином дозволяючи

людям голосувати за те, що, на їхню думку, найкраще відображає їхні політичні уподобання. Підзвітність у процесі голосування є важливою, оскільки для того, щоб люди могли прийняти результат виборів у цілому, особливо якщо цей результат не є репрезентативним для рішень, які вони ухвалили під час процесу, вони повинні вірити, що голосування є чесним, що кожен має справедливий шанс бути представленим, і ніхто не може суттєво вплинути на результат, отримати несправедливу перевагу, або що їхні голоси не перевищують голоси інших. Їм також потрібно вірити, що їхній голос віддано серед інших, а не для задоволення чиїхось політичних потреб. Зрештою, люди ніколи не бачать підрахунку чи відкидання своїх голосів після того, як вони їх віддали. Спостерігачі та резервні копії необхідні, щоб люди відчували впевненість, що їхні голоси чують, незважаючи на відсутність особистих доказів.

1.5. Важливість голосування

Згідно з опитуванням, в якому респондентів просили дати визначення демократії, більшість обрали "голосування" та "вибори" [4]. Однак для того, щоб вибори відображали погляди і прагнення народу та здійснювали владу через народ, виборчий процес має бути не лише чесним і неупередженим, але й таким, який народ вважає чесним і неупередженим. Це вимагає, щоб чесність виборчого процесу могла бути перевірена громадськістю, і в той же час, щоб громадськість не могла втручатися або неналежним чином впливати на виборчий процес.

Електронне голосування — це процес волевиявлення виборців за допомогою електронних засобів, а також автоматична перевірка та підрахунок голосів за допомогою електронного обладнання та програмного забезпечення.

Використання електронного голосування як способу волевиявлення громадян вже має прецеденти у світі [5]. В Україні також є спроби впровадити системи електронного голосування в законотворчий та законодавчий процеси [5; 6].

Управління — це процес прийняття та реалізації рішень в організації чи суспільстві [7]. Кожна країна, як форма суспільства, має свою форму правління. Існують різні способи, якими суспільства досягають певної форми правління.

Протягом більшої частини історії монархізм, феодалізм, авторитаризм і тоталітаризм практикували ті, хто мав владу, багатство, військову могутність і політичний вплив. Однак за останні кілька століть більшість країн світу прийняли демократичні форми правління.

Демократія існувала в тій чи іншій формі протягом тисячоліть [8]. Тому існують різні способи існування демократії в житті суспільства. Одним із них є пряма демократія, коли всі члени суспільства (села, міста, країни тощо) можуть безпосередньо брати участь і голосувати з будь-якого питання, яке виноситься на обговорення (і зрештою на голосування).

Однак спроба впровадження цієї системи стає складнішою, оскільки кількість людей збільшується. Незалежно від того, чи йдеться про підрахунок кількості піднятих рук, чи збирання та підрахунок папірців (чи інших жетонів) для визначення позиції більшості спільноти в цілому, централізоване виконання цього стає непереборним тягарем із збільшенням масштабу. Мало того, що кількість людей збільшується, то чим більше міст, регіонів і різних суб-спільнот, тим більше проблем вони створюють і тим більше є речей, за які можна голосувати. Таким чином, кожен член суспільства повинен взяти на себе більше психічного тягаря, щоб ефективно вирішувати проблеми, що виникають.

Це означає, що з точки зору розумових і психологічних ресурсів, існує обмеження на кількість людей, які можуть брати участь у прямій демократії. Крім цього, збирання та підрахунок усіх голосів займе надто багато часу, а самі люди, які мають бути в одному місці, щоб брати участь у процесі прийняття рішень, займуть занадто багато місця. Оскільки демократія залежить від добре поінформованого електорату, перевантажуючи кожного окремого представника в демократичному процесі, ми досягаємо протилежного. Тому майже в усіх громадах такого розміру, де пряма демократія зжила себе, її місце займає непряма демократія.

1.6. Складові голосування як такого

Для того, щоб розробити безпечні методи голосування, спочатку необхідно визначити критерії, яким ці методи повинні відповідати, а також специфічні

властивості, якими повинен володіти процес голосування, щоб вважатися безпечним і надійним.

Метою цієї роботи є створення методу голосування, який відповідає наступним вимогам:

— прозорість;

— облік;

— таємність;

— звітність.

Прозорість — зацікавлені сторони можуть незалежно перевірити чесність і точність процесу. Усі виборці повинні мати можливість відстежувати джерело голосів, автентичність бюлетенів та виборців, чи були бюлетені заповнені, точність та автентичність коду, що виконується на обладнанні (або, принаймні, точність результатів цього коду), а також всі інші аспекти процесу голосування.

Облік — кожен голос має бути підрахований. Процес голосування повинен включати механізми, які доводять, що всі голоси були успішно отримані та підраховані, що голоси були втрачені або що були додані фальсифіковані голоси.

Таємність — голос виборця не повинен бути нікому розголошений і що ніхто, окрім цього громадянина, не повинен мати змоги ідентифікувати голос, відданий цим громадянином.

Крім того, як і будь-яка інша апаратна або програмна система, система електронного голосування повинна гарантувати конфіденційність, цілісність і доступність інформації.

Висновок по розділу 1

Дослідження традиційних виборчих систем показує, що існує потреба в певній формі системи управління та контролю над ресурсами, правами та обов'язками учасників суспільства. Історична форма правління, феодалізм, не могла представляти інтереси народу, і сучасні суспільства в основному прийняли демократичні форми правління. Пряма демократія добре працює для невеликих інституцій, але зі збільшенням кількості виборців вона стикається з низкою труднощів, таких як

збільшення часу і складність підрахунку голосів, небезпека прийняття корисливих рішень зацікавленими частинами суспільства, а також тягар інформування громадян з усіх питань. Представницька демократія вирішує багато з цих проблем, але має свої недоліки та виклики, які потребують вирішення. Концепція голосування є центральною як для прямої, так і для представницької демократії, де групи формують консенсус шляхом підрахунку індивідуальних голосів. Використання електронних систем голосування може підвищити ефективність і точність процесу голосування, але для того, щоб ці системи вважалися безпечними та надійними, вкрай важливо, щоб вони відповідали певним критеріям, таким як прозорість, підзвітність, конфіденційність і надійність. Завдання будь-якої системи голосування полягає в тому, щоб збалансувати потребу в анонімності під час голосування з підзвітністю впродовж усього процесу.

РОЗДІЛ 2
ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ПРОБЛЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

2.1. Огляд поняття електронного голосування

Згідно з [6], «електронне голосування — голосування з будь-якого публічного питання, зокрема участь в опитуваннях, виборах, референдумах, що передбачає використання електронних засобів для ідентифікації та підрахунку голосів.». Крім того, за даними [6], більшість українців (71% опитаних) зацікавлені в діалозі з представниками влади.

Електронне голосування є дуже популярною темою для багатьох українців, але впровадження ефективної системи електронного голосування вимагає необхідних заходів безпеки. Низький рівень розвитку інформаційної інфраструктури та неналежні стандарти обробки та зберігання інформації, а також такі питання, як безпека процесу, запобігання фальсифікаціям, подвійному підрахунку голосів, підзвітність та відстежуваність голосів, забезпечення конфіденційності голосів громадян — це проблеми, які необхідно вирішити до запровадження електронного голосування в Україні. У цій роботі пропонується система електронного голосування, яка може бути адаптована та впроваджена в Україні, що забезпечить надійне волевиявлення без втрати таємниці голосування.

2.2. Аналіз вже створених рішень в інших країнах

2.2.1. Досвід електронного голосування Швейцарії

З 2005 року у швейцарському кантоні Невшатель технологія інтернет-голосування використовується щороку для численних електронних консультацій, обов'язкових виборчих процедур та референдумів.

У червні 2008 року федеральний уряд Швейцарії вперше обрав інтернет-голосування як метод голосування, доступний для громадян Швейцарії, що проживають за кордоном.

Кантон Невшатель перейшов на останню версію інформаційної системи інтернет-голосування в 2011 році, коли портал електронного уряду був модернізований і отримав нові та оновлені функції.

Нові протоколи були розроблені та інтегровані в портал електронного урядування Невшателя в 2014 році. Цей інноваційний підхід базується на новому поколінні протоколів електронного голосування, які забезпечують не лише наскрізне шифрування, але й особисту автентифікацію за допомогою вдосконалених криптографічних алгоритмів, заснованих на системах індивідуальних кодів повернення виборців.

Референдуми та вибори зазвичай проводяться щоквартально, причому федеральні, штатні та муніципальні вибори відрізняються за роками. Інтернет-голосування зазвичай відбувається за 15-30 днів до проведення виборів на паперових носіях, і голосувати можна протягом усього виборчого періоду. У деяких випадках понад 60 відсотків усіх голосів віддається в електронному вигляді.

2.2.2. Система електронного голосування в США

В США для електронного голосування використовуються різні електронні системи та машини. До них відносяться сенсорні екрани, які дозволяють виборцям вказувати свій вибір, сканери для читання паперових бюлетенів, сканери для перевірки підписів на конвертах для відкріпних бюлетенів і веб-сервери для публічного відображення підрахунку голосів [9]. Крім того, комп’ютерні системи використовуються для керування реєстрацією виборців та надання списків виборців персоналу виборчих дільниць. Враховуючи, що більшість виборчих офісів мають справу з тисячами бюлетенів, машинний підрахунок виявляється більш ефективним і рентабельним, ніж ручний.

Комісія зі сприяння виборам (Election Assistance Commission, EAC), незалежна агенція уряду США, створила Рекомендації щодо системи добровільного голосування

(VVSG) 2005 року [10]. Ці рекомендації спрямовані на вирішення деяких вимог щодо безпеки та доступності виборів. EAC також акредитує три випробувальні лабораторії, які виробники наймають для оцінки свого обладнання. На основі звітів цих лабораторій EAC визначає, чи відповідає обладнання для голосування добровільним вимогам, сертифікуючи його відповідно.

Вимоги до використання машини відрізняються в різних штатах. Дванадцять штатів вимагають сертифікації EAC для машин; 17 штатів вимагають тестування в лабораторії, що є акредитованою EAC, але не сертифікацію. Дев’ять штатів і Вашингтон вимагають тестування за федеральними стандартами, незалежно від лабораторії. Ще чотири штати розглядають федеральні стандарти, але приймають незалежні рішення, а решта вісім штатів взагалі не посилаються на федеральні стандарти [9].

Оновлений набір інструкцій, VVSG 1.1, був розроблений у 2009 році та затверджений у 2015 році. Виробники машин для голосування мають можливість дотримуватися оригінальних або оновлених інструкцій. Наразі нова версія VVSG 2.0 або VVSG Next Iteration знаходиться на стадії оцінки [10].

В оптичних системах голосування виборці вказують свій вибір на одному або кількох аркушах паперу, які потім проходять через сканер. Сканер створює електронне зображення кожного виборчого бюлетеня, інтерпретує його для створення підрахунку для кожного кандидата та, зазвичай, зберігає зображення для подальшого перегляду.

Виборці проставляють помітки безпосередньо на аркушах паперу у спеціально відведеному для кожного кандидата місці, а потім надсилають його поштою або залишають у виборчій скриньці.

Інший варіант передбачає використання машин з сенсорним екраном для того, аби громадянин міг обрати конкретного кандидата, та друк вибраного імені на папері, часто зі штрих-кодом або QR-кодом, що містить усі варіанти. Цей екран і принтер, відомий як пристрій для маркування бюлетенів (BMD), особливо корисний для виборців з обмеженими можливостями, оскільки вони можуть взаємодіяти з ним за допомогою навушників, великих кнопок, затяжок, або маніпуляторів, якщо вони не

може безпосередньо керувати екраном або папером [11]. Обладнання для підрахунку голосів зазвичай не зберігає та не підраховує голоси. Натомість офіційний бюлетень — це роздрукований аркуш паперу зі штрих-кодами, який вставляється в систему сканування, яка в свою чергу підраховує ці штрих-коди.

Більшість виборців не перевіряють надрукований машиною папір, щоб переконатися, що їхні вподобання точно відображені. Згідно [12], 81% зареєстрованих виборців не повідомляють працівникам дільниці про помилки, якщо вони їх допускають. Жоден штат не вимагає централізованого звітування про помилки, про які повідомляють виборці, тому спорадичні звіти не призводять до виправлення програмного забезпечення. Хоча виборці легше впізнають паперові бюлетені з ручними позначками, деякі з них дозволяють використовувати коригуючу рідину або стрічку, що дозволяє замінити бюлетені пізніше.

Дві компанії, Hart і Clear Ballot, пропонують сканери, які підраховують надруковані імена, які виборці можуть перевірити, на відміну від штрих-кодів або QR-кодів, які виборці не можуть перевірити [13]. Коли сканери використовують штрих-коди або QR-коди, кандидат представляється у вигляді числа на коді, і сканер підраховує цей код замість імені. Якщо через помилку або атаку система нумерації пристрою для маркування бюлетенів відрізняється від системи нумерації сканера, голоси за неправильного кандидата можуть бути зараховані. Ця розбіжність у нумерації також може виникнути з електронними машинами прямого запису [13].

Відтворені бюлетені — це паперові або електронні бюлетені, які виготовляються працівниками виборчих комісій, коли оригінал бюлетеня не може бути підрахований з різних причин, наприклад: розриви; пошкодження від води; згини, які не проходять через сканер; виборці обводять кандидатів або роблять на них інші незвичні позначки; а також іноземні громадяни, які використовують федеральні відкріпні посвідчення після того, як не отримали вчасно свої звичайні бюлетені. Під час виборчого процесу до 8% бюлетенів можуть бути відтвореними.

Під час аудиту виборчого процесу перевіряються оригінальні бюлетені, а не дублікати, щоб виявити помилки в процесі дублювання.

