

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

ФІЛОСОФСЬКИЙ ФАКУЛЬТЕТ

КАФЕДРА ПОЛІТОЛОГІЇ

Пояснювальна записка

до кваліфікаційної роботи першого (бакалаврського) рівня вищої освіти на тему:

Інтернет-голосування: світовий досвід та перспективи впровадження в Україні

Виконала: студентка IV курсу,
групи ФФІ-41с
спеціальності «052 Політологія»
Карапуз О. О.

Науковий керівник:
д.політ.наук, проф. Романюк А. С.

Рецензент:
д.політ.наук, проф. Шипунов Г.В.

Львів – 2022 р.

Список скорочень та абревіатур:

ДВК — дільнична виборча комісія

ОВК — обласна виборча комісія

PKI — інфраструктура відкритих ключів

DRE — електронна машина для голосування з прямим записом

OMR — система голосування з оптичним скануванням

VVPAT або VPR — система прямого електронного голосування з паперовим слідом

CAPTCHA — комп'ютерний тест, який використовується для того, щоб визначити, хто використовує систему — людина чи комп'ютер

RSA — криптографічний алгоритм з відкритим ключем

ЗМІСТ

ВСТУП.....	4
Розділ 1. Теоретичні засади вивчення електронного та інтернет-голосування	8
1.1. Явище голосування: підходи до визначення.....	8
1.2. Електронне голосування: концептуальні підходи та класифікація .	11
1.3. Інтернет-голосування: концептуальне визначення та технології забезпечення	16
1.4. Технології захисту інтернет-голосування	25
Розділ 2. Практика застосування інтернет-голосування.	30
2.1. Досвід використання інтернет-голосування в Естонії, Австралії, Канаді та Швейцарії.....	30
2.2. Загрози зовнішнього втручання у інтернет-вибори: досвід Нідерландів, Британії та Франції	40
2.3. Інтернет-голосування у недемократичних державах: приклад Російської Федерації.....	47
Висновки	52
Список використаної літератури	54

ВСТУП

Актуальність дослідження. Через війну в Україні приблизно 5 млн громадян були змушені покинути країну. Гуманітарна криза та зруйнована інфраструктура, у тому числі житлова (за даними KSE, на кінець квітня вартість втрат житлових будинків сягає 28 млрд дол.), дає підстави говорити про те, що після закінчення війни більшість з цих людей одразу не повернуться в Україну. Цей факт змушує до пошуків шляхів для забезпечення цій категорії громадян можливість брати участь у виборчому процесі в Україні.

Зважаючи на катастрофічні економічні наслідки через війну з Росією, (за різними оцінками, у середньому Україна втратила 35% ВВП), інтернет-голосування могло б допомогти з оптимізацією грошових витрат через виключення логістичних питань, утримання діляниць, друк виборчих бюлетенів та зарплатні для членів ДВК та ОВК. Також питання про можливість впровадження інтернет-голосування варто розглянути у контексті оптимізації часу на процес голосування та встановлення результатів, що є особливо актуальним зважаючи на останні зміни виборчої системи на місцевих та виборах до Верховної Ради (пропорційна та мажоритарна відносної більшості для місцевих та пропорційна система з відкритими виборчими списками для депутатів ВР).

Окрім того, в українській політичній науці відсутній всебічний аналіз успішного досвіду впровадження інтернет-голосування. Ця робота спроба

систематизувати українські та зарубіжні наукові доробки та порівняти у вітчизняній науці досвід світовий інтернет-голосування.

Об'єкт дослідження: процес голосування у зарубіжних країнах. **Предмет дослідження:** використання інтернет-технологій у виборчому процесі зарубіжних країн.

Мета роботи: дослідити існуючі практики інтернет-голосування у світі, визначити їх позитивні та негативні параметри та визначити можливості використання під час виборів в Україні. На цій підставі нашими завданнями виступають:

1. Визначити поняття «електронне голосування», його класифікацію та види;
2. Визначити поняття інтернет-голосування та його відмінні від електронного-голосування ознаки;
3. Проаналізувати можливі проблеми використання інтернет-голосування та методи захисту від фітсифікацій і зовнішніх втручань;
4. Проаналізувати методи, правила, досвід та можливі проблеми використання інтернету під час голосування та підрахунку голосів у зарубіжних країнах.

У цій роботі були використані наступні **методи дослідження:** порівняння, аналіз, синтез, абстрагування, узагальнення та моделювання.

Структура роботи. Робота складається зі вступу, двох розділів (перший розділ містить чотири структурних підрозділи, другий – три підрозділи), висновків та

списку використаних джерел. Загальний обсяг роботи становить 58 сторінок, а список використаних джерел представлений 29 позиціями, в тому числі присутня англомовні джерела.

Огляд літератури. Серед наукових доробків майже відсутній всебічний аналіз досвіду інтернет-голосування у світі. Окремо дослідники розглядають найбільш успішні випадки впровадження голосування в інтернеті. Найбільше у цьому плані ми зустрічили роботи щодо аналізу функціонування інтернет-голосування в Естонії. У цьому плані дослідження проводили такі науковці, як В. Чуприн, В. Вишняков, М. Пригара, які аналізували аспекти функціонування інтернет-голосування у країні [13]. Дослідник Х. Кохалик у своїх працях аналізує досвід інтернет-голосування на виборах в Естонії на прикладі останніх виборів [9]. Докторка політичних наук Ярина Турчин у своїх працях аналізує, яким чиним використання інтернет-голосування в Естонії вплинуло на збільшення загальної явки на виборах.

Щодо інших країн, то українська дослідниця О.С. Корчагіна у своїх працях розглядала деякі аспекти інтернет-голосування у Швеції. Окремо варто ввідзнати праці аналітиків громадської мережі «ОПОРА», які аналізують проблеми використанні інтернет-голосування у Росії та описують принципи використання інтернет-технологій у виборчому процесі в Естонії, Швеції та США [3]. До цього часу інші країни в українському науковому дискурсі у контексті всебічного аналізу впровадження та функціонування інтернет-голосування не були проаналізовані.

Найбільш повний науковий доробок у сфері інтернет-голосування ми зустрічали у роботі міжнародного «Інституту демократії та електронних виборів» (IDEA), яка лягла в основу нашої наукової роботи. Водночас варто зазначити, що аналітики Інституту взяли до уваги не усі країни світу, де наразі функціонує інтернет-голосування [3]. Аналіз досвіду країн Швеції, Великобританії, Нідерландів та Франції ми проводили на основі зарубіжних наукових доробок та інформації виборчих комісій країн.

Розділ 1. Теоретичні засади вивчення електронного та інтернет-голосування

1.1. Явище голосування: підходи до визначення

Для подальшого аналізу явищ електронного- та інтернет-голосування варто першочергово пояснити визначення самого явища голосування.

Традиційно його розглядають, як одну із центральних стадій виборчого процесу. Водночас існують різні підходи до процедури голосування. Перший підхід — трактування голосування у широкому здійсненні. У цьому випадку поняття торкається усіх сфер, де застосовується процедура подачі та підрахунку голосів. Сюди, зокрема у розвинених демократіях відносять голосування у рамках інструментів місцевої демократії (бюджет участі, місцеві референдуми, засідання громадських рад тощо) [9, с. 1]

Інша частина дослідників визначають електронне голосування лише в рамках виборчого процесу. До прикладу, С.О. Сомова визначає голосування, як встановлену законом форму вираження волі виборця відносно самостійного визначення кожним з них бажаної перемоги на виборах того чи іншого кандидата. А. М. Колодій та В. Г. Князєв розглядають голосування, як безпосереднє волевиявлення виборців шляхом заповнення виборчих бюлетенів у спеціально відведених приміщеннях [12, с.188].

У цій роботі наша увага буде зосереджена на дослідженні голосування у вузчому значенні — як інструмент передачі влади й формування представницьких органів влади.

Організаційно голосування характеризується особливим колом суб'єктів, які беруть участь у цьому процесі. До таких, наприклад, за визначенням Фоміної С. В. відносять суб'єктів, що здійснюють безпосереднє волевиявлення, суб'єктів, що здійснюють організаційно-правове забезпечення умов реалізації волевиявлення, а також суб'єктів, що забезпечують зовнішньо-організаційне спостереження за волевиявленням та підведенням підсумків голосування. На практиці суб'єкти голосування — це самі виборці, спостерігачі, довірені та уповноважені особи та органи управління виборчим процесом (члени ДВК/ОВК).

Виборець — це особа, що підпадає під затверджені виборчі цензи конкретної території і на основі чого має право обирати представників на до першого органу влади. Кандидат на виборах — висунутий у встановленому законом порядку і зареєстрований виборчою комісією відповідного рівня претендент/тка на представницький мандат [11, с.8].

Члени виборчих комісій — це особи, які можуть брати участь в організації виборчого процесу, безперешкодно відвідувати всі приміщення, ознайомлюватися з усіма документами виборчої комісії, членом якої він є, та комісії нижчого рівня на відповідній території.

Виборчий ценз — це обмежувальні умови, відповідність яким є підставою для допуску (не допуску) громадян до участі у виборах. Основними виборчими цензами у сучасних країнах є віковий, ценз осілості, мовний, освітній, громадянства та судимості [6, с.1].

Спостерігач — це особа, що здійснює спостереження за голосуванням та підрахунком голосів. Спостерігачі можуть бути, як на офіційній основі, пройшовши необхідну процедуру акредитації, так і неофіційній. Офіційні спостерігачі можуть чинити вплив на перебіг виборчого процесу та його результати через запити, скарги та звіти за результатами [11, с. 9].

Виборчі бюлетні — офіційний документ для голосування на виборах, у якому виборець зазначає своє волевиявлення на підтримку окремих кандидатів та виборчих списків кандидатів, висунутих політичними партіями [11, с. 12].

У окремих зарубіжних країнах на стадії голосування беруть участь специфічні суб'єкти. Так, у Великобританії у день голосування можуть брати участь помічники кандидатів, які мають статус «лічильників», роль яких полягає в з'ясуванні реєстраційних номерів виборців без порушення таємниці голосування [11, с. 6].

Також існують позиції щодо місця голосування по відношенню до процесу виборів. Одна частина науковців ототожнює голосування із поняттям «виборчий процес», інша — розрізняє. На нашу думку, друге розуміння більш точно допомагає ідентифікувати та виокремити поняття голосування. У цьому випадку увагу варто приділити позиції С.Д. Князевій, що трактувала голосування як найбільш відповідальну стадію виборчого процесу, під час якої відбувається «розв'язка» всієї виборчої компанії. Підтримують та доповнюють цю тезу юристи, які акцентують увагу на юридичних наслідках цієї стадії. Фактично

вибори ніколи не можуть мати консультативний характер. Рішення, прийняте на голосуванні має обов'язковий характер. Це вирізняє цей процес від референдуму. Окрім того, голосування у контексті виборчого процесу обов'язково безпосередньо закріплюється нормами Конституції (Основного Закону) або конституційного законодавства [12, с.191].

1.2. Електронне голосування: концептуальні підходи та класифікація

Окремо варто розглянути позиції щодо розуміння процесу електронного голосування. У цьому випадку одна частина дослідників визначають електронне голосування лише як процес волевиявлення із використанням електронних засобів. Зокрема, у Рекомендаціях Комітету міністрів Ради Європи з правових, організаційних і технічних стандартів електронного голосування закріплено, що електронне голосування — це «електронні вибори, що включають використання електронних засобів, як мінімум, при подачі голосів». Інша — підходить до електронного голосування, як до комплексного процесу безпосередньо волевиявлення, підрахунку та друку або оприлюднення результатів з використанням комплексу цифрових технологій і систем автоматизації. З такої позиції електронне голосування розглядає дослідниця Н. Гусаревич [1, с. 8]. Саме це розуміння ми використовуватимемо і в нашій роботі.