Вартість систем сканування варіюється в залежності від методу, що використовується. Якщо більшість виборців самостійно ставлять позначки на своїх паперових бюлетенях, а на кожній виборчій дільниці встановлено маркувальний пристрій для виборців з інвалідністю, загальна вартість обладнання та обслуговування в штаті Джорджія за 10 років, починаючи з 2020 року, оцінюється в 12 доларів США на одного виборця (загалом 84 мільйони доларів США). Вартість попередньо надрукованих бюлетенів з відмітками для виборців становить від 4 до 20 доларів США на одного виборця (загалом 113-224 мільйони доларів США на обладнання, технічне обслуговування та друк). Мінімальні оцінки свідчать про суму 0,40 доларів США на друк одного бюлетеня та достатню кількість бюлетенів для минулих рівнів явки. Згідно максимальних оцінок, 0,55 доларів США за один бюлетень і достатню кількість бюлетенів на одного зареєстрованого виборця, а також три бюлетені (від різних партій) на одного зареєстрованого виборця в історично низькоактивних виборчих округах. Якби всі виборці проголосували, витрати становили б 29 доларів США на одного виборця (загалом 203 мільйони доларів США).

У Пенсильванії, якщо більшість виборців ставлять позначки на своїх паперових бюлетенях, а на кожній виборчій дільниці є пристрій для маркування бюлетенів для виборців з інвалідністю, капітальні витрати на обладнання у 2019 році становлять 11 доларів США на одного виборця, порівняно з 23 доларами США, якщо всі виборці будуть використовувати пристрої для маркування бюлетенів Вартість обладнання для маркування бюлетенів становить 23 долари США, якщо всі виборці будуть використовувати пристрої для маркування бюлетенів. Ця вартість не включає витрати на друк бюлетенів.

Дослідження (неопубліковане), яке порівнює капітальні витрати в Нью-Йорку, показує, що система, де всі виборці використовують обладнання для підрахунку голосів, коштує вдвічі дорожче, ніж система, де більшість виборців його не використовує. Автори стверджують, що додаткове технічне обслуговування машин збільшує цю різницю і що витрати на друк будуть однаковими за обох підходів. Однак це припущення відрізняється від оцінки штату Джорджія: $0,40 або $0,50 за

бюлетень. 0,40 або 0,50 доларів США за попередній друк бюлетенів і 0,10 доларів США за маркерний друк. 0,40 або 0,50 доларів США за попередній друк бюлетенів і 0,10 доларів США за маркерний друк.

2.2.3. Основні принципи електронного голосування Естонії

Естонія стала першою країною, яка створила систему електронного голосування через Інтернет. Перше онлайн-голосування відбулося у 2005 році.

З принципів електронного голосування в Естонії можна виділити наступні:

1. Голосування в Інтернеті є добровільним.

Електронне голосування є необов'язковим для всіх громадян Естонії; вся виборча система базується на паперових бюлетенях. Інтернет-голосування — це лише інший спосіб надати виборцям право голосу і не має на меті замінити традиційне голосування на виборчих дільницях.

2. Можливе дострокове голосування.

Інтернет-голосування є одним з трьох способів, за допомогою яких громадяни Естонії можуть проголосувати заздалегідь. Крім того, виборці можуть проголосувати поштою або на уповноваженій виборчій дільниці до дня виборів. Однак 33% виборців віддали перевагу голосуванню через Інтернет, голосуючи до дня виборів, таким чином усуваючи попит на голосування поштою.

3. Голосування з декількома варіантами вибору.

Виборці можуть віддати стільки голосів, скільки забажають. Кожен голос підписується цифровим підписом і має електронну позначку часу, так що зараховується лише останній поданий голос. Виборці також можуть проголосувати особисто на виборчій дільниці в день виборів, і в цьому випадку всі раніше подані голоси анулюються.

4. Переваги паперових виборчих бюлетенів.

Голоси, віддані особисто, завжди мають пріоритет над голосами, відданими онлайн. Як наслідок, всі обміняні електронні голоси можуть бути легко анульовані в день виборів шляхом голосування від руки, що зводить нанівець саму мету обміну голосами.

5. Шахраї стикаються з серйозними наслідками.

Виборці, викриті у продажу своїх голосів, стикаються з суворими покараннями, у тому числі позбавлення волі.

Наступне голосування в Естонії буде проведено в період з 3 по 9 червня 2024 року.

Для того, аби голосувати дистанційно, в Естонії використовуються спеціальні системи зчитування даних з електронних носіїв, якими слугують їх національні паспорти.

2.2.4. Аналіз виборчого процесу в Австралії

В Виборча комісія Нового Південного Уельсу відповідає за адміністрування загальнодержавних виборів, виборів до органів місцевого самоврядування та деяких корпоративних виборів у Новому Південному Уельсі, Австралія. Існуюча система iVote була модернізована у 2014 році, щоб дозволити голосування через Інтернет та телефон.

Голосування за допомогою iVote дозволено під час передвиборчого періоду та в день виборів, і користувачі повинні попередньо зареєструватися, щоб користуватися системою; реєстрація відкривається за місяць до початку передвиборчого періоду.

У 2015 році значна кількість виборців скористалася системою iVote, і було віддано понад 280 000 голосів. Система також доступна для людей з вадами зору, які проживають за межами держави або живуть на відстані понад 20 км від виборчої дільниці. Використання системи зросло на 500 відсотків з моменту її запуску в 2011 році.

Система iVote Виборчої комісії Нового Південного Уельсу — це веб-система для голосування, яка також дозволяє голосувати по телефону за допомогою системи IVR (інтерактивної голосової відповіді).

2.3. Аналіз процесу голосування в Україні

Український виборчий процес має наступні механізми забезпечення безпеки та прозорості процесу голосування:

— наявність списків виборців;

— облік та видача виборчих бюлетенів;

— організація роботи персоналу виборчих дільниць;

— участь незалежних громадських спостерігачів;

— забезпечення прав виборців, які не можуть пересуватися самостійно;

— відбір виборчих бюлетенів та визнання їх недійсними;

— створення протоколу підрахунку голосів.

Розглянемо кожен з цих механізмів та оцінимо, як вони забезпечують безпеку та прозорість процесу голосування:

Існування реєстру виборців запобігає можливості подвійного голосування, оскільки виборці розподіляються по виборчих округах відповідно до зареєстрованого місця проживання.

Облік та розподіл виборчих бюлетенів дозволяє контролювати їх походження та використання, порівнювати кількість виданих бюлетенів з кількістю підрахованих голосів, а також відстежувати можливі порушення, пов'язані з використанням незаповнених бюлетенів з метою впливу на результати голосування на виборчій дільниці.

Персонал виборчих дільниць повинен бути обраний у прозорий спосіб за участю громадськості. На кожній виборчій дільниці представники всіх політичних партій повинні мати можливість спостерігати за процесом голосування та підрахунку голосів.

Незалежні спостерігачі від громадськості повинні мати можливість контролювати виборчий процес на виборчих дільницях, щоб уникнути ситуації, коли всі інші посадові особи (в тому числі ті, що належать до більш ніж однієї політичної партії) співпрацюють, а спостерігати і контролювати це нікому. У той же час,

незалежні спостерігачі не повинні мати можливості втручатися у виборчий процес і впливати на результати виборів.

Деякі виборці не можуть прийти на виборчу дільницю через проблеми зі здоров'ям, але мають законне право голосувати. Система повинна забезпечити їм можливість проголосувати. Наразі це робиться за допомогою мобільних виборчих дільниць, укомплектованих кількома людьми, які спостерігають за процесом голосування та перевіряють його чесність.

Деякі бюлетені заповнені неправильно, мають позначки або написи, які можуть ідентифікувати виборця, малюнки або написи з новими "кандидатами", яких немає в офіційному списку, або залишаються повністю порожніми. Для того, щоб забезпечити чесне голосування, бюлетені повинні перевірятися на точність під час підрахунку голосів.

Наприкінці процесу підрахунку голосів слід підготувати письмову процедуру для кожної виборчої дільниці та для країни в цілому, в якій повідомляється про статус кожного голосу, хто отримав скільки голосів тощо.

2.4. Проблеми цифрового голосування в умовах непрямої демократії

Цифрове голосування стосується тих самих проблем, що й аналогове «паперове» голосування. Необхідно захистити анонімність окремих виборців і забезпечити, щоб ніхто не міг пов’язати голосування з окремою особою. Але також необхідно переконатися, що кожен знає, що його голосування зареєстровано, що ніхто не може голосувати двічі, що лише ті, хто має законні права, можуть голосувати, і що кожен має рівний доступ до бюлетеня.

Але ми також стикаємося з новими викликами. Ключовою гарантією традиційних паперових бюлетенів є те, що вони розповсюджуються на тисячі окремих виборчих дільниць. Така система практично гарантує, що масштабне шахрайство виборців залишиться непоміченим. Проте, щоб мати суттєвий вплив на загальний результат виборів, шахрайство виборців має відбуватися на десятках, сотнях або тисячах різних виборчих дільниць по всій країні та потребує співпраці незліченної кількості людей, які контролюють виборчий процес і забезпечують його

справедливість і прозорість. Для десятків тисяч людей практично неможливо зберегти таємницю та перешкодити вільному та чесному виборчому процесу. Ця стійкість до широкомасштабних атак і шахрайства є причиною традиційного голосування таким, яким воно є сьогодні.

2.5. Можливі рішення для систем онлайн-цифрового голосування

Простим вирішенням проблеми відстеження голосів кожного було б зробити всі голоси публічними. Хоча це, безсумнівно, спрацювало б (зрештою, кожен міг би побачити, як їхні голоси підраховуються в загальному підрахунку), це абсолютно не змогло б зберегти анонімність голосів. Крім того, партійна приналежність людини була б не тільки загальнодоступною, але й видимою для всіх в Інтернеті з моменту її публікації, майже безкінечно. Це неприпустимо у випадку, якщо ми хочемо захистити права і свободи громадян.

Звичайно, деякі існуючі сьогодні системи не використовують такий підхід, щоб уникнути порушень анонімності. Відповідно до глави 6 книги «Електронне голосування в реальному світі: проектування, аналіз і розгортання» Фенг Хао, Пітера Й. А. Райана [14, С. 129-141], електронне голосування в Естонії надає перевагу простоті, а не абсолютній перевіреності та анонімності. Виборці спочатку шифрують свій голос відкритим ключем виборів за допомогою інфраструктури відкритих ключів, а потім підписують його за допомогою цифрового підпису, виданого урядом, пов’язаного з їх особою. Анонімізація або відхилення голосів досягається за допомогою апаратної ізоляції: комп’ютер перевіряє всі підписи та гарантує, що лише ті, хто має право голосу, можуть проголосувати, а також виконує інші необхідні перевірки. Потім окремий комп’ютер розшифровує голоси та підраховує результати. Система ґрунтується на довірі, якої можна досягти за допомогою незалежних спостерігачів, відкритого вихідного коду та процедур складання машин, які можна перевірити, що розділення інтересів є достатнім, щоб гарантувати виборцям право на анонімність під час голосування.

Але що, якби публічна доступність голосів громадян під час виборів не була проблемою? Що, якби ми змогли знайти спосіб дозволити людям відстежувати свої

голоси без необхідності публікувати, чий це був голос? В цьому нам може допомогти алгоритм засліплення. Спочатку створений у Cloudflare Алексом Девідсоном, аспірантом із криптографії в Royal Holloway Лондонського університету [15], процес сліпого цифрового підпису можна адаптувати для полегшення захисту анонімності в системах електронного голосування онлайн. Користувач створює токен, який потім буде засліплений, що дозволяє користувачеві надіслати засліплений токен разом із підтвердженням особи на урядовий сервер. Після того, як сервер перегляне надані облікові дані та переконається, що особа справді контролює свої облікові дані та має право брати участь у голосуванні згідно з чинним законодавством, він застосовує підпис до засліпленого токена, спеціально створеного з метою проведення цих виборів. Додавши до процесу інші системи стримувань і противаг, користувач може мати підписаний засліплений бюлетень. Прибравши засліплення, користувач може отримати звичайний підписаний бюлетень, який можна використовувати для участі у виборах, тоді як уряд може підтвердити, що конкретна особа заявила про токен у певний момент часу, мати докази та дозволити іншим перевірити, що підписаний токен не існує, коли його не слід підписувати. У день виборів користувач може підписати свій голос підписаним токеном і додати доказ того, що він підписав і володіє токеном, фактично не розкриваючи сам токен (інакше хтось інший може використати цей токен, щоб вкрасти чи маніпулювати голосом цієї особи). Ця система ефективно забезпечує анонімність і підзвітність одночасно, дозволяючи кожному бачити свій голос серед голосів інших, не показуючи, який голос є їхнім.

Цей підхід набагато складніший, ніж естонський підхід, але він також має потенціал для вирішення проблеми повної перевірки підзвітності та анонімності вздовж ланцюга голосування. Звичайно, він все ще базується на деяких припущеннях. Одна з них полягає в тому, що підконтрольні державі сервери справно виконують свої завдання. Якщо хтось відчуває параною щодо можливості повної перевірки всього ланцюга процесу голосування, контрольований державою сервер є чорною скринькою, яка може складатися з будь-якого апаратного забезпечення, на якому працює будь-який набір програмного забезпечення, включно з недокументованим, шкідливим та іншим чином здатним виконувати неавторизовані операції, і його

статус неможливо перевірити з повною впевненістю. Звичайно, можна надати вихідний код для сервера, але це лише одна з багатьох проблем із системою. Також необхідно довести, що ця конкретна версія програмного забезпечення фактично використовується на контрольованому урядом сервері; що програмне забезпечення не було додатково модифіковано або змінено способом, відмінним від того, який опубліковано в декларації відкритого коду; що програмне забезпечення не було змінено апаратним забезпеченням, на якому воно виконується; що результати, отримані від виконання програмного забезпечення, є точними; що самі результати не були підроблені; і що результати, опубліковані урядом, генеруються програмним забезпеченням. Іншими словами, потрібна повна впевненість у тому, що система працює належним чином, інакше вона стає слабкою ланкою в ланцюжку довіри всієї системи голосування.

Крім того, оскільки основні методи, які використовуються для ідентифікації, автентифікації та авторизації людей для участі в процесі голосування в цифровому середовищі, покладаються на асиметричне шифрування та цифрові сертифікати, їхня видача також викликає занепокоєння. Оскільки уряди несуть відповідальність за видачу приватних і відкритих сертифікатів як частини інфраструктури відкритих ключів і сертифікацію їх власними підписами, для урядів є тривіальним втручання в деякі аспекти ідентичності шляхом створення підроблених сертифікатів. Таким чином, повна прозорість кожного цифрового сертифіката, виданого компетентними органами, має вирішальне значення для того, щоб цифровий підпис особи не ховався в тіні або неприродним чином змінював баланс результатів виборів.

Забезпечення того, щоб нікому не було дозволено голосувати двічі на виборах, є ще одним важливим моментом. Оскільки контрольований державою сервер відповідає за підписання виборчого бюлетеня, ніщо не заважає особі підписати випадковий рядок символів, який би дозволив їй незаконно віддати більш ніж один голос. Щоб вирішити цю проблему, сервери можуть видати квитанцію про отримання підпису. По суті, це підтвердження сервером того, що особа підписала бюлетень. Додавши дані про особу особи, сліпий бюлетень для голосування, дату й час його підписання, а також відповідь користувача на виклик, вони можуть гарантувати, що

нікому не було видано бюлетень для голосування двічі. Зрештою, квитанція стає загальнодоступним і може містити список тих, хто брав участь у виборах. Воно є не менш таємним, ніж голосування на паперових носіях, оскільки уряд вимагає від усіх учасників підписатися про те, що вони отримали бюлетень.

Висновок по розділу 2

Електронне голосування є складним питанням, і для забезпечення безпеки, прозорості та чесності процесу голосування необхідно ретельно враховувати багато факторів. Аналіз існуючих рішень у різних країнах показує, що не існує універсального підходу до е-голосування. Тематичні дослідження зі Швейцарії, США, Естонії та Австралії підкреслюють важливість вирішення таких питань, як автентифікація виборців, таємниця голосування, доступність, перевірка та аудит при розробці та впровадженні систем електронного голосування. Аналіз процесу голосування в Україні виявив кілька механізмів забезпечення безпеки та прозорості процесу голосування, зокрема наявність списків виборців, розподіл і підрахунок бюлетенів, роль персоналу виборчих дільниць, участь незалежних спостерігачів та підрахунок голосів. Однак виклики цифрового голосування в контексті непрямої демократії потребують подальших досліджень і розробки інноваційних рішень, які б збалансували потребу в безпеці, прозорості та доступності із захистом приватності виборців і запобіганням масштабним фальсифікаціям. Можливі рішення для систем цифрового голосування в Інтернеті включають використання алгоритмів сліпого підпису, які дозволяють виборцям відстежувати свої голоси без розкриття їхньої особистості, а також впровадження надійних заходів безпеки для захисту цілісності процесу голосування. Загалом, розробка та впровадження систем е-голосування вимагає міждисциплінарного підходу в поєднанні з технічними знаннями та хорошим розумінням політичного, соціального та культурного контексту, в якому вони використовуються.

РОЗДІЛ 3
СТВОРЕННЯ СИСТЕМИ БЕЗПЕЧНОГО ЕЛЕКТРОННОГО ГОЛОСУВАННЯ В УКРАЇНІ

У цьому розділі буде надано необхідні алгоритми та пояснення для того, аби читач мав змогу зрозуміти процес запропонованого методу електронного голосування, та мав достатній обсяг знань для розуміння того, яким чином забезпечуються необхідні умови, поставлені у розділі 2.

3.1. Функції хешування

Хеш-функції — це обчислювальні алгоритми, які перетворюють вхідні дані будь-якого розміру на вихідні дані фіксованої довжини, відомі як хеш або хеш-код. Цей процес є детермінованим, тобто ті самі вхідні дані постійно створюватимуть однаковий хеш-код. Основна мета хеш-функцій — забезпечити унікальне та стисле представлення вхідних даних із дотриманням певних криптографічних властивостей.

Одним із популярних прикладів широко поширеної хеш-функції є алгоритм SHA-256 (Secure Hash Algorithm — 256 біт) На рисунку 0.04 показано приклад використання цієї функції. SHA-256 була розроблена Національним інститутом стандартів і технологій США (NIST), з метою забезпечення надійного від колізій та інших криптографічних загроз, перетворюючи вхідні дані в окремий 256-бітний хеш-код.

Хеш-функції створені для ефективної та швидкої роботи, що дозволяє їм обробляти великі обсяги даних за короткий проміжок часу. Крім того, ці функції розроблені як односторонні, що означає, що обчислювально неможливо провести зворотне проектування вихідних вхідних даних із хеш-коду. Ця функція має вирішальне значення для безпечного зберігання та перевірки паролів, оскільки сам пароль не потрібно зберігати.

Хеш-функції знаходять застосування в різних областях, включаючи цифрові підписи, коди автентифікації повідомлень (MAC) і технологію блокчейн. У цифрових

підписах хеш-функції створюють унікальний цифровий відбиток, який можна використовувати для перевірки автентичності та цілісності повідомлення. У MAC хеш-функції поєднуються з секретним ключем для забезпечення автентифікації та цілісності повідомлення.

```
// Функція хешування здатна приймати значення будь-якої довжини та завжди виводить значення однакової та
// визначеної довжини
SHA256("1");                                  // 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
SHA256("Рядок");                              // 1f52375474a6c4b1e1bd13b50353cd11ad4208115f91c8d7cf03948cd3202d54
SHA256("Довший рядок");                       // 69e496d27c7c07a1036cd5bd5b19857588506f0d73f68312b301959dce218e17
SHA256("Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et
dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea
commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla
pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est
laborum.");
// 2d8c2f6d978ca21712b5f6de36c9d31fa8e96a4fa5d8ff8b0188dfb9e7c171bb

// У криптографічно стійкій функції хешування зміна навіть одного біту вхідних даних призводить до значної
// зміни результату
SHA256("Кібербезпека понад усе");             // 1e952a860746f0103555f481a8c994cbb161d6d6956918d031f4fbdff4d87e3e
SHA256("кібербезпека понад усе");             // 1f38101e1c67e1670dfec03031877d64735db7acd061e3132cb1f7fc94fc0acd

SHA256("Word");                               // 3a2860ece5a4ee0b48b41ee96dd8054cf9bc6f113249ec601478b2582d72ead4
SHA256("word");                               // 98c1eb4ee93476743763878fcb96a25fbc9a175074d64004779ecb5242f645e6
SHA256("Cord");                               // 1da84fcc2f2e747fb9d754a52b9bbc01469228fed29cca870eba3b71726bf835

// Однакові вхідні дані завжди призводять до однакового результату
SHA256("Дипломна робота не містить плагіату"); // 437a1a7e2d1cac302bb38da9e062e9ece62190d0a0209dd0b34af355e4a15641
SHA256("Дипломна робота не містить плагіату"); // 437a1a7e2d1cac302bb38da9e062e9ece62190d0a0209dd0b34af355e4a15641
SHA256("Дипломна робота не містить плагіату"); // 437a1a7e2d1cac302bb38da9e062e9ece62190d0a0209dd0b34af355e4a15641
```

Рисунок 3.1 — Приклад використання та результатів криптографічно стійкої функції хешування SHA-256

3.1.1. Колізія хеш-функції

У криптографії хеш-функції схильні до колізій: ситуації, коли кілька різних вхідних даних дають однакове вихідне хеш-значення. Це відбувається через нескінченну кількість можливих входів і кінцевий простір результатів хеш-функції. Оскільки простір визначення нескінченний, на відміну від простору значень, явище колізій є невід’ємною частиною функцій хешування.

Щоб уникнути виникнення колізій, використовуються криптографічно безпечні хеш-функції, такі як SHA-256. Ці функції мають великий вихідний простір (256 біт у випадку SHA-256) і наділені складною структурою, що робить ідентифікацію двох

різних вхідних даних, які дають однакове хеш-значення, обчислювально неможливим. Стійкість до колізій є фундаментальною властивістю криптографічних хеш-функцій.

Це досягається завдяки використанню складних математичних операцій, таких як модульне додавання та XOR, перестановки, трансформації, та інші операції, які виконуються над вхідними даними велику кількість разів. Вихідні дані кожного раунду подаються в наступний раунд, таким чином приховуючи будь-який зв’язок між вхідними даними та результатом. Криптографічні хеш-функції ретельно перевіряються та аналізуються за допомогою таких методів, як диференціальний криптоаналіз, який досліджує відмінності між парами входів і відповідних виходів для виявлення шаблонів або змін у поведінці хеш-функції; лінійний криптоаналіз, який апроксимує поведінку хеш-функцій за допомогою лінійних рівнів для виявлення недоліків і кореляцій; та інших видів криптографічного аналізу.

3.2. Криптографічно стійкі функції хешування

Одним із способів використання хеш-функцій є порівняння еквівалентності двох різних наборів даних, що зазвичай вимагає перевірки, щоб переконатися, що кожен біт даних є однаковим. Однак існують ситуації, наприклад, зберігання паролів у базі даних, коли саме зберігання вихідних даних викликає проблеми, яких слід уникати. Пряме зберігання паролів може становити значний ризик для безпеки. Це пояснюється тим, що якщо базу даних зламано, усі збережені паролі можуть бути розповсюджені зловмисниками. Дослідження показують, що принаймні 65% людей використовують той самий пароль для кількох або всіх онлайн-сервісів [16]. Як наслідок, якщо паролі зберігаються напряму, а одна служба скомпрометована, зловмисник може отримати доступ до більшості, якщо не до всіх, облікових записів користувача в інших незачеплених службах.

Одним із способів зменшити вплив таких атак є зберігання хеш-коду пароля замість самого пароля. Оскільки хеш-функції є детермінованими, вони завжди дають однаковий вихід за тих самих вхідних даних. Тому, якщо хеш-коди різні, вхідні дані повинні бути різними. Однак неможливо визначити, що той самий хеш-код

представляє однакові вхідні дані. Це тому, що в хеш-функціях виникають колізії, і різні вхідні дані можуть створити однаковий хеш-код.

Хоча зіткнення неможливо повністю усунути, можливо мінімізувати ймовірність зіткнень до такої міри, що ймовірність того, що зловмиснику вдасться виявити зіткнення, є дуже низькою, і її можна ігнорувати при формулюванні моделей безпеки. Криптографічно захищені хеш-функції характеризуються дуже низькою ймовірністю колізій і високими обчислювальними зусиллями для виявлення колізій і забезпечення достатньої безпеки для криптографічних програм. Вихід таких функцій не дає жодної інформації про вхід, і навіть невеликі зміни на вході викликають непередбачувані та незворотні зміни на виході, подібні до випадкового шуму.

Криптографічно безпечні хеш-функції можна використовувати для перевірки рівності різних наборів даних без безпосереднього їх порівняння. Криптографічні системи, які замінюють рівність даних рівністю хеш-коду, повинні гарантувати, що припущення щодо чесності та дійсності цієї заміни є правильними на практиці. Тому пошук колізій і вхідних значень із хеш-коду хеш-функції не повинен бути значно швидшим, ніж атака грубою силою, яка перевіряє кожне значення по черзі, доки не буде знайдено відповідне значення.

Хеш-функції зазвичай використовують два основні механізми перетворення даних: перестановку та підстановку. Перестановка перемішує або змішує різні частини даних, змінюючи порядок бітів у вхідних даних, полегшуючи правильну обробку структурованих даних, таких як послідовність нулів і одиниць. Підстановка вимагає групування вхідних даних у блоки, а потім заміни їх іншими даними відповідно до попередньо визначеної статичної таблиці підстановки, узгодженої для всіх вхідних даних.

Сучасні хеш-функції часто включають додаткові методи для підвищення безпеки та продуктивності. Наприклад, кілька раундів перестановок і підстановок з різними операціями в кожному раунді можуть ще більше ускладнити взаємозв’язок введення-виведення. Пропускну здатність і затримку також можна значно збільшити за допомогою таких методів, як нарізка бітів і векторизація для розпаралелювання

обчислень хеш-функцій на кількох процесорах або блоках SIMD (одна інструкція з кількома даними).

3.3. Функція хеш-коду аутентифікації повідомлень

Функція хеш-коду аутентифікації повідомлень (MAC) — це криптографічний метод, який використовується для перевірки автентичності та цілісності даних у незахищених середовищах. Особливим варіантом цієї функції є функція хеш-коду автентифікації повідомлення (HMAC), яка базується на певному алгоритмі хешування. Вона поєднує алгоритм хешування з секретним ключем, відомим як генератору хеш-коду автентифікації повідомлення, так і об’єкту, який його перевіряє. Повідомлення та секретний ключ приймаються як вхідні дані, і генерується хеш-код автентифікації повідомлення.

Структура функції хеш-коду автентифікації повідомлення дозволяє використовувати існуючі хеш-функції, потенційно усуваючи необхідність розробки та захисту нових хеш-функцій. Це також полегшує заміну однієї функції іншою, якщо у вибраній функції виявлено вразливість чи недолік або якщо функція з надійними властивостями виявляється еквівалентною швидшому алгоритму.

3.4. Кваліфікований електронний підпис

Кваліфікований електронний підпис є видом електронного підпису, який відповідає вимогам Регламенту ЄС № 910/2014 (eIDAS) для електронних транзакцій на внутрішньому європейському ринку [17]. Він забезпечує можливість перевірки авторства даних або документів в електронному обміні даних протягом тривалого періоду часу та може розглядатися як цифровий еквівалент підпису, створеного власноруч [18; 19].

Кваліфікований електронний підпис містить інформацію про особу, якій він був виданий, та може використовуватися для її ідентифікації та аутентифікації [19].

3.5. Алгоритми у складі системи електронного голосування

3.5.1. Алгоритм засліплення

Нехай існують дві сторони, клієнт та сервер, причому сервер має секретний ключ. Клієнт бажає отримати підпис сервера на деякому значенні, при цьому не розкриваючи самого значення. Для цього клієнт та сервер можуть домовитися про використання еліптичної кривої та її параметрів. Для вирішення цієї задачі може бути використана процедура засліплення.

Нехай існує точка еліптичної кривої, створена на основі токена, яке потребує підпису секретним ключем серверу.

Аби зберегти секретність цієї точки і не дати серверу можливості його дізнатися, клієнт генерує випадкове значення, яке називається засліпленням. Завдяки використанню еліптичної кривої, ми можемо знайти значення, зворотне до засліплення, і використати його для того, аби це засліплення пізніше прибрати. Клієнт накладає засліплення на бюлетень та надсилає його серверу. Сервер підписує надісланий засліплений бюлетень. Результат надається користувачеві. Потім клієнт знімає засліплення і отримує дійсний бюлетень з підписом державного сервера. Завдяки цій стратегії сервер не дізнався нічого про сам бюлетень, адже він мав доступ тільки до засліплених значень. Тим часом, громадянин отримав підпис на значення, про яке держава нічого не може знати.