По-різному визначають і поняття волевиявлення з позиції використання електронних засобів. У першому значенні до електронних виборів відносять голосування з використанням усього спектру інформаційно-комунікаційних

технологій. У цьому випадку електронне голосування визначають, як волевиявлення з використанням машин для голосування, які передбачають фізичну присутність у місці, де вони розташовані, а також з використанням засобів дистанційного голосування, у тому числі через інтернет. Радник із поліції та адвокації Європейського альянсу цифрового розвитку Дмитро Круткий трактує електронне волевиявлення як «голосування із застосуванням комп'ютерних та інтернет-технологій принаймні для голосування та підрахунку голосів» [9, с.9]. Дослідниці Садекова Г.У і Токарева Є.А. сюди також відносять голосування за допомогою мобільного зв'язку і мобільних телефонів [7, с. 4].

Інша частина дослідників визначають електронне-голосування, як окремий вид волевиявлення з використанням електронних засобів, яке проводиться лише у контрольованому середовищі. Натомість голосування з допомогою дистанційних засобів у неконтрольованому середовищі учені виділяють у окремий вид — інтернет-голосування. Як пояснюють експерти «Міжнародного інституту демократії та сприяння виборам», контрольоване середовище означає, що голосування проводиться в спеціально-оснащеному для цього приміщенні під наглядом офіційних спостерігачів та членів ДВК. Неконтрольоване середовище натомість означає, що виборець може проголосувати без нагляду та у будь-якому зручному для себе місці з доступом до інтернету [3, с.5].

На нашу думку, варто розділяти інтернет та електронне голосування як дві окремі форми волевиявлення із використанням дистанційних цифрових засобів, а також систем автоматизації.

Отже, електронне голосування — це процес волевиявлення, підрахунку, друку або оприлюднення результатів з використанням спеціальних систем автоматизації у контрольованому середовищі.

Зазвичай під електронним голосуванням мають на увазі голосування на спеціальній електронній машині прямого запису (direct recording electronic machines – DRE) [17, с.8]. Другий варіант поєднує у собі електронне та паперове голосування, коли виборець здійснює волевиявлення на папері, який потім сканують пристроєм для підрахунку голосів (Optical scanner recognition – OMR) [18, с.10].

У першому випадку немає потреби використовувати паперовий бюлетень для голосування, адже волевиявлення здійснюється шляхом прямого запису голосу за допомогою електронного дисплея, забезпеченого механічними або оптико-електронними компонентами, які може активувати виборець. При цьому голос виборця записується та обробляється за допомогою спеціального комп'ютера, підключеного до сенсорного екрана. Окрім цього, пристрій дозволяє зберігати всі голоси, підраховувати їх та передавати результати голосування з дільниць до центральних пунктів, а також попереджувати виборця про помилку під час заповнення бюлетеня. Всі голоси зберігаються в пам'яті комп'ютера, а тому будь-який перерахунок у разі виникнення неточностей здійснюється в електронному вигляді [7,с. 10].

Інший варіант цієї системи — пряме електронне голосування з паперовим слідом (voter-verified paper audit trail (VVPAT) або Verifiable Paper Record (VPR).

VVPAT - це метод надання зворотного зв'язку виборцям, які голосують з допомогою DRE. VVPAT працює таким чином, що після голосування виборець отримує видруковане паперове підтвердження того, що його голос був врахований. При цьому на видрукованому папері має міститись ім'я кандидата або партії, за яких віддано голос.

Такий спосіб допомагає підтвердити виборцям, що їхній голос був відданий правильно, виявити можливу фальсифікацію виборів або несправність, а також забезпечити засоби для перевірки збережених електронних результатів.

Залежно від виборчого законодавства паперовий контрольний лист може являтися законним бюлетенем і, отже, забезпечувати засіб, за допомогою якого можна провести ручний підрахунок голосів у разі необхідності повторного підрахунку голосів.

Таким чином голосування з використанням VVPAT застраховує від випадків людського втручання у записи машини для голосування з метою фальсифікації результатів волевиявлення або їх неправильного запису через механічне пошкодження пристрою.

Альтернативою голосуванню з DRE є голосування за допомогою системи оптичного розпізнавання міток (optical mark recognition – OMR).

Вона передбачає використання сканерів, що можуть розпізнати вибір громадянина на спеціальних виборчих бюлетенях, що піддаються автоматичному зчитуванню. Тобто, використання цієї системи передбачає заповнення паперового бюлетеня зі спеціальним захистом і печаткою виборцем та опускання

його лицьовою стороною донизу у пристрій, що сканує. Через таке поєднання деякі дослідники говорять, що цей вид електронного голосування доречніше віднести до паперово-електронної форми [1, с. 107].

За способом підрахунку системи OMR поділяються на центральні, коли виборчі бюлетені сканують і підраховують у спеціальних центрах підрахунку голосів та дільничні системи оптичного сканування й підрахунку (precinct count optical scanning – PCOS), коли сканування та підрахунок відбуваються на виборчій дільниці, безпосередньо коли виборці вкидають свій виборчий бюлетень до автомата для голосування.

Виділяються дві базові технологічні схеми: штрих-код сканер та система ручного сканування (Optical Scan Marksense). В обох випадках система оптичного сканування становить собою пристрої введення, що використовують промені світла для сканування кодів (штрих-кодів), тексту або графічних зображень. При цьому, отримані дані миттєво передаються в комп'ютер або систему комп'ютерів.

Щоб розпізнати знаки, бюлетень повинен бути заповненим темним кольором. У деяких азійських країнах для заповнення використовують спеціальні маркери. В окремих випадках система може бути оснащена спеціальними сертифікованими сканерами, які повідомляють виборцю про допущені неточності в заповненні бюлетеня і в разі помилки дозволяють заповнювати його спочатку [15, с. 2].

Ще один варіант OMR — голосування за допомогою перфокарт. Цей метод полягає у тому, що виборці записують свій голос, пробиваючи дірки в картці в певному місці залежно від їхнього вибору. Картки підраховуються в

центральному лічильному центрі за допомогою пристрою зчитування перфокарт, підключеного до комп'ютерної системи [18, с. 20].

1.3. Інтернет-голосування: концептуальне визначення та технології забезпечення

Щодо інтернет-голосування, то, на наш погляд, найбільш точне визначення цього явища дає аналітик European Digital Development Alliance Дмитро Круткий, на думку якого — це воєвиявлення із застосуванням комп'ютерних та інтернет-технологій принаймні для голосування та підрахунку голосів [8, с.6].