3.5.2. Алгоритм початку процесу голосування

Оскільки дані можуть зберігатися протягом необмеженої кількості часу, необхідно коректно налаштувати процес початку голосування. В кожному окремому голосуванні сервер зобов’язаний використовувати окрему унікальну пару публічного і приватного ключа, які не використовуються будь-де в іншому місці. Це необхідно для того, аби громадяни не могли використовувати старі бюлетені в новому голосуванні, а також задля того, аби старі бюлетені взагалі не могли вважатися дійсними в новому голосуванні. Логічно, адже ми не використовуємо одні і ті самі

паперові бюлетені в традиційному, паперовому голосуванні повторно, а друкуємо і розповсюджуємо нові.

3.5.3. Алгоритм створення електронного бюлетеня та його підписання

Для створення бюлетеня, який придатний для використання під час голосування, необхідно врахувати низку вимог та важливих аспектів, кожен з яких впливає на безпеку всієї системи та не дозволяє будь-яким зловживанням з боку зловмисних сторін.

Для того, аби почати сам процес голосування, клієнт створює випадкове значення, яке називається токеном. Цей токен пізніше буде доступним публічно. Через це до нього застосовується декілька ключових вимог:

— довжина токена фіксована системою: 256 біт;

— токен має генеруватися з використанням криптографічно випадкових джерел та систем.

Фіксована довжина ключа не дозволяє одному (або малому набору) клієнтів створювати величезні токени, що запобігає атакам відмови в обслуговуванні. Якщо цієї вимоги не дотримуватися, існує загроза створення токенів розмірами з гігабайти, або навіть терабайти даних. Навіть один такий токен здатен перевантажити практично будь-які існуючі інформаційно-телекомунікаційні системи. Нам достатньо 256 біт криптографічно випадкових значень для того, аби на практичному рівні на задовільному рівні прибрати загрози колізій або грубої сили. З очевидних причин, криптографічна випадковість дозволяє нам прибрати ризики витоку даних і відповідного зменшення ентропії створених токенів, а значить і простору значень, в якому ці токени існують, до критично вразливих величин.

Після того клієнт генерує засліплення аналогічним чином, з аналогічними обмеженнями. Оскільки до використання рекомендована крива Curve25519, обгорнута в систему Ristretto, значення розміром більше за 256 біт не мають практичної цінності, адже вони не дадуть жодної користі користувачеві. Тим більше, виключно користувач зазнає впливу збільшеного розміру значення засліплення, адже користувачеві доведеться генерувати значення, обернене до засліплення. Чим більше

це значення, тим більше обчислювальних ресурсів доведеться використати клієнту для своїх обчислень, що шкодитиме виключно йому. З цих міркувань, нам достатньо такого значення, яке не дозволить зловмисникам підібрати засліплення грубою силою. 256 біт є достатньою довжиною для цього.

Використовуючи токен, клієнт генерує бюлетень, який є точкою на обраній еліптичній кривій. Для цього використовується обрана функція хешування. Крива і хеш-функція обрані таким чином, аби уникнути необхідності перевірок на те, чи є згенероване значення дійсною точкою, адже воно буде завжди дійсним.

Після того, на створений бюлетень накладається засліплення використовуючи скалярне множення числа на точку еліптичної кривої. Аналогічним чином пізніше буде накладено підпис і значення, обернене до засліплення.

Державний сервер отримує від клієнта засліплений бюлетень. Використовуючи існуючу інфраструктуру підтвердження особистості громадянина (Дія.Підпис, BankID, кваліфіковані електронні підписи, тощо), держава впевнюється в тому, що громадянин має право приймати участь в цьому голосуванні. Згідно статті 70 Конституції України [20], наразі для цього в Україні існують наступні вимоги:

— громадянин має досягнути вісімнадцятирічного віку на день проведення виборів;

— громадянин має бути дієздатним.

Також можуть існувати інші обмеження. Наприклад, відсутність судимості або позбавлення волі. Оскільки ці норми можуть змінюватися з часом в залежності від змін законодавства або Конституції, налаштування обмежень здійснюється на рівні редагувань умов, які мають бути виконані для надання конкретному громадянину права участі в електронному голосуванні.

Додатково, системою електронного голосування накладаються наступні обмеження:

— громадянин має право отримати не більше одного дійсного і непогашеного підписаного електронного бюлетеня;

— громадянин має надати дійсний кваліфікований електронний підпис, виданий уповноваженим і дійсним кваліфікованим надавачем електронних довірчих послуг.

У разі успішного проходження усіх перевірок, сервер надає громадянинові підписану копію засліпленого бюлетеня, а також публікує квитанцію, що засвідчує видання громадянинові електронного бюлетеня з наданими параметрами.

Квитанція — це хеш публічної точки голосування, її підписаної копії, бюлетеня, його підписаної копії, часу голосування, та випадкового числа, що використовується виключно один раз (nonce).

Також сервер надає доказ дискретної логарифмічної еквівалентності, що дозволяє клієнту пересвідчитися, що його бюлетень було підписано ключем, який опублікований державою перед початком голосування, і що його бюлетень не помічено унікальним маркером.

Після отримання всіх даних від серверу, клієнт знімає засліплення з отриманого бюлетеня, отримуючи підписаний незасліплений бюлетень, придатний для використання в електронному голосуванні.

У випадку, якщо не сталося ніяких проблем під час цього процесу, алгоритм вважається успішно виконаним.

3.5.4. Алгоритм голосування з використанням електронного бюлетеня

Вважаємо, що клієнт має токен; бюлетень, створений на основі цього токену; та підписану копію цього бюлетеня. Цей бюлетень не має бути анульованим (згідно пункту 3.5.6 нижче).

Також вважаємо, що сервер визначився з конкретним форматом, згідно якого має бути поданий електронний голос. Цей формат визначено в підрозділі 3.6 нижче.

Для початку, клієнт формує своє повідомлення та оброблює його, разом зі значенням підписаного бюлетеня, через функцію хеш-коду аутентифікації повідомлень. Після цього клієнт передає результуюче значення, а також саме повідомлення та токен, на основі якого сформовано бюлетень, підписану копію якого було використано.

Після отримання цих значень, сервер проводить наступні перевірки:

— повідомлення голосу не містить символів окрім тих, що дозволені для використання у повідомленнях голосу;

— повідомлення голосу відповідає специфікації JSON;

— повідомлення голосу має всі поля, що вимагаються у форматі, та не містить жодних додаткових полів;

— всі поля повідомлення голосу мають коректний формат, як зазначено в описах формату конкретних полів;

— поле версії має значення «1»;

— поле унікального числового ідентифікатора кандидата відповідає дійсному кандидату, що був опублікований під час створення голосування;

— поле повного імені кандидата заповнено відповідно до опублікованих державним сервером даних та співпадає з унікальним числовим ідентифікатором цього кандидата;

— поле дати народження кандидата заповнено відповідно до опублікованих державним сервером даних та співпадає з унікальним числовим ідентифікатором цього кандидата;

— поле додаткових даних щодо кандидата заповнено відповідно до опублікованих державним сервером даних та співпадає з унікальним числовим ідентифікатором цього кандидата;

— поле часової мітки наданого голосу має коректний формат та відрізняється від часу серверу не більше як на 15 секунд;

— поле значення, що використовується виключно один раз, має коректний формат і довжину, а також не використовувалося раніше в цьому голосуванні.

Токен, переданий клієнту, використовується для генерації бюлетеню, підписана копія якого дозволяє підтвердити, що передане значення функції хеш-коду аутентифікації повідомлення є дійсним.

Якщо всі ці перевірки пройдено успішно та, голос вважається успішно наданим. Сервер публікує це повідомлення, результат функції хеш-коду аутентифікації повідомлень, та позначає час отримання цього голосу.

Якщо надані дані призводять до помилки, яка не дозволяє підтвердити усі вимоги, зазначені вище, сервер видає помилку з поясненням допущеної помилки, і не реєструє такий голос як успішно наданий.

3.5.5. Процес завершення процесу голосування та підрахунку результатів голосування

Після завершення часу, відведеного на голосування, сервер припиняє приймати нові голоси і починає підрахунок результатів. Сервер перевіряє всі надані голоси на дійсність та підраховує унікальні числові ідентифікатори кандидатів в повідомленнях голосів, які успішно пройшли перевірку та вважаються дійсними. Також сервер проводить підрахунок усіх голосів, які не вдалося врахувати і які вважаються недійсними. Ці дані публікуються сервером.

3.5.6. Процес анулювання бюлетеня

Для того, аби анулювати свій бюлетень, клієнт зобов’язаний надати доказ, що саме він володіє зазначеним бюлетенем. Для цього він надає значення засліплення до серверу, вказує на квитанцію, згідно якої сервер підписав засліплений бюлетень, та надає токен такого бюлетеня. У разі, якщо сервер здатний підтвердити, що наданий токен та засліплення створюють засліплений бюлетень, вказаний в квитанції, така квитанція анулюється і токен такого бюлетеня вважається недійсним. Сервер знаходить усі голоси, що були створені за цим токеном, і видаляє їх з своєї системи. Громадянин отримує право повторно підписати бюлетень.

3.6. Формат подання електронного голосу

3.6.1. Загальні вимоги до формату подання

Для подання повідомлення, яке становитиме власне голос кандидата, виставляються наступні вимоги:

— Повідомлення має бути подане в форматі JSON (JavaScript Object Notation) [21].

— Повідомлення може складатися виключно з символів, перелік яких надано нижче.

— Повідомлення може мати виключно поля з назвами і значеннями, обмеження на які викладено нижче.

— Повідомлення може містити поля в будь-якому порядку.

3.6.2. Вимоги щодо символів, допустимих до використання в повідомленні

Вичерпний перелік символів, які дозволено використовувати в повідомленні:

— Великі символи українського алфавіту (кирилиці): "А", "Б", "В", "Г", "Ґ", "Д", "Е", "Є", "Ж", "З", "И", "І", "Ї", "Й", "К", "Л", "М", "Н", "О", "П", "Р", "С", "Т", "У", "Ф", "Х", "Ц", "Ч", "Ш", "Щ", "Ь", "Ю", "Я".

— Малі символи українського алфавіту (кирилиці): "а", "б", "в", "г", "ґ", "д", "е", "є", "ж", "з", "и", "і", "ї", "й", "к", "л", "м", "н", "о", "п", "р", "с", "т", "у", "ф", "х", "ц", "ч", "ш", "щ", "ь", "ю", "я".

— Арабські цифри: "0", "1", "2", "3", "4", "5", "6", "7", "8", "9".

— Великі літери англійського алфавіту (латиниці): "A", "B", "C", "D", "E", "F", "G", "H", "I", "J", "K", "L", "M", "N", "O", "P", "Q", "R", "S", "T", "U", "V", "W", "X", "Y", "Z".

— Малі літери англійського алфавіту (латиниці): "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o", "p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z".

— Окремі спеціальні символи: "." (крапка), "," (кома), "!" (знак оклику), "?" (знак питання), "-" (дефіс), "'" (апостроф), "\"" (лапки), "(", ")" (круглі дужки), "[", "]" (квадратні дужки), "{", "}" (фігурні дужки), ";" (крапка з комою), "+" (плюс), "_" (нижнє підкреслення).

— Пробіл: " ".

3.6.3. Вимоги щодо полів, які дозволено використовувати в повідомленні

Для того, аби повідомлення голосу мало зміст і могло сприйматися як машинами, так і людьми, вимагається використовувати наступні поля та наступні значення цих полів:

«version» — це поле типу рядка, яке може містити виключно арабські цифри і має бути цілим числовим значенням в межах від 1 до 32767. Це поле позначає версію формату повідомлень системи голосування і створено для того, аби дозволити покращення або модифікації до даного формату у майбутньому. Наразі єдиною коректною версією є версія 1, того «1» вважається єдиним коректним значенням.

«candidate-id» — це поле типу рядка, яке може містити виключно арабські цифри і має бути цілим числовим значенням в межах від 1 до 32767. Це поле позначає унікальний числовий ідентифікатор кандидата. Співвідношення кандидатів до їх унікальних числових ідентифікаторів задається при створенні голосування і публікується разом з іншими даними.

«candidate-name» — поле типу рядка, яке містить повне законне ім’я кандидата у форматі «Прізвище Ім’я По-батькові». Воно може складатися з символів кирилиці, латиниці, апострофів, дефісів та пробілів. Список імен кандидатів публікується центральною виборчою комісією. Системи створення повідомлень голосів зобов’язані надавати користувачам доступ вводити в це поле виключно дійсні імена кандидатів, які співпадають з унікальним числовим ідентифікатором такого кандидата, що зазначено в полі «candidate-id».

У випадку, якщо ім’я кандидата містить символи поза цим списком, замість таких символів використовується дефіс. Якщо така заміна призводить до значної альтерації імені кандидата, рекомендується створення нової версії формату повідомлень голосів для того, аби надати можливість коректно репрезентувати ім’я такого кандидата.

«candidate-date-of-birth» — поле типу рядка, яке містить дату народження кандидата, подану у форматі «чч.мм.рррр», де «чч» — це число дати народження, подане рівно двома арабськими цифрами; «мм» — це місяць дати народження, подане

рівно двома арабськими цифрами; а «pppp» — це рік дати народження, подане рівно чотирма арабськими цифрами. Це значення має відповідати даті народження кандидата, унікальний числовий ідентифікатор якого зазначеного в полі «candidate-id». Системи створення повідомлень голосів зобов’язані коректно заповнювати це поле, виходячи з опублікованих державним сервером даних.

«extra» — додаткові дані, які подані текстовим рядком довільної форми. Ці значення мають відповідати даним, унікальний числовий ідентифікатор яких зазначеного в полі «candidate-id». Системи створення повідомлень голосів зобов’язані коректно заповнювати це поле, виходячи з опублікованих державним сервером даних.

«timestamp» — поле типу рядка для часової мітки, поданої згідно формату RFC 8601 [22].

«nonce» — поле типу рядка для значення, яке згенероване виключно один раз. Це значення має бути довжиною 256 біт і закодоване за допомогою формату кодування base64url, яке подане в стандарті RFC 4648 [23].

На рисунку .5 показано приклад коректно заповненого повідомлення голосу, що відповідає кандидату з наступними даними:

— Унікальний числовий ідентифікатор: 4.

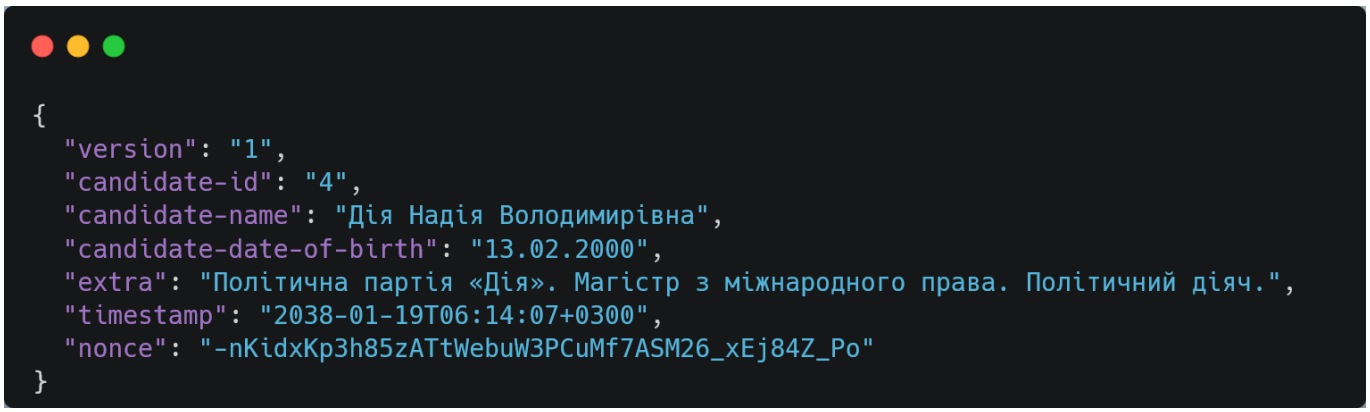
— Повне законне ім’я: Дія Надія Володимирівна.

— Дата народження: 13.02.2000.

— Додаткові дані: «Політична партія «Дія». Магістр з міжнародного права. Політичний діяч.».

— Часова мітка: «2038-01-19T06:14:07+0300» [24].

— Значення, що використовується виключно один раз: «-nKidxKp3h85zATtWebuW3PCuMf7ASM26_xEj84Z_Po».



```
{
  "version": "1",
  "candidate-id": "4",
  "candidate-name": "Дія Надія Володимирівна",
  "candidate-date-of-birth": "13.02.2000",
  "extra": "Політична партія «Дія». Магістр з міжнародного права. Політичний діяч.",
  "timestamp": "2038-01-19T06:14:07+0300",
  "nonce": "-nKidxKp3h85zATtWebuW3PCuMf7ASM26_xEj84Z_Po"
}
```

Рисунок 3.2 — Приклад коректного повідомлення голосу

3.7. Забезпечення відмовостійкості системи

Відмовостійкість означає здатність системи продовжувати нормальне функціонування у разі збою або помилки певного компонента. У системах, які не призначені для роботи з такими ситуаціями, навіть незначні збої викликають повний крах, тоді як у відмовостійких системах погіршення якості роботи зазвичай пропорційне ступеню збою. Ця характеристика дуже бажана в системах, які мають вирішальне значення для успіху місії, високої доступності або життєзабезпечення. Плавна деградація — це термін, який використовується для опису здатності системи продовжувати роботу, коли певний компонент виходить з ладу. [25]

Для забезпечення відмовостійкості системи необхідно використовувати якісні системи та алгоритми, аби елементи системи могли виходити з ладу плавно, дозволяючи системі як такій продовжувати свою роботу, навіть якщо і зі зменшеною ємністю до навантаження. Для цього можливо використовувати розробку, запропоновану в [26]. Протокол виявлення стану репліки (Replica State Discovert Protocol RSDP), розроблений в цій роботі, може бути використаний для досягнення відмовостійкості в розподілених системах. Нижче наведені деякі зі способів, за допомогою яких RSDP може сприяти підвищенню відмовостійкості:

— Надання узгодженої інформації про стан: RSDP гарантує, що узгоджена інформація про стан підтримується в декількох репліках розподіленої системи. Гарантуючи, що всі репліки мають однакову інформацію про стан, система може

легше відновлюватися після збою, оскільки репліки можуть синхронізувати свій стан за допомогою RSDP.

— Обробка помилок під час синхронізації реплік: RSDP включає механізми для обробки помилок під час процесу синхронізації реплік. Наприклад, якщо репліка не може отримати повідомлення, вона може попросити відправника повторити спробу надіслати повідомлення або використати механізм резервного копіювання для відновлення після збою.

— Плавний перехід між репліками: RSDP забезпечує безперебійний перехід між репліками, коли додається нова репліка або існуюча репліка виходить з ладу; система забезпечує безперебійний перехід, використовуючи RSDP для підтримки узгодженої інформації про стан у всіх репліках і гарантує, що інформація про стан не буде суперечливою.

— Зменшення впливу збоїв на систему; використовуючи RSDP для підтримки узгодженої інформації про стан і обробки збоїв під час синхронізації реплік, система може зменшити загальносистемний вплив збоїв. Це підвищує відмовостійкість розподіленої системи і дозволяє їй продовжувати роботу в разі збою.

— Підвищена масштабованість системи: Розподіляючи інформацію про стан між декількома репліками і використовуючи RSDP для підтримки узгодженості, система може впоратися з більшим навантаженням і збільшити масштабованість. Це особливо важливо в розподілених системах, які обробляють велику кількість запитів і транзакцій.

Replica State Detection Algorithm можна використовувати для досягнення відмовостійкості в розподілених системах, надаючи узгоджену інформацію про стан, обробляючи збої під час синхронізації реплік, забезпечуючи плавний перехід між репліками, зменшуючи вплив збоїв на систему і покращуючи масштабованість системи. Завдяки цьому у разі можливої розподіленої атаки відмови в обслуговуванні (DDoS) ми можемо досягнути швидке відновлення окремих компонент системи і їх самосинхронізацію та самоналаштування одне відносно одного.

3.8. Поєднання системи з державними ресурсами

3.8.1. Дія

Мобільний додаток, веб-портал і бренд Дія, запущений у 2020 році, дозволяє українцям використовувати цифрові документи на своїх смартфонах замість фізичних для ідентифікації та обміну. Через портал «Дія» громадяни мають доступ до величезної кількості державних послуг, кінцевою метою яких є забезпечення всіх форм взаємодії між владою через цю платформу На рисунку .6 зображено приклад інтерфейсу застосунку.

Дія була розроблена у співпраці зі Сполученими Штатами та призначена для використання як в Україні, так і в інших країнах. Вперше оголошена 27 вересня 2019 року Міністерством цифрової трансформації України, Дія є значним кроком у напрямку спрощення та оптимізації державних послуг. Об’єднавши всі державні сервіси в одну платформу, міністр цифрової трансформації Михайло Федоров створив зручну та ефективну систему взаємодії громадян і бізнесу з владою.

Основною перевагою Дія є зручність, яку вона пропонує, дозволяючи громадянам зберігати та отримувати доступ до багатьох документів на своїх смартфонах, не турбуючись про втрату чи пошкодження. За потреби люди можуть легко отримати доступ до цих цифрових документів через свої смартфони, зменшуючи потребу у фізичних документах і підвищуючи швидкість і ефективність державних послуг.

Впровадження Дія призвело до скорочення штату державних службовців на 10%, заощадивши сотні мільйонів доларів, а також підвищивши швидкість, ефективність і прозорість державних послуг. Крім того, цифровізація державного сектору сприяла зростанню IT-індустрії країни та покращенню цифрової обізнаності та освіти людей, що, у свою чергу, має позитивний вплив на інші сектори, сприяючи прийняттю цифрової інфраструктури та прискоренню загальних темпів цифровізації.

Рисунок 3.3 — Інтерфейс додатку цифрової демократії «Дія»

3.8.2. Єдиний державний реєстр виборців

Єдиний державний реєстр виборців (ЄДРВ) — автоматизована інформаційно-телекомунікаційна система, яка існує на теренах України. Доступ до неї здійснюється виключно по закритих каналах передачі інформації, доступ пересічним громадянам до даних заборонений. Цей реєстр призначений для зберігання та обробки даних, які регулюються Законом України «Про державний реєстр виборців» [27].

В реєстрі зберігаються наступні дані про виборців:

— ПІБ.

— Дата народження.

— Виборча адреса (адреса проживання).

— Місце народження (ця інформація не фіксується під час проведення самих виборів).

Використання цієї системи дозволяє мати точні дані про виборців. Вважається, що у випадку змін законодавства щодо того, хто має виборче право в Україні та які обмеження накладаються на виборче право, вони будуть відображені у єдиному державному реєстрі виборців шляхом додання або видалення з нього людей, які мають або не мають (відповідно) права приймати участь у голосуванні.

3.8.3. Центральна виборча комісія України

Центральна виборча комісія України (ЦВК) — це державний орган України, який здійснює проведення виборів:

— Президента України;

— народних депутатів України;

— депутатів Верховної Ради Автономної Республіки Крим;

— депутатів місцевих рад та сільських, селищних, міських голів, голів громад;

а також займається організацією всеукраїнських та місцевих референдумів в порядку та в межах, встановлених законами України.

Центральна виборча комісія здійснює реєстрацію кандидатів на участь в голосуванні, організацію виборчого процесу, закупівлю необхідного обладнання та ресурсів для проведення самого голосування, наймання працівників, що організовуватимуть сам процес голосування, а також підтримку цифрових ресурсів, які використовуються в процесі голосування.

В рамках даної системи пропонується використовувати інфраструктуру та ресурси центральної виборчої комісії для розміщення апаратного забезпечення та під’єднання інформаційно-телекомунікаційної системи до мережі Інтернет, а також розміщення на такому апаратному забезпеченні програмного забезпечення, створеного для проведення голосування як державного серверу, до якого громадяни під’єднуються у якості клієнтів.

Висновки по розділу 3

Побудова безпечної системи електронного голосування в Україні вимагає глибокого розуміння математичних примітивів та операцій. Зокрема, використання полів та еліптичних кривих забезпечує міцний фундамент для системи. Здатність знаходити адитивну обернену точку, суму двох точок та скалярний добуток точки і скаляра є важливими операціями в системі. Крім того, використання алгоритму подвійного додавання для скалярного добутку гарантує ефективні та безпечні обчислення. Система повинна розв'язувати задачу дискретних логарифмів на

еліптичних кривих; Ro-алгоритм Полларда наразі є найкращим методом для знаходження логарифмів, який має квадратичну складність; 256-бітний ключ надає 128 біт безпеки. Система також повинна забезпечувати спосіб доведення еквівалентності дискретних логарифмів без розкриття їх істинних значень. Цього можна досягти за допомогою протоколу "виклик-відповідь". Протокол "виклик-відповідь" складається з того, що верифікатор генерує випадкове число nonce, обчислює відповідну точку на кривій і надсилає її верифікатору. Верифікатор повинен відправити назад значення виклику і обчислити добуток nonce, виклику і відповідної точки на кривій. Верифікатор може довести еквівалентність, не розкриваючи нонсе, перевіряючи, чи дорівнює обчислена точка добутку вихідної точки та виклику. Система повинна гарантувати цілісність та автентичність голосування. Це може бути реалізовано за допомогою криптографічних хеш-функцій та цифрових підписів. Шляхом хешування бюлетеня та підписання його особистим ключем виборця можна перевірити автентичність та цілісність бюлетеня. Крім того, система повинна забезпечувати конфіденційність голосування і гарантувати, що голос не може бути пов'язаний з виборцем. Цього можна досягти за допомогою технології "засліплення", коли голос виборця покривається випадковою величиною і виявляється системою після того, як голос був перевірений і зареєстрований. Система повинна бути розроблена з урахуванням відмовостійкості, щоб вона могла продовжувати функціонувати належним чином у разі виходу з ладу або деградації деяких її компонентів. Погіршення продуктивності має бути пропорційним серйозності збою, на відміну від системи, яка не розрахована на такі ситуації і може повністю вийти з ладу. Відмовостійкість особливо важлива для систем з високим рівнем доступності, критично важливих або життєво необхідних систем, де здатність підтримувати функціональність при виході з ладу частини системи називається плавною деградацією. Створення безпечної системи електронного голосування в Україні вимагає глибокого розуміння математичних примітивів, арифметики та криптографічних методів. Система повинна вирішувати питання дискретних логарифмів, цілісності та автентичності голосу, таємниці голосування та відмовостійкості. Використання полів, еліптичних кривих, криптографічних хеш-

функцій, цифрових підписів, методів із зав'язаними очима та відмовостійких принципів проектування може забезпечити міцну основу для систем. Однак розробка і впровадження таких систем є складним і відповідальним завданням і вимагає ретельного врахування низки факторів, а також ретельного тестування і оцінки для забезпечення їхньої безпеки і надійності.

РОЗДІЛ 4
ДОСЛІДЖЕННЯ БЕЗПЕЧНОСТІ ЗАПРОПОНОВАНОЇ СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

4.1. Аналіз розглянутих атак на систему та шляхи їх знешкодження

4.1.1. Розмноження електронних бюлетенів

Оскільки клієнти мають доступ одночасно до підписаного та непідписаного бюлетеня, які є точками еліптичної кривої, нічого не заважає клієнтам помножити обидва значення на довільний скаляр, при цьому зберігаючи підпис серверу на бюлетені. Використовуючи подібний метод, зловмисники здатні згенерувати практично нескінченну кількість підписаних бюлетенів.