За визначенням Міжнародного інституту демократії та сприяння виборам (IDEA), інтернет-голосуванням називають воєвиявлення у неконтрольованому середовищі, «коли голоси передаються через інтернет до центрального сервера підрахунку» [3, с.6].

Як вже зазначалось, відмінну від електронного, інтернет-голосування найчастіше проводиться в неконтрольованих умовах поза традиційною виборчою дільницею. Під «традиційною» мається на увазі дільниця, на якій присутні виборчої комісії, спостерігачі та виборчі списки.

Водночас інтернет-голосування не обов'язково має проводитись лише в домашніх умовах. На думку Крутького, за методами воєвиявлення інтернеті можна поділити на статичне голосування на виборчих дільницях через виділені комп'ютери чи мережі, голосування через мобільний інтернет за допомогою пристроїв, які мають виїзні виборчі дільниці, а також дистанційне інтернет-голосування, коли виборці використовують будь-який пристрій із підключенням

до інтернету [9, с.7]. Саме у першому варіанті інтернет-голосування проводиться у контрольованому середовищі, у двох інших — навпаки.

У IDEA інтернет-голосування поділяють на голосування з комп'ютерів у громадських місцях, кіосків для голосування на виборчій дільниці та з будь-якого підключеного до інтернету комп'ютера [3, с.7].

Таку ж класифікацію наводить і автор дослідження «Міжнародний досвід електронного голосування». За його словами, інтернет-голосування на виборчій дільниці схоже до голосування за допомогою електронних машин прямого запису. Процес здійснюється на виборчих дільницях за допомогою публічних комп'ютерів, під'єднаних до інтернету. Тут інтернет використовують для передачі даних з виборчої дільниці до місцевого, регіонального чи центрального виборчого органу [1, с. 5]. Щодо голосування за допомогою кіосків, то в його рамках використовують спеціальні комп'ютери розташовані в громадських приміщеннях, таких як бібліотеки, школи чи торгові центри. Тут виборчий процес не може контролюватись держорганами, а тому аутентифікація виборця здійснюється за допомогою спеціальних інструментів, наприклад, цифрового підпису, смарт-карти, відбитків пальців тощо [4]. Водночас голосування у контрольованому середовищі через виділенні комп'ютери радше використовують як опційне, тобто на додачу до дистанційного інтернет-голосування, аби надати доступ до голосування через інтернет для незахищених або верст населення, що знаходяться за межею бідності.

Під час дистанційного інтернет-голосування для ідентифікації та аутентифікації використовують software-програми або інші інструменти, такі як смарт-картки [3, с.7].

Переваги інтернет-голосування на перший погляд очевидні: інклюзивність, швидкість і точність голосування та підрахунку, а також відносна дешевезна. Крім того, більшість країн вводять інтернет-голосування у надії залучити молоде покоління виборців.

Водночас у цих аргументів існує й інший бік. По-перше, фізична інклюзивність може працювати у зворотньому напрямку, коли існує інший нюанс — відсутність широкополосного інтернет-покриття. Це особливо гостра проблема для нерозвинених та країн, що розвиваються. У цьому випадку інтернет-голосування стає навпаки — дискримінаційним. Щодо відносної дешевезни, то тут важливо відзначити, що ця перевага працює за умови, якщо інтернет-воєвьявлення — єдиний канал для голосування. За підрахунками дослідників Роберта Криммера, Девіда Дуенаса-Сіда і Юлії Кривоносової, інтернет-голосування є найбільш рентабельним і найдешевшим (з точки зору вартості одного виборця) каналом голосування [26, с.23].

Водночас, як показує досвід проаналізованих нами країн, інтернет-голосування впроваджується поряд із традиційними формами. Це означає, що друк бюлетней, їх логістика, зарплатні для спостерігачів та членів ДВК тощо, все одно входять до статті витрат на проведення голосування. Ба більше, ще додаються витрати на закупівлю та обслуговування виборчого обладнання.

До всього цього додається ще одна проблема — безпеки та порушення таємниці голосування через нездатність систем відділити інформацію про виборця та його голос. Під час традиційного голосування відповідальність за таємницю та безпеку зазвичай несуть державні органи у особі членів та голови ДВК і спостерігачів. Водночас постійно виникають питання довкола того, яким чином контролюються ці аспекти під час інтернет-голосування. Особливе заклопотання викликає можливість зовнішнього втручання у країнах, задіяних у інформаційних війнах та підлив довіри до голосування до демократичних інституцій. Особливо часто це зустрічається у авторитарних або так званих країнах зі спін-диктаторами, демократичних держав, де велику вагу мають популістичні або партії, що представляють інтерес держав з політикою імперіалізму. Найчастіше загроза безпеки та конфіденційності інтернет-голосування полягає у загрозі маніпуляцій та розповсюдження недовіри до результатів інтернет-голосування або в цілому до легітимно-обраної влади. У випадку з популістичними силами, то політики можуть поширювати недовіру до результатів такого голосування, побоюючись, що його використання активізує електорат опонентів.

Водночас за умов використання інтернет-голосування у суспільстві з розвиненими демократичними інституціями та належною цифровою інфраструктурою інтернет-воєв'явлення може дійсно пришвидшити процес голосування та підрахунку голосів (до прикладу, в Естонії підрахунок голосів на

президентських виборах займає до 2 годин), збільшити явку та довіру до виборів й інституцій у цілому [4].

Під час аналізу ми виявили, що інтернет-голосування на різних рівнях впроваджували 18 країн. З них 10 у тій чи іншій формі використовує інтернет-голосування до сьогодні. Водночас серед усіх країн досвід впровадження голосування в інтернеті на усіх можливих рівнях (місцевий, національний та вибори до Європарламенту) мала лише Естонія. Як технологію найчастіше розроблені системи інтернет-голосування дозволяли використовувати комп'ютери, а як додатковий канал використовували кіоски для голосування [3, с. 7- 12; 1, с.15; 10, с 4; 19, с.3; 22, с. 4; 23, с. 1; 27, с. 7-12].