Аби цього уникнути, необхідно обмежити здатність клієнтів маніпулювати точками еліптичної кривої. Для цього достатньо зробити так, аби клієнт не міг самостійно обрати довільно задану точку еліптичної кривої. Цього можна досягнути, якщо замість самої точки використовувати токен, згідно якого вона була згенерована. Клієнту не потрібно мати контроль над точкою еліптичної кривої. Вона є виключно носієм скаляру підпису, який було накладено саме на точку клієнта, а не когось іншого. Токен вирішує цю проблему: координати точки (які визначають точку на кривій) задаються клієнтом не напряму, а використовуючи хеш токену. Завдяки цьому ми можемо самостійно згенерувати точку бюлетеня з токену і виконувати операції над нею як нам завгодно. При цьому користувач не має здатності впливати на ці точки якимось чином. В результаті, єдина цінність знання підписаної версії точки, згенерованої за деяким токеном, полягає в наявності знання цього підписаного значення, яке можна було отримати виключно пройшовши процес створення бюлетеню.

4.1.2. Пов’язування громадян з їх голосами

Забезпечення конфіденційності голосу кожного учасника системи є необхідною складовою системи. Простими словами, ніхто не має мати можливість з упевненістю сказати, хто віддав який голос за якого кандидата. Проблема полягає у тому, що держава має перевірити, чи має громадянин право приймати участь у голосуванні, і для цього їх потрібно знати її персональні дані. В паперовому голосуванні, бюлетень відділяється від корюшка фізично, а сам бюлетень надається людині тільки після того, як вона надала документ, що посвідчує її особу, співробітникам пункту голосування. Оскільки всі бюлетені фізично та візуально перемішуються, вважається, що жодна людина або система не здатна з точністю відслідковувати голоси людей.

Цифрові технології, нажаль, такого припущення собі допустити не можуть. Відслідковування даних є тривіальною задачею для будь-якої інформаційно-телекомунікаційної системи. Саме через це в розробленій системи використовується процес засліплення, завдяки якому держава позбавляється можливості зіставити бюлетень особи з її особистими даними. Навіть якщо держава відслідковуватиме всі дані, вона матиме лише інформацію про те, хто прийняв участь у голосуванні, але не детальне зіставлення людини до її голосу. Ця інформація доступна для держави і в традиційних системах голосування, того це не створює витоку інформації в порівнянні з нею. Єдиним недоліком розробленої системи є те, що у порівнянні з паперовим голосуванням, інформація про факт участі у голосуванні є публічно доступною і загальновідомою.

4.1.3. Відсутність обліку підписаних електронних бюлетенів

Ведення обліку бюлетенів під час голосування є важливою складовою процесу голосування. Без цього держава не знатиме, звідки взялися голоси, і система не матиме жодних інструментів підтвердження того, що не відбулося підкидання голосів.

Спеціально для цього в системі існують квитанції, які слугують способом забезпечити обліку виданих бюлетенів. Держава вимушена видати квитанцію для

того, аби підтвердити, що вона використовує свій підпис виключно за призначенням. У випадку, якщо під час підрахунку голосів виявиться, що голосів у системі більше, ніж отриманих квитанцій, ми можемо зробити висновок про підкидання голосів і маніпуляції з боку держави.

4.1.4. Відслідковування голосів

Анонімність голосу клієнта є однією з головних властивостей розробленої системи безпечного електронного голосування в Україні. Саме для цього використовується алгоритм засліплення. Але нічого не заважає відслідковувати клієнтів за допомогою різних підписів. Якщо кожен клієнт має свій унікальний підпис, який сервер використав для підписання точки конкретно цієї людини і жодної іншої, сервер має змогу зіставити людину з її голосом. Сервер бачив, хто створював конкретний бюлетень, того у нього є персональні дані цієї людини. Підписаний бюлетень цієї людини має підпис, який був виданий лише їй особисто. Значить, якщо такий бюлетень було використано для голосування, держава знатиме, хто віддав цей голос і матиме беззаперечний доказ цього.

Для уникнення такої ситуації використовується доказ дискретної логарифмічної еквівалентності. Цей доказ дозволяє серверу показати, що дві точки були підписані одним і тим самим підписом, не розкриваючи при цьому сам підпис. Сервер публікує приклад підпису і посилається на нього, накладаючи підписи на бюлетені інших людей. Завдяки доказу дискретної логарифмічної еквівалентності, який сервер зобов’язує надавати клієнтам при підписуванні їх бюлетенів, громадяни здатні одразу перевірити, чи їх не надурили. Оскарження некоректних доказів є поза розглядом цієї системи, але вважається, що у разі масштабного маніпулювання процесу голосування достатня кількість людей заявить про свої проблеми, аби підірвати довіру до результатів голосування.

4.1.5. Державна підробка бюлетенів

У процесі створення та підписання електронного бюлетеня громадянин спочатку створює та передає квитанцію, що підтверджує отримання підписаного бюлетеня, створеного сервером. Однак, оскільки зв'язок здійснюється через Інтернет, передача даних може бути нестабільною або з'єднання може бути розірвано з будь-якої причини. Щоб запобігти таким можливостям, сервер зобов'язаний опублікувати копію підписаного засліпленого бюлетеня та опублікувати інформацію про отримання цієї копії. У випадку відмови держава зобов’язана повідомити користувача про причину відмови. Держава не може відмовити у підписанні бюлетеня громадянину, якщо вона не може знайти квитанцію, яка підтверджує факт отримання таким громадянином підпису на вже існуючому і ще досі дійсному бюлетені.

Громадянин може використати квитанцію, щоб знайти копію підписаного засліпленого електронного бюлетеня. Якщо з будь-якої причини громадянин не може знайти надану квитанцію у списку, опублікованому сервером, вважається, що національний сервер електронного голосування не може довести причину відмови. Це може стати підставою для підозри в неправомірності процесу голосування як такого та визнання результатів такого голосування недійсними у зв'язку з порушенням процедури голосування.

4.1.6. Захист від зловмисного анулювання чужих бюлетенів

Оскільки процес електронного голосування передбачає публікацію значної кількості даних, особа, яка бажає скасувати певний бюлетень, повинна мати можливість чітко довести, що саме вона створила цей бюлетень. Для цього вона повинна надати токен і засліплення, яке було використано під час підписання бюлетеню. Оскільки цими значеннями може володіти виключно той, хто їх створив (вважається, що значення засліплення є секретом, який клієнти зобов’язані не розголошувати), то вона створила бюлетень і хоче його скасувати. Усі бюлетені, створені за допомогою наданого токена, втрачають свою силу і всі голоси, враховані в системі, анулюються та видаляються.

4.1.7. Перехоплення бюлетенів під час їх використання

Коли громадянин хоче використати свій підписаний бюлетень для того, аби надати свій голос до системи, він має надати доказ того, що він володіє цим підписаним бюлетенем. Найпростішим рішенням є передати саме значення цього підписаного бюлетеня серверу для того, аби сервер міг перевірити дійсність цього підпису. Нажаль, канали зв'язку не завжди є захищеними, того система має розглядати ризик перехоплення зловмисниками всіх даних, які передаються між сторонами, у разі використання атаки людини посередині (man in the middle).

Але нам не обов'язково передавати саме значення підписаного бюлетеня аби довести, що ми ним володіємо. Замість цього ми можемо відправити результат функції хеш-коду аутентифікації повідомлення, аргументами якої є повідомлення голосу та підписаний бюлетень. Для того, аби сервер міг впевнитися в тому, що цей підписаний бюлетень дійсно є тим, чим заявляє клієнт, клієнт має надіслати також свій токен.

Для перевірки, сервер генерує бюлетень з токену, підписує цей потенційний бюлетень, і перевіряє, чи передане повідомлення голосу, використане у якості аргументу до функції хеш-коду аутентифікації повідомлення, разом з новоствореним підписаним бюлетенем відповідає результату функції хеш-коду аутентифікації повідомлення, який передав клієнт. У разі співпадіння можна зробити висновок, що клієнт мав доступ до значення підписаного бюлетеня, бо вважається, що лише сервер має доступ до самого ключа підпису. Відповідно, якщо клієнт мав доступ до підписаної копії бюлетеня, він пройшов всі необхідні перевірки та має право приймати участь у даному електронному голосуванні, і його голос має бути врахований у фінальному підрахунку.

4.1.8. Часові мітки

Теоретично, нічого не заважає клієнтам надсилати свої голоси до початку або після кінця голосування. Для того, аби це не відбувалося, в самому форматі

повідомлення, а також в квитанції, вбудовано часові мітки, які використовуються для визначення часу, коли дані були створені та сформовані.

Важливо зазначити, що ці часові мітки є простими текстовими рядками,

4.1.9. Створення бюлетенів з однаковими токенами

Під час створення та підписання бюлетеня клієнти самостійно створюють токени, використовуючи криптографічно стійкі джерела випадковості. Оскільки клієнти здатні обрати будь-яке значення під час підписання бюлетеню, і сервер, за побудовою системи як такої, не має (і ніколи не має мати) відомості про токен, який клієнт намагається підписати, нічого не заважає зловмиснику використати цей самий токен для того, аби пройти процедуру підписання бюлетеня. Оскільки використання випадкового значення засліплення зловмисник майже гарантовано матиме іншу версію засліпленого бюлетеня, він може пройти процедуру підписання бюлетеня. Після зняття засліплення з підписаного бюлетеня, ми отримаємо ситуацію, в якій дві особи мають підписаний бюлетень, який відповідає одному і тому самому токену. Це буде значити, що зловмисник може змінити голос жертви навіть без її відома.

Для уникнення такої ситуації відповідальність за збереження секретності токену покладається виключно на користувачів. Користувачі мають розуміти важливість тримання значень токену та засліплення у секреті для уникнення подібних інцидентів.

4.1.10. Захищеність від DDoS-атак

DDoS (Distributed Denial of Service) — це тип атаки на інформаційні та комунікаційні системи, під час якої велику кількість запитів надсилають одночасно з кількох різних джерел, щоб вичерпати ресурси системи та порушити роботу легітимних користувачів.

Для захисту від DDoS-атак використовується кілька основних методів. Один із них полягає у створенні інформаційно-комунікаційної системи, здатної обробляти запити, що значно перевищують типовий обсяг запитів за певний період часу. Якщо

зловмисник не зможе вичерпати ресурси системи під час досить великої атаки, то система може бути захищена від DDoS-атак.

Інший метод — контроль запитів, які клієнти можуть надсилати в інформаційно-комунікаційну систему. Наприклад, підрахунок кількості запитів певного типу, отриманих з одного джерела (наприклад, з однієї IP або MAC-адреси, або з використанням інших джерел для отримання даних і відстеження користувачів). Якщо кількість запитів за певний період часу перевищує допустиму межу, усі наступні запити автоматично блокуються. Це обмежує доступ порушників до ресурсів інформаційно-комунікаційних систем і запобігає необмеженому виснаженню ресурсів.

В розробленій системі електронного голосування запроваджено наступні обмеження:

— Не більше 20 успішних спроб голосування з використанням одного бюлетеня на добу.

— Не більше 100 спроб, не важливо, успішних чи ні, з використанням одного бюлетеня, на добу.

— Не більше 10 спроб створення та підписання бюлетеня від однієї особи на добу.

— Не більше 200 запитів до сервера щодо створення, використання, або анулювання бюлетеня, з однієї IP-адреси на добу.

Ці обмеження цілком прийнятні для звичайного користування і не мають обмежувати звичайних користувачів у можливості використовувати запропоновану систему. У разі, якщо з якихось причин ці обмеження виявляться занадто жорсткими, система надає можливість розробникам вручну змінити ці параметри в режимі реального часу.

4.1.11. Відсутність знання про невикористані бюлетені

Розроблена система захищеного електронного голосування не має гарантій відносно того, що створений і підписаний електронний бюлетень буде обов’язково використаний під час голосування. Оскільки ми не знаємо, які саме бюлетені

залишились невикористаними, це створює потенційну проблему, яка полягає у тому, що кількість квитанцій про видачу бюлетеня може вийти значно більшою, ніж кількість бюлетенів, використаних під час голосування. Оскільки ми не знаємо, які конкретно бюлетені входять в цю різницю, нічого не заважає державі створити нові, фіктивні бюлетені, і використати їх для впливу на результати голосування.

Для цієї проблеми поки що не знайдено математичної моделі вирішення. Замість цього в системі встановлено організаційні рішення, які мають на меті зменшення впливу цієї проблеми до такого рівня, який нівелює можливість використання цієї вразливості для успішного впливу на результати голосування. Клієнтське програмне забезпечення рекомендується створити таким чином, аби воно автоматично відправляло «пустий» голос після завершення строку голосування. Це дозволяє серверу зменшити простір можливих токенів, які не були використані під час голосування.

4.1.12. Втрата електронного бюлетеня

Оскільки існує значна різниця у часі між створенням бюлетеня та його використанням під час голосування, існує ймовірність того, що користувач втратить доступ до свого токену і засліплення, таким чином втративши можливість прийняти участь в електронному голосуванні, та в голосуванні загалом.

Для цього необхідно створити можливість користувачам зробити резервну копію своїх голосів. Така система має бути максимально зручною; в ідеалі — автоматичною, але з можливістю створення додаткових резервних копій вручну, у тому числі з можливістю експорту та імпорту цих даних.

4.2. Вибір еліптичної кривої

4.2.1. Крива secp256k1

Крива secp256k1 — це крива Кобліца з рівнянням $y\hat{}2 = x\hat{}3 + 7$. Ця крива була створена в той час, коли ще не було Curve25519, а кривій NIST не довіряли. Згідно з рекомендаціями SECG [28], єдиною можливою альтернативою було використання

кривої Кобліца. Крива secp256k1 майже виключно використовується в криптовалютах, і її застосування не зазнало значного впливу з боку незалежних наглядових органів або експертів. Існуючі реалізації досить повільні, не оптимізовані, не гарантовано працюють протягом певного періоду часу і мають велику кількість вразливостей.

Використання цієї кривої не рекомендується через недоліки безпеки та продуктивності. Крива secp256k1 призначені для 128-бітних рівнів безпеки, але існують більш безпечні та ефективні альтернативи, такі як Curve25519.

4.2.2. Криві NIST

Криві secp256r1, secp384r1 та secp521r1 були розроблені Національним інститутом стандартів і технологій (NIST) для криптографічних операцій. Однак безпеку цих кривих неможливо перевірити, оскільки NIST не надав жодних доказів того, що параметри еліптичних кривих обрані випадковим чином. Тому багато дослідників в області криптографічної безпеки рекомендують не використовувати ці еліптичні криві, оскільки можливі вразливості, навмисно введені NIST, можуть спотворити безпеку використання цих кривих і призвести до компрометації інформації.

Криві secp256r1, secp384r1 і secp521r1 були створені на початку розвитку криптографії еліптичних кривих, тому їм бракує багатьох гарантій безпеки більш пізніх розробок і вони вимагають особливої обережності при застосуванні. До 2015 року алгоритму додавання і множення кривих Вейєрштрасса з фіксованим часом і досконалого алгоритму (тобто такого, що працює для всіх можливих значень вхідних змінних) не існувало [29]. Однак зараз існують формули, які дозволяють побудувати алгоритми, що працюють у постійному часі, і безпека цих кривих не менша, ніж у кривих Curve25519. Однак криві Curve25519 все одно значно швидші і мають вищий ступінь захисту від помилок при реалізації проекту.

Криві secp256r1, secp384r1 та secp521r1 розраховані на 128-бітний, 192-бітний та 260-бітний рівні безпеки відповідно.

4.2.3. Curve25519

Curve25519 має рівняння $y^2 = x^3 + 486662x^2 + x$. Графік цієї функції зображено на рисунку .5.

Ця крива була створена не просто так. Форма кривої є еліптичною кривою Монтгомері, що надає цій кривій певних математичних властивостей, що підвищують безпечність та швидкодію систем на її основі. Значення $2^{255} - 19$, яке використовується як базис цієї кривої у двовимірному полі, є наближеним до степені двійки, причому такої, що вміщається в 256 біт. Більш того, завдяки тому, що воно вміщається у 255 біт, реалізації можуть уникнути проблем при використанні беззнакових числових змінних. Значення 486662, яке використано як коефіцієнт аргументу другого порядку, було використане через те, що це найменше додатне ціле значення, яке задовольняє низку критеріїв, які дозволяють нам уникнути проблем безпеки та полегшити реалізацію систем безпеки на основі даної кривої.

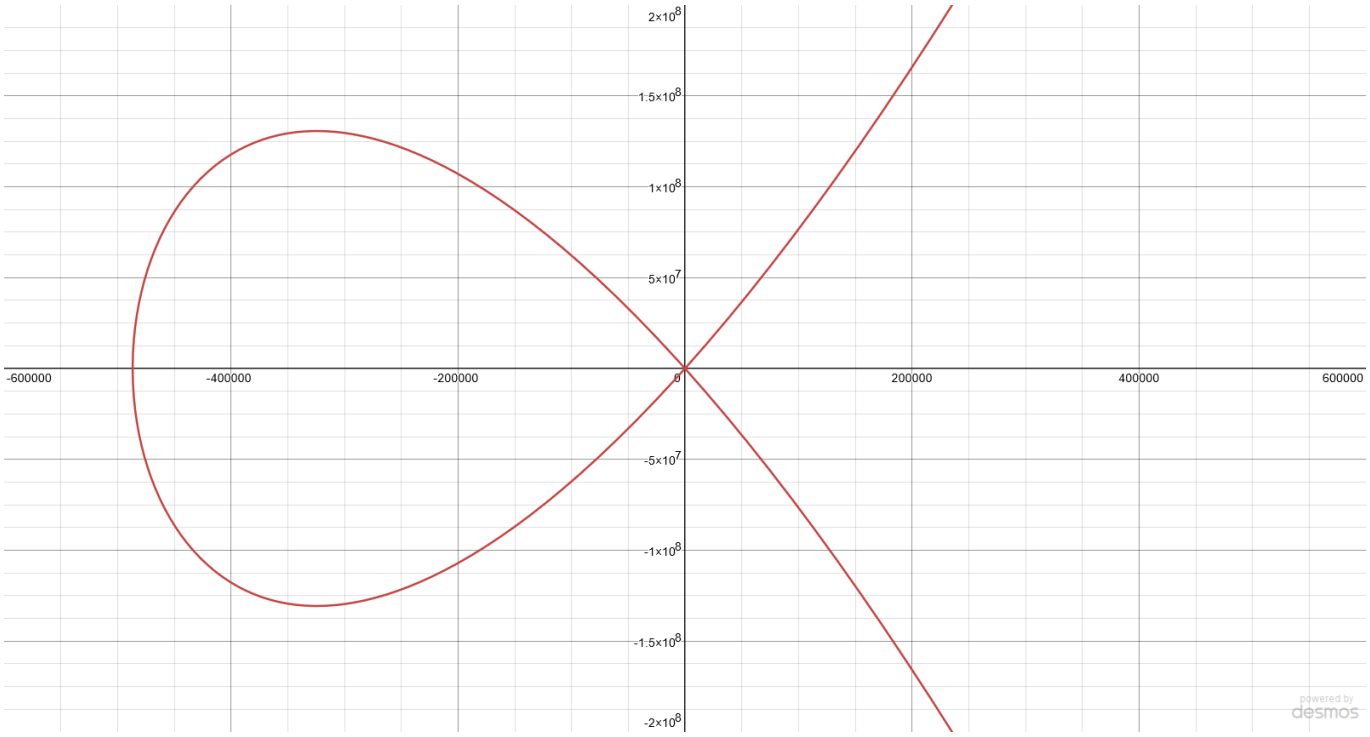


Рисунок 4.1 — Графік кривої Curve25519

Однією з властивостей даної кривої є те, що до неї можна передати будь-яке значення розміром 256 біт і бути впевненим у тому, що воно може бути досягнутим

перетвореннями базисної точки. Це дозволяє уникнути перевірки на придатність значення кривій, а значить, практично полегшує використання даної кривої у системах безпеки.

Ця еліптична крива використовується в алгоритмі Ed25519. Цей алгоритм затверджений для використання в Україні згідно стандарту ДСТУ 9041:2020 [30], і має заявлений рівень безпеки у 128 біт.

4.2.4. Curve448

Крива Curve448 побудована за тим самим принципом, що й крива Curve25519, і базується на полі $2^{448} - 2^{224} - 1$. Вона має рівняння $y^2 + x^2 = 1 - 39081x^2y^2$. За аналогією, форма кривої Curve448, її базис, та числовий параметр 39081, обрані спеціально для того, аби реалізації могли уникнути багатьох математичних проблем безпеки, зайвих перевірок, які тільки ускладнюють використання еліптичної кривої в системі безпеки, та мати можливість використовувати швидке множення за Каратсубою.

У порівнянні з кривою Curve25519, арифметичні операції на кривій Curve448 мають значно більшу обчислювальну складність, через що її реалізації є значно повільнішими. Ця крива може використовуватися для забезпечення безпеки на рівні 224 біти.

4.2.5. Ristretto255

Ristretto Group є математичною абстракцією, яка застосовується до кривих з базисом 4 або 8, таких як Curve25519 [31]. Ця абстракція дозволяє ефективно перетворювати такі криві в еліптичні криві з базисом 1, забезпечуючи додаткові гарантії безпеки та спрощуючи реалізацію необхідних алгоритмів. Оскільки вона є надбудовою над кривою Curve25519, вона має такий самий рівень безпеки: 128 біт.

Ristretto255 є спеціалізованою реалізацією протоколу Ristretto на основі кривої Curve25519. Протокол Ristretto зберігає властивості своєї базової кривої та додає додаткові гарантії безпеки без значних обчислювальних накладних витрат, тому його

використання практично не впливає на швидкодію. Однією з проблем є те, що через низьку популярність даного підходу, кількість розробленого програмного забезпечення та бібліотек, що підтримують протокол Ristretto є значно меншою у порівнянні з іншими запропонованими кривими. Це не є значною проблемою, оскільки для реалізації системи у будь-якому випадку розробникам доведеться створювати програмне забезпечення самостійно. На сайті протоколу існують тестові вектори та приклади реалізації протоколу, що дозволяє полегшити процес розробки та підтвердити справність створеного коду.

Ristretto використовує ідею, схожу на ту, що була запропонована в [32], яка полягає в використанні не-простої порядку кривої EE для реалізації простої порядку групи шляхом конструювання фактор-групи. Проте, Ristretto використовує інші формули, щоб дозволити використання кофактор-88 кривих, таких як Curve25519.

Внутрішньо, Ristretto точка представлена як точка Едвардса. Дві точки Едвардса P, Q можуть представляти одну і ту ж точку Ristretto, так само як різні проективні координати X, Y, Z можуть представляти одну і ту ж точку Едвардса. Групові операції над точками Ristretto виконуються без додаткових витрат, виконуючи операції над відповідними точками Едвардса.

Для цього, Ristretto визначає:

— новий тип для точок Ristretto, який містить відповідну точку Едвардса;

— рівність для точок Ristretto, таку що всі еквівалентні представники вважаються рівними;

— функцію кодування для точок Ristretto, таку що всі еквівалентні представники кодуються як однакові бітові рядки;

— функцію декодування бітових рядків з вбудованою перевіркою, таку що приймаються лише канонічні кодування дійсних точок;

— відображення з бітових рядків у точки Ristretto, придатне для операцій hash-to-point.

Отже, існуюча реалізація кривої Едвардса може реалізувати правильну абстракцію для складних протоколів, просто додавши новий тип та три або чотири

функції. Крім того, перевірка рівності для групи Ristretto насправді дешевша, ніж перевірка рівності для базової кривої.

4.3. Вибір криптографічно стійкої функції хешування

При використанні в якості вхідних параметрів еліптичних кривих, що застосовуються в додатках, рекомендується використовувати хеш-функцію SHA-256 або іншу функцію сімейства SHA-2 або SHA-3, що підходить для необхідної задачі Функція SHA-2 є криптографічно стійкою хеш-функцією, яка є швидкою і надійною у використанні. широко використовується. Під час дослідження цих функцій не було знайдено жодної інформації про колізії, а успішне виявлення колізії вважалося б шокуючим відкриттям.

Для розробленої системи електронного голосування було обрано функцію SHA2-256, як таку, що існує в стандартах України та широко розповсюджену для використання у всьому світі для криптографічних потреб.

4.4. Вибір еліптичної кривої

Для забезпечення належного рівня безпеки та найкращої продуктивності рекомендується використовувати еліптичну криву Curve25519; еліптична крива Curve25519 була спеціально створена з урахуванням багатьох проблем, з якими можуть зіткнутися розробники арифметичних та обчислювальних додатків цієї еліптичної кривої.

Якщо потрібен вищий рівень безпеки і ризик вразливості не є проблемою, рекомендується використовувати криву Curve448.

Запропонована схема безпечного електронного голосування не залежить від параметрів базової кривої і тому може бути використана з будь-якою кривою. Якщо у вимогах до реалізації існують явні обмеження на криві, які можуть бути використані, достатньо враховувати ці обмеження при виборі кривих, на яких базуватиметься запропонована реалізація безпечного методу електронного голосування.

Для запропонованої системи обрано криву Ristretto255, оскільки вона є зрозумілою та простою математичною надбудовою над вже існуючою та прийнятою як державний стандарт кривої Curve25519, що використовується в стандарті ДСТУ 9041:2020 [30].

4.5. Вибір алгоритму електронного підпису на основі еліптичної кривої

Для використання в українських державних справах існує стандарт ДСТУ 4145:2015, який встановлює норми для еліптичних кривих, рекомендованих для використання в криптографічних роботах у законодавчій сфері в Україні.

Якщо вибір алгоритму ЕЦП на основі еліптичних кривих не обмежений законодавчими вимогами або іншими стандартами, рекомендується використовувати алгоритм Ed25519. Цей алгоритм заснований на запропонованій еліптичній кривій Curve25519 і забезпечує надійний захист з якомога меншою кількістю граничних ситуацій і вразливостей, які можуть виникнути в разі некоректної реалізації.

Алгоритм ECDSA не рекомендується через велику кількість вразливостей, які можуть виникнути в разі некоректної реалізації, можливість атак побічних каналів, використання еліптичної кривої, яка не рекомендується як основа цього алгоритму, а також можливе використання застарілих функцій криптографічно стійкої хеш-функції SHA-1. Не рекомендується через наявність знайдених вразливостей та атак. По можливості слід відмовитися від цього алгоритму на користь Ed25519.

Якщо необхідно використовувати алгоритм цифрового підпису на основі еліптичної кривої з рівнем безпеки вище 128 біт, рекомендується використовувати алгоритм Ed448. Цей алгоритм має ті ж властивості безпеки, що і алгоритм Ed25519, але спрямований на рівень безпеки 224 біт.

Для розробленої системи обрано алгоритм шифрування Ed25519, також відомий як ДСТУ 9041:2020 [30].

Висновки по розділу 4

Розроблену електронну систему голосування було проаналізовано на предмет потенційних загроз безпеці та обговорено заходи щодо їх пом’якшення. Однією з головних проблем у системах електронного голосування є запобігання дублюванню бюлетенів, чого можна досягти, якщо виборці подають лише жетони замість справжніх бюлетенів під час процесу перевірки голосування. Іншою проблемою є забезпечення анонімності виборців, яку можна вирішити за допомогою процедур засліплення, які унеможливлюють серверу пов’язати голосування з конкретним виборцем. Система також повинна вести облік виданих бюлетенів і перевіряти, чи особа, яка отримує бюлетень, має на нього право. Це досягається за допомогою процесу отримання, який генерує унікальний ідентифікатор для кожного бюлетеня, який можна використовувати для підтвердження того, що бюлетень було створено для конкретних виборів і не може використовуватися для будь-яких інших цілей. Використання засліплених електронних голосів гарантує, що сервер не зможе зв’язати копію електронного голосування без засліплених очей із особою, яка його створила, але оскільки засліплення має бути таємним і лише виборець із засліпленими очима може скасувати голосування, це можна визначити, хто має право скасувати голосування та створити інше голосування. Використання мітки часу дозволяє чітко ідентифікувати та перевірити час, коли було подано запит на підпис у бюлетені для голосування. Коли виборець отримує квитанцію, єдиними невідомими цінностями є підпис, надрукований на квитанції, і вартість виборчого бюлетеня, підписаного засліпленими очима. Тому, коли виборець підписує цю квитанцію, це не більше ніж випадкове значення, яке використовується сервером як тест для перевірки автентичності особи виборця. Оскільки значення, підписане виборцем, неможливо відрізнити від випадкового значення, ймовірність того, що це значення вже було підписано виборцем і зловмисник використовує наявний підпис для отримання бюлетеня, надзвичайно низька. При цьому виборець після підпису може переконатися в автентичності підписаної цінності та підтвердити, що підписана цінність справді є квитанцією. Система також має захищати від потенційних атак, таких як відстеження

голосів, підробка бюлетенів за державну підтримку, зловмисне анулювання бюлетенів інших людей і перехоплення бюлетенів під час використання. Їх можна вирішити за допомогою таких заходів, як підтвердження дискретної логарифмічної еквівалентності, публікація копій електронних бюлетенів із сліпим підписом та інформації про їх отримання, надання квитанції, яка підтверджує успішне створення, підписання та отримання бюлетеня, використання хеш-функції для генерації код автентифікації повідомлення та використання безпечного каналу для передачі інформації.