Таблиця 1.1

Практика використання інтернет-голосування у світі

Країна	Чи використовують інтернет-голосування зараз?	На яких рівнях і де застосовують (або застосовували) інтернет-голосування?	Які пристрої можливі для використання ?
Австралія	Так	На муніципальному (У Новому Південному Уельсі)	Комп'ютери, кіоски

Естонія	Так	Усіх	Персональні та комп'ютери у громадських місцях, кіоски
Об'єднані Арабські Емірати	Так	На усіх рівнях (для виборців за кордоном)	Комп'ютери, кіоски
Велика Британія	Ні	Місцевий	Комп'ютери, кіоски, телефони
Оман	Так	На усіх рівнях (для виборців за кордоном)	Комп'ютери
Пакистан	Так	Місцевий	Комп'ютер
Канада	Так	Місцевий (У провінціях Отаріо, Нова Шотландія)	Комп'ютери, телефони, кіоски

Казахстан	Ні	Національний	Комп'ютери
Мексика	Ні	Місцевий	Комп'ютер
Нідерланди	Ні	Місцевий	Комп'ютери, телефони
Нова Зеландія	Так	Місцевий, національний	Комп'ютери, телефон
Норвегія	Ні	Місцевий, Національний	Комп'ютери, телефони
Росія	Так	Національний	Комп'ютер
Швейцарія	Так	Місцевий, національний (У кантонах Женева, Цюріх і	Персональні та комп'ютери у громадських місцях, кіоски

		Невшатель)	
США	Так	Місцевий	Комп'ютери
Франція	Ні	Місцевий	Комп'ютер
Фінляндія	Так	Місцевий	Комп'ютер
Японія	Ні	Місцевий	Комп'ютери, кіоски, телефони

Для аналізу ми відібрали країни, які найчастіше приводили в приклад як успішних досвід інтернет голосування, та які провели за цією технологією одні й більше виборів не у тестовому режимі — Естонію, Австралію, Канаду та Швейцарію; країни, які через загрозу зовнішнього втручання відмовились від технології — Францію, Великобританію та Нідерланди; а також недемократичу державу, що не забезпечила належний захист від фальсифікацій під час голосування в інтернеті — Росію.

1.4. Технології захисту інтернет-голосування

Системи інтернет-голосування використовують кілька технологій для забезпечення аутентифікації, секретності та безпеки. Вони включають криптографію (захист переданої інформації від несанкціонованого доступу) та електронні підписи (сюди також входять паролі, персональні ідентифікаційні номери (PIN), смарт-картки, біометричні дані та цифрові підписи) для перевірки особистості виборця і забезпечити цілісність даних (тобто впевненість, що дані не змінюються під час передачі) [15, с.4].

Також використовують такі технології, як антивірусні програми та системи виявлення вторгнень. Розглянемо детальніше найбільш використовувані з них.

Криптографія — це метод, за допомогою якого інформація (відкритий код) перетворюється на секретний, який приховує справжній зміст цієї інформації.

Криптографія може використовуватися для захисту конфіденційності чи цілісності та/або достовірності інформації. Перший реалізується шляхом шифрування, другий — шляхом підписання [15, с.5].

Шифрування означає скремблювання даних, тобто їх обробка і шифрування таким чином, що їх можна прочитати тільки приймачем, що оснащений спеціальним дешифратором. Для шифрування і розшифровки даних використовується криптографічний ключ, що містить собою дуже велике число [15, с.6].

Криптографію використовують у блокчейн-технології, яку все більше країн починають (або планують) застосовувати під час інтернет-голосування.

Блокчейн — можливість збирати дані та зберігати їх на багатьох серверах. Подібна технологія мінімізує втручання у вибори, адже для фасифікації голосів необхідно встановити контроль більше, ніж над половиною комп'ютерів, що зберігають інформацію.

У процесі умовної голосування дані на бюлетні виборця анонімізуються. Він може бачити, за кого віддає голос, але самого виборця не бачить ніхто. Виборець може перевірити, що його голос зарахований і скільки голосів набирають кандидати[2, с.4].

PKI— це технологія, у якій зазвичай використовують систему відкритих ключів і сертифікатів. Така система застосовується на голосуванні в Естонії. В естонській системі виборець шифрує голос відкритим ключем, а потім підписує його власним закритим ключем. Такі системи вимагають, щоб кожен виборець мав сертифікат і закритий ключ. Закритий ключ має бути доступний виборцю у безпечний і простий у використанні спосіб. У естонському випадку такий ключ вбудований у його ID-карку, до якої потрібен пристрій для її читання, щоб мати можливість голосувати на власному комп'ютері [10, с.5].

Ще одна технологія захисту — сліпий підпис. Сліпі підписи корисні, якщо ми хочемо дозволити виборцям обирати власні виборчі дані, наприклад ключ, який використовується для шифрування їх голосування. Вони можуть зробити це, не розкриваючи цю інформацію владі, через процедуру засліплення. Вони «акривають» інформацію, підписують її і знову «розкривають». Проте канал

зв'язку потребує захисту, оскільки інакше легко побачити, з якого комп'ютера походить голос.

Гомоморфне шифрування — спосіб підрахувати голоси в зашифрованому вигляді. Воно дозволяє підраховують окремі голоси, не розкриваючи зміст кожного окремого голосування.

Рандомізовані бюлетені забезпечують кожному бюлетені різний порядок, що може бути відновлений лише шляхом обробки за допомогою змішаної мережі.

Таким чином виборцям забороняється «підготувати» свій голос вдома, знайшовши ім'я кандидата в попередньо опублікованому списку кандидатів. З іншого боку, розміщення кандидатів у різному порядку в кожному бюлетені може підвищити чесність виборів, оскільки це уникає можливого упередження виборців щодо кандидатів, включених до першого списку. Крім того, однією із загроз для інтернет-голосування є також можливість вірусу на комп'ютері виборця, який змінює голосування. Рандомізовані бюлетені також можуть допомогти запобігти таким нападам, адже технологія змінює номери кандидатів у бюлетнях [15, 8].