ВИСНОВКИ

У кваліфікаційній роботі на здобуття освітнього ступеня магістра було розроблено систему безпечного електронного голосування, яку можливо використовувати в Україні, забезпечуючи можливість вільного та доступного волевиявлення для кожного, у кого є доступ до смартфону або іншого девайсу, здатного отримувати доступ до мережі Інтернет, шляхом використання методу наукової абстракції, індукції та дедукції, аналізу, синтезу, структурування, та алгоритмізації.

У першому розділі було досліджено поняття голосування як такого, а також його соціальну важливість та роль у суспільстві. Було розглянуто різні форми правління та те, як здатність волевиявлення громадян впливає на розвиток суспільства, різні форми демократії (пряму та представницьку), їх переваги та недоліки, можливі проблеми, важливі моменти, та потенційні рішення цих проблем. Це дослідження дозволяє сформулювати соціальну важливість цього дослідження та розглянути, як вплив на цей процес може мати сприятливі ефекти на розвиток державності та спільноти.

У другому розділі було досліджено існуючі системи електронного голосування в інших країнах, а також існуюче та потенційне законодавство та законотворчість на теренах України. Серед розглянутих країн були представлені Швейцарія, США, Австралія, та Естонія, кожна з яких по-різному підійшла до розв’язання задачі створення безпечної системи електронного голосування для своїх громадян. Деякі країни, такі як США, по факту використовують електронні обчислювальні системи виключно для сприяння процесу голосування та допомоги людям з інвалідністю під час їх волевиявлення. Інші країни створили повноцінні цифровізовані державні системи, які дозволяють їм безпечно та ефективно проводити процес голосування в електронній формі.

У третьому розділі було проведено дослідження математичних примітив і структур, які були використані при розробці системи безпечного електронного голосування в Україні, про що також було викладено у цьому розділі. Було розглянуто

конкретні рішення щодо забезпечення одночасної анонімності окремих користувачів під час використання системи та звітності системи загалом як такої.

У четвертому розділі було розглянуто потенційні атаки та зловмисні дії, які можуть бути вчинені проти системи, та рішення, які були прийняті для їх усунення, знешкодження, або щонайменше мінімізування. Було проведено аналіз векторів атаки, які розглядалися під час розроблення системи безпечного електронного голосування в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Smelser N.J. Theory of collective behavior. New York: The Free Press of Glencoe, 1963.
2. Карасевич А.О., Шачковська Л.С. Політологічна енциклопедія. 2nd ed. Умань. 2016.
3. Кочубей Л. Голосування // Політична енциклопедія. Парламентське видавництво, 2011.
4. Fuchs D., Roller E. Learned Democracy? Support for Democracy in Central and Eastern Europe // International Journal of Sociology. 2006. No. 36. pp. 70-96.
5. Верховна Рада України. Проект Закону про Концепцію "Запровадження системи електронного голосування в Україні" 2011. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=40636 (дата звернення: 08.02.2024).
6. Верховна Рада України. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації 2017. URL: https://zakon.rada.gov.ua/laws/show/797-2017-%D1%80#Text (дата звернення: 29.01.2024).
7. Anonymous. Governance // Wikipedia. 2024. URL: https://en.wikipedia.org/wiki/Governance (дата звернення: 18.03.2024).
8. J. Ober K.R.R.W.W. Origins of Democracy in Ancient Greece. University of California Press, 2007.
9. Wikipedia. Electronic voting in the United States URL: https://en.wikipedia.org/wiki/Electronic_voting_in_the_United_States (дата звернення: 04.05.2024).
10. U.S. Election Assistance Commission. Voluntary Voting System Guidelines URL: https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines (дата звернення: 04.05.2024).

11. Cohn J. What is the latest threat to democracy? // Medium. 2018. URL: https://medium.com/@jennycohn1/what-is-the-latest-threat-to-democracy-ballot-marking-devices-a-k-a-electronic-pencils-16bb44917edd (дата звернення: 17.03.2024).
12. Bernhard M., McDonald A., Meng H., Hwa J., Bajaj N., Chang K., Halderman J.A. Can Voters Detect Malicious Manipulation of Ballot Marking Devices? San Francisco: 41st IEEE Symposium on Security and Privacy, 2020.
13. Perez E., London J., Miller G. Georgia State Election Technology Acquisition, Assessing Recent Legislation in Light of Planned Procurement // OSET Institute. 2019. URL: https://trustthevote.org/wp-content/uploads/2019/03/29Mar19-OSETBriefing_GeorgiaTechAcquisitionAnalysisFinal.pdf (дата звернення: 01.03.2024).
14. F. Hao P.Y.A.R. Real-World Electronic Voting: Design, Analysis and Deployment. CRC Press, 2016.
15. Davidson A. Privacy Pass - “The Math” // Cloudflare Blog. 2017. URL: https://blog.cloudflare.com/privacy-pass-the-math (дата звернення: 09.04.2024).
16. Google/Harris. Online Security Survey // Google Services. 2019. URL: https://services.google.com/fh/files/blogs/google_security_infographic.pdf (дата звернення: 18.04.2024).
17. Turner D.M. Qualified Electronic Signatures For eIDAS // Cryptomathic. 2016. URL: http://www.cryptomathic.com/news-events/blog/qualified-electronic-signatures-for-eidas (дата звернення: 13.07.2016).
18. Bundesnetzagentur. Qualified Electronic Signature // Bundesnetzagentur. 2016. URL: http://www.bundesnetzagentur.de/EN/Service-Funktionen/QualifizierteelektronischeSignatur/qualifizierteelektronischesignatur-node.html (дата звернення: 13.07.2016).
19. Верховна Рада України. Про електронні документи та електронний документообіг // Законодавство України. 2022. URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 02.03.2024).

20. Верховна Рада України. Конституція України // Сайт Верховної Ради України. 1996. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр/conv#n4394 (дата звернення: 13.02.2024).
21. International Organization for Standardization. ISO/IEC 21778:2017 — Information technology — The JSON data interchange syntax 2017. URL: https://www.iso.org/standard/71616.html (дата звернення: 16.03.2024).
22. International Organization for Standardization. ISO 8601 — Date and time format 2019. URL: https://www.iso.org/iso-8601-date-and-time-format.html (дата звернення: 13.04.2024).
23. Josefsson S. RFC 4648 — The Base16, Base32, and Base64 Data Encodings // IETF DataTracker. 2006. URL: https://datatracker.ietf.org/doc/html/rfc4648#section-5 (дата звернення: 28.04.2024).
24. Anonymous. Year 2038 Problem // Wikipedia. 2024. URL: https://en.wikipedia.org/wiki/Year_2038_problem (дата звернення: 02.05.2024).
25. Anonymous. Fault tolerance // Wikipedia. 2024. URL: https://en.wikipedia.org/wiki/Fault_tolerance (дата звернення: 28.02.2024).
26. Kotov M., Toliupa S., та Nakonechnyi V., "REPLICA STATE DISCOVERY PROTOCOL BASED ON ADVANCED MESSAGE QUEUING PROTOCOL," // Cybersecurity: Education, Science, Technique, 2024.
27. Верховна Рада України. Закон України "Про державний реєстр виборців" 2007. URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=698-16#Text (дата звернення: 18.03.2024).
28. Certicom Corp. Standards for Efficient Cryptography 2 (SEC 2) // Standards for Efficient Cryptography Group. 2010. URL: Standards for Efficient Cryptography 2 (SEC 2) (дата звернення: 02.05.2024).
29. Renes J., Costello C., Batina L. Complete addition formulas for prime order elliptic curves // Cryptology ePrint Archive. 2015. URL: https://eprint.iacr.org/2015/1060 (дата звернення: 05.02.2024).

30. Технічний комітет стандартизації «Інформаційні технології» (ТК 20). ДСТУ 9041:2020 Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса. Київ: ДП «УкрНДНЦ», 2020.
31. The Ristretto Group. 2018. URL: https://ristretto.group/ (дата звернення: 29.04.2024).
32. Hamburg M. Decaf: Eliminating cofactors through point compression // 35th International Cryptology Conference. Santa Barbara. 2015.
33. Карасевич А.О., Шачковська Л.С. Демократія. Т. 2. // В кн.: Політологічна енциклопедія / ред. Карасевич А.О., Шачковська Л.С. Умань. 2016. С. 227-236.
34. Шаталов. О, Кочубінський А, редактори. ДСТУ 4145:2002 — Криптографічний захист інформації цифровий підпис, що ґрунтується на еліптичних кривих, Формування та перевіряння. Київ: Державний комітет України з питань технічного регулювання та споживчої політики, 2003.
35. Bernstein D.J. Curve25519: new Diffie-Hellman speed records // Public key cryptography—PKC 2006, 9th international conference on theory and practice in public-key cryptography. New York. 2006. Vol. 3958. pp. 207–228.
36. Menezes A. The Elliptic Curve Discrete Logarithm Problem: State of the Art // Advances in Information and Computer Security, Third International Workshop on Security, IWSEC. Kagawa, Japan. 2008.
37. Adamson I.T. Introduction to Field Theory. 2nd ed. Mineola, N.Y: Dover Publications, 2007.
38. Allenby R. Rings Fields And Groups An Introduction To Abstract Algebra. 1st ed. Butterworth-Heinemann, 1991.
39. Blake I., Seroussi G., та Smart N. Elliptic Curves in Cryptography. Cambridge University Press, 2000.
40. Brown E., "Three Fermat Trails to Elliptic Curves," // The College Mathematics Journal, № 31, 2000. С. 162–172.

41. Crandall R., Pomerance C. Elliptic Curve Arithmetic // В кн.: Prime Numbers: A Computational Perspective. Springer-Verlag, 2001. С. 285–352.
42. Johnson D., Menezes A., Vanstone S., "The Elliptic Curve Digital Signature Algorithm (ECDSA)," // International Journal of Information Security, Т. 1, № 1, August 2001. С. 36–63.
43. Josefsson S., Liusvaara I. Edwards-Curve Digital Signature Algorithm (EdDSA) // Internet Engineering Task Force. 2017. URL: https://datatracker.ietf.org/doc/html/rfc8032 (дата звернення: 31.07.2017).
44. NIST. FIPS 186-5 (Draft): Digital Signature Standard (DSS) // NIST. 2019. URL: https://csrc.nist.gov/publications/detail/fips/186/5/draft (дата звернення: 23.07.2020).
45. Bernstein D.J., Lange T. ECDLP Security: Rho // SafeCurves: choosing safe curves for elliptic-curve cryptography. 2013. URL: https://safecurves.cr.yp.to/rho.html (дата звернення: 16.11.2016).
46. Johnson D і Menezes A, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," CiteSeerX 10.1.1.38.8014, 1999.
47. Cendyne. A Deep dive into Ed25519 Signatures 2022. URL: https://cendyne.dev/posts/2022-03-06-ed25519-signatures.html (дата звернення: 22.03.2024).
48. Bernstein D.J. Cryptography in NaCl. 2009. URL: https://cr.yp.to/papers.html#naclcrypto (дата звернення: 23.04.2024).
49. Hamburg M. Ed448-Goldilocks, a new elliptic curve // Cryptology ePrint Archive. 2015. URL: https://eprint.iacr.org/2015/625 (дата звернення: 17.05.2024).
50. Bernstein D.J., Josefsson S., Lange T., Schwabe P., Yang B.Y. EdDSA for more curves. 2015. URL: https://cr.yp.to/papers.html#eddsa (дата звернення: 28.04.2024).
51. Norwegian Ministry of Foreign Affairs. Feasibility study on Internet Voting for the Central Electoral Commission of the Republic of Moldova 2016. URL: https://www1.undp.org/content/dam/moldova/docs/Publications/MD-IVOTE-FS-and-Roadmap_cleanENG.pdf (дата звернення: 28.04.2024).

52. Soatok. Guidance for Choosing an Elliptic Curve Signature Algorithm in 2022 // Dhole Moments. 2022. URL: https://soatok.blog/2022/05/19/guidance-for-choosing-an-elliptic-curve-signature-algorithm-in-2022/ (дата звернення: 29.03.2024).
53. Krawczyk H., Bellare M., Canetti R. HMAC: Keyed-Hashing for Message Authentication, RFC 2104 // Internet Engineering Task Force. 1997. URL: https://datatracker.ietf.org/doc/html/rfc2104 (дата звернення: 29.04.2024).
54. e-Estonia. i-Voting 2019. URL: https://e-estonia.com/wp-content/uploads/2019aug-facts-a4-v02-i-voting.pdf (дата звернення: 08.03.2024).
55. Buchanan B. Non-interactive Zero-Knowledge Proof of Discrete Log Equality // Medium. 2021. URL: https://billatnapier.medium.com/non-interactive-zero-knowledge-proof-of-discrete-log-quality-f6f543d2ba2e (дата звернення: 21.03.2024).
56. Davidson A., Goldberg I., Sullivan N., Tankersley G., Valsorda F. Privacy Pass 2018. URL: https://github.com/privacypass/protocol (дата звернення: 30.03.2024).
57. Національна академія внутрішніх справ. Конституційне право України. ТЕМА 6. НАРОДНЕ ВОЛЕВИЯВЛЕННЯ. // Національна академія внутрішніх справ. 2020. URL: https://arm.naiau.kiev.ua/books/konst_pu/rozdil/rozdil6.html (дата звернення: 18.02.2024).
58. Верховна Рада України. Про основні засади забезпечення кібербезпеки України 2021. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 08.02.2024).