Хеш — це криптографічна операція, яка на основі персональних даних і пін-код генерує унікальну хеш-строку, що разом із вибраним кандидатом передає на сервер. Простими словами хеш генерує унікальний для кожного голосування код, а тому майже неможливо відслідкувати, за якого кандидата був відданий голос [15, 9].

Отже, електронне голосування — це процес волевиявлення, підрахунку, друку або оприлюднення результатів з використанням спеціальних систем автоматизації у контрольованому середовищі.

Електронне голосування існує у двох варіантах: з використанням машин прямого запису (directrecordingelectronicmachines – DRE) і у поєднанні електронного та паперового голосування, волевиявлення відсканують пристроєм для підрахунку голосів (Opticalscannerrecognition – OMR).

Система прямого електронного голосування може бути з паперовим слідом (voter-verified paper audit trail (VVPAT) або Verifiable Paper Record (VPR). За способом підрахунку системи OMR поділяються на центральні та дільничні системи оптичного сканування й підрахунку (precinct count optical scanning – PCOS). Виділяються дві базові технологічні схеми OMR: штрих-код сканер та система ручного сканування (Optical Scan Marksense).

Окремо виділяють голосування за допомогою перфокарт, яке полягає у записуванні голосу через пробивання дірок в картці й сканування вибору за допомогою спеціальних машин зчитування.

Інтернет-голосування — це дистанційне голосування у неконтрольованому середовищі із застосуванням комп'ютерних технологій.

Серед технологій на голосування в інтернеті виділяють воєвиявлення з комп'ютерів у громадських місцях, кіосків для голосування та з будь-якого підключеного до інтернету комп'ютера.

Перевагами інтернет-голосування є інклюзивність, швидкість, точність голосування та підрахунку, а також відносна дешевезна.

Недоліками голосування в інтернет є ризик технічних збоїв та кібератак, загроза зовнішнього втручання, порушення безпеки таємниці та розповсюдження недовіри до результатів інтернет-голосування або в цілому до легітимно-обраної влади, потреба у широкомасштабному покритті інтернету та наявності у всіх виборців мінімум одного електронного пристрою для участі у голосуванні.

Наразі інтернет-голосування у тій чи іншій формі використовує 10 країн. Серед них досвід впровадження голосування в інтернеті на усіх можливих рівнях мала лише Естонія.

Серед найпопулярніших технологій захисту інтернет-голосування виділяють криптографію, шифрування, блокчейн, РКІ, сліпий підпис, гомоморфне шифрування, рандомізовані бюлетені, хеш.

Розділ 2. Практика застосування інтернет-голосування.

2.1. Досвід використання інтернет-голосування в Естонії, Австралії, Канаді та Швейцарії.

Естонія вважається одним із найуспішніших прикладів впровадження інтернет-голосування. Країна вперше почала використовувати голосування в інтернеті у 2005 році як додатковий канал воєвьявлення. Тоді всього 2% відсотки виборців вирішили проголосувати в інтернеті. Відтоді частка е-голосів постійно зростала і досягла 32% на місцевих виборах у 2017 році. Водночас на загальну явку це особливо не вплинуло [4].

Інтернет-голосування в Естонії дозволено на усіх рівнях виборів. За законом, проголосувати в інтернеті виборець має право три дні. Голосування починається у понеділок о 9:00 та закінчується о 20:00 у суботу. Протягом цього часу можна змінювати свій вибір необмежену кількість разів. Остаточний вибір зараховуватиметься на основі останньої спроби.

Важливо зазначити, що поруч із інтернет- країна також використовує паперове голосування. Проголосувати на папері можна як окремо від інтернет-голосування, так і разом. Якщо з якоїсь причини виборець стурбований тим, що конфіденційність бюлетеня була порушена, то закон дозволяє після інтернет воєвьявлення прийти на дільницю віддати свій голос на паперовому бюлетні. Після цього інтернет голос автоматично анулюється. Це дозволяє уникнути можливості фальсифікацій та неправильного підрахунку унаслідок збоїв системи та примусу до голосування [8, с. 16].

Проголосувати можливо лише за допомогою комп'ютеру, під'єданого до інтернету. Якщо у виборця немає власного пристрою для голосування, то він має можливість використовувати загальнодоступні комп'ютери, розміщені у публічних місцях.

Для ідентифікації під час голосування використовується електронне посвідчення особи з е-підписом та персональний ідентифікаційний номер (PIN-код). У кожному посвідченні вбудованих цифровий сертифікат, заширований криптографічним алгоритмом з відкритим ключем (RSA). Він допомагає кодувати дані таким чином, щоб на носії не залишався видимого тексту. RSA містить інформацію для аутентифікації та цифрового підпису, а сертифікат допомагає підтвердити зв'язок між ними.

Для ідентифікації закодованої персональної інформації з посвідчення користувачеві потрібен пристрій зчитування смарт-карт, який вставляється в доступний порт комп'ютера. Виборцю потрібно придбати його самостійно [24, с.5].

Щоб проголосувати, потрібно завантажити додаток на свій комп'ютер та аутентифікуватися за допомогою посвідчення. Додаток автоматично перевірить, чи має людина право голосу та відобразить список кандидатів. Після цього користувач може проголосувати за обраного кандидата.

Під час голосування програма закодує дані виборця на бюлетні та перемішує їх таким чином, аби неможливо було ідентифікувати час та послідовність здійснення голосування [14, с.6].

За весь час проведення голосування не було жодного відомого випадку фальсифікацій чи втручання у вибори.

Так як Швейцарія має високий рівень децентралізації політичної системи, то і підготовкою та організацією виборів займається кожен кантон окремо. Наслідком цього є те, що кантони мають свою електронну систему для голосування. Водночас федеральна влада запроваджує стандарти інтернет-голосування та вирішує, наскільки кантон дотримується їх.

Також за кордоном перед впровадження інтернет-воєвиявлення кантони мають проконсультуватись із федеральною радою. Після тестування пілотного інтернет-голосування на окремо визначеній території та аудиту безпеки рада має ознайомитись із процедурою й її результати і лише потім вирішити, чи давати дозвіл на введення інтернет-голосування у кантоні. За весь час спроб впровадити інтернет-голосування рада відмовляла 9 кантонам через те, що в ході пілотного випробування система не пройшла аудит безпеки [27, с.10].

Вперше інтернет-голосування на виборах випробували ще 2006 році. З тих пір три кантони періодично використовували інтернет-воєвиявлення на муніципальних виборах. Водчас до цього часу практика постійного використання інтернет-голосування не закріплена у жодному з кантонів країни. Вона частіше та територіально ширше використовується для референдумів.

Першими і єдиними, хто використовує інтернет-голосування не як пілотний проєкт, були Женева, Цюріх і Невшатель. У перших двох кантонах голосування проводили за схожою схемою – виборці отримували доступ до онлайн-

платформи, вводили індивідуальний ідентифікаційний код, який раніше отримували поштою, і голосували. У цьому випадку можливе використання як інтернету, так і мобільних телефонів для електронного голосування [27, с. 5].

Для збереження таємниці голосування система містить двоетапне шифрування. Зокрема, комп'ютер виборця спочатку шифрує голоси та характеристики ідентифікації та аутентифікації, а система електронного голосування потім перевіряє їх на структуру та цілісність, перш ніж ще раз зашифрувати їх. Дві резервні підсистеми зберігають віддані голоси в базі даних.

На відміну від цього, кантон Невшатель використав розроблену платформу i-voting, яку раніше місцеві могли використати для участі у референдумах та отримання адмінпослуг.

Одразу після впровадження система інтернет-голосування набула популярності серед жителів кантонів. При першій пробі у Женеві інтернет-голосуванням скористались понад 45% населення кантону, у Цюріху — майже 40%. Водночас у Невшателі ця частка була майже незначною — трохи більше за 1% виборців. У перших двох випадках дослідники пов'язують таку популярність із ефектом новизни, адже з часом частка користувачів зменшувалась у середньому до 20%. Щодо Невшателі, то невисоку частку інтернет-користувачів на виборах пов'язують із роботою самої системи для голосування. Зазначається, що для того, аби віддати свій голос користувач мав спочатку авторизуватись на платформі, що створювало додаткові передшкоди та зменшувало бажання виборця дійти до етапу голосування. З часом ситуація почала покращуватись і з

2011 року частка користувачів збільшувалась у середньому приблизно на 2-5%, що пов'язується із запровадженням можливості подання декларації на порталі електронного уряду, яка могла привернути увагу та популяризувати платформу [21, с.5].

Також у 2009 році у Швейцарії вперше запровадили можливість голосування через інтернет для швейцарців за кордоном. Базель-Сіті став першим з непілотних кантонів, який запровадив інтернет-голосування для своїх виборців за кордоном. Протягом двох років до нього додалися Ааргау, Берн, Фрібург, Граубюнден, Люцерн, Шаффхаузен, Золотурн, Санкт-Галлен та Тургау. Наразі майже половина швейцарських кантонів (12 з 26) пропонують своїм громадянам за кордоном голосування через інтернет. У цьому плані більшість кантонів співпрацюють з одним із пілотних для запровадження його моделі інтернет-голосування, попри можливість впровадити свою. Тому для голосування виборців за кордоном використовують дві моделі: модель Цюрихського інтернет-голосування (7 кантонів) та Женевської системи (3 кантони). Невшательську систему поки не прийняли у жодному іншому кантоні.

Загалом через інтернет у середньому голосує від 40 до 60% усіх виборців за кордоном. У деяких кантонах, як, до прикладу, у Ааргау або Тургау, цей відсоток досягає 70%. За весь час впровадження пілотного проєкту інтернет-голосування для виборців за кордоном частка користувачів такою формою збільшувалась на 2% щорічно. Загалом у середньому 7 з 10 швейцарців за кордоном обирали канал для голосування в інтернеті.

Водночас дослідження інтернет-голосування у Женеві й Цюриху серед виборців на території країни та за кордоном показало, що загальну явку такий спосіб голосування так і не підвищив [21, с. 12].

У 2015 році у Цюрихській системі виявили вразливість у коді, який зашифровував дані, та відклали інтернет-голосування у кантоні до липня 2019 року. Про випадки фальсифікації або неправильного підрахунку голосів невідомо [26, с. 14].

Канаду теж зараховують до успішних прикладів використання інтернет-голосування. Водночас країна ще жодного разу не мала досвіду голосування в інтернеті на національному рівні. Наразі жодна провінція не має законодавчого положення, яке б спеціально дозволяло використання інтернет-голосування на загальних виборах.

Окрім того, у Канаді не існує єдиних стандартів проведення інтернет-голосування. У цьому плані абсолютну свободу мають провінції країни: вони вирішують, чи дозволяти інтернет-голосування та встановлюють умови його проведення.

Для імплементації голосування через інтернет муніципалітети має законодавчо дозволити його у Законі про муніципальні вибори (MunicipalElectionsAct). Водночас для цього попередньо муніципалітет має отримати дозвіл провінції, який видають після консультації з незалежною виборчою комісією та голосування муніципальним парламентом за відповідне рішення [20, с.7].

Наразі у своїх законах лише провінції Онтаріо та Нова Шотландія мають положення, що підтримують використання та/або експериментування з інтернет-голосуванням. Муніципалітети інших провінцій також виявляли бажання впровадити, як законодавчо, так і практично інтернет-голосування, однак не отримали підтримку провінцій.

З 2003 року провінції Нова Шотландія та Онтаріо почали впроваджувати голосування на місцевому рівні. Ці спроби робились, аби першочергово збільшити явку на виборах та покращити доступність для окремих категорій виборців.

На початку в Онтаріо створила законодавчу базу, яка підтримує використання альтернативних методів голосування. За офіційною інформацією, запровадження інтернет-голосування коштувало муніципалітету 25 тис. дол [3, с.20].

Окремо у муніципалітеті Окремо місто Маркем дозволяли проголосувати в інтернеті за 5 днів до початку голосування на дільниці, а сама процедура вимагала реєстрації від виборця, під час якого вони мали б створити унікальне таємне питання і отримати PIN-код на пошту. Зареєстровані виборці повинні були також надати свою адресу та рік народження.

Варто відзначити особливість веб-сайту для голосування у Маркемі — у ньому окрім імен кандидатів, виборчий бюлетень містив посилання на програми кандидатів або партій та загальну інформацію про них.

Інші муніципалітети дозволяли інтернет-голосування під усього часу, відведеного на голосування на виборчих ділянках. Крім того, розроблений сайт для голосування у цих випадках не вимагав додаткової попередньої реєстрації. У всіх випадках голосування можливе з усіх пристроїв, що мають доступ до інтернету. Відомо, що у Маркем використовують також кіоски для голосування.

В одному з муніципалітетів Онтаріо Ньюмаркеті інтернет-голосування заборонили використовувати у 2014 року офіційно через побоювання міської адміністрації щодо безпеки та конфіденційності. Водночас, як наголошують дослідники, рішення мало більше політичний характер і було ініційоване тими представниками, які вважали, що можливість голосування через інтернет може сприяти участі виборців, які не є електоратом їх та зазвичай утримуються від виборів [27, с.12].

У Новій Шотландії використання інтернет-голосування почалося в 2008 році, коли чотири муніципалітета законодавчо зафіксували цю можливість. Подібно до Маркхема та інших муніципалітетів Онтаріо, мотивація запровадження інтернет-голосування була покращення доступу, зручності та явки на виборах. У більшості муніципалітетів Нової Шотландії, за винятком столиці Галіфаксу, можливість голосування в інтернеті залишалася відкритою після попереднього періоду голосування, включаючи день виборів. У кількох випадках, таких як Дігбі-Таун, Труро та Ярмут, паперове голосування в день виборів було припинено, а всі вибори проводилися за допомогою інтернет- та телефонних

бюлетенів. Процес голосування включас підтвердження сособи через введення PIN-коду і дати народження та проходження CAPTCHA [27, с.16].

Інтернет-голосування в Австралії використовується лише в одному штаті — Новому Південному Уельсі. Реєстрація та голосування у ньому обов'язковими для майже всіх повнолітніх громадян на виборах, а тому мета запровадження такого способу голосування була не підвищити загальну явку виборців, а покращити доступ до виборчого бюлетеня для громадян, яким інакше було б важко проголосувати.

Водночас скористатись цією можливістю може окрема категорія виборців. Зокрема, Закон про парламентські вибори та вибори штату Новий Южний Уельс визначає, що «голосування за допомогою технологій», наприклад дистанційне онлайн-голосування, призначене лише для використання виборцями з вадами зору, неписьменними чи іншими вадами, які унеможливають можливість участі в голосуванні без сторонньої допомоги, а також виборцями, які проживають за 20 кілометрів або більше від виборчої дільниці, або перебувають за межами штату у день голосування [20, с.10].

Проголосувати можна з будь-якого пристрою, під'єданого до інтернету. Щоб це зробити потрібно попередньо зареєструватись на сайті у період з четверга, 12 лютого, 10:00 до суботи, 28 березня, 13:00. Під час реєстрації вам потрібно прикріпити заявку про те, що ви маєте право на голосування в інтернеті. Також система вимагає надати персональний ідентифікаційний номер (PIN-код) із 6 цифр, який надішлють за допомогою SMS, електронної пошти або телефону.

Після того, як виборець заверше процес реєстрації, він матиме час голосувати з 8:00 (EDST) понеділка, 16 березня, до 18:00 (EDST) суботи, 28 березня.

Під час голосування система дозволяє редагувати вибір або залишити сеанс голосування і повернутись за деякий час. Після голосування виборець отримує номер квитанції.

Щоб дізнатись, чи вірно виборець віддав свій голос, потрібно зателефонувати на гарячу лінію і сказати свій PIN-код і номер квитанції. Якщо голос зарахований невірно, то виборець маж право переєструватись повторно і проголосувати [24, с.10].

У грудні 2021 року Верховний суд Нового Південного Уэльсу визнав недійсними результати трьох виборів до місцевих органів влади через несправність системи. Аналіз, проведений виборчою комісією Нового Південного Уэльса, показав, що 34 бюлетені iVote у Кемпсі, 55 у Сінглтоні та 54 у Шелхарборі були зараховані невірно.

Виборча комісія звернулася до Верховного суду з проханням скасувати результати виборів «для захисту цілісності виборчої системи».

Крім того, дослідник комп'ютерної безпеки виявили серйозну вразливість у системі у Новому Южному Уэльсі під час виборів у березні 2015 року. За їх словами, проблему виявили у коді, що зашифровує особисті дані виборця на бюлетні. Це означало, що інтернет-зловмисник міг викрити бюлетні та змінити їх.

Комісія штату заявила, що не буде використовуватися інтернет-голосування на виборах 2023 року, оскільки система потребує заміни програмного забезпечення [20, с. 16].

2.2. Загрози зовнішнього втручання у інтернет-вибори: досвід Нідерландів, Британії та Франції

Інтернет-голосування у Нідерландах вперше випробували на виборах до Європаламенту у 2004 року для громадян, які проживають за кордоном. Паралельно проводили вибори інтернет-голосування до рад з водних ресурсів.

Для цього розробили систему KOA11. Для голосування виборці мали зареєструватися за поштою та обирати власний код доступу як пароль. Натомість вони отримували код голосування як «логін» разом зі списком кандидатів, які також мали свої унікальні коди, які потрібно було ввести на сайт.

У 2006 році провели другий експеримент з використання інтернет-голосування на виборах до рад з водних ресурсів. Для цього розробили систему RIES, що використовує криптографічні операції для захисту голосів. Виборці могли підтвердити свій голос після виборів, а незалежні інституції — провести повний перерахунок результатів. Система RIES використовує хеші для публікації передвиборчій таблиці, яка дозволяла після оприлюднення підрахувати результат виборів. Завдяки використанню хеш-функцій система була відносно простою, забезпечувала захист голосів і дозволяє перевіряти результати. У той час як хеші всіх можливих голосів були публічними, дізнатись із них інформацію про виборця було неможливо неможливо без необхідного ключа. Можливо лише

порівняти кількість виборців у цій таблиці з кількістю зареєстрованих виборців [22, с.4].

Водночас, як зазначають дослідники, фундаментальна проблема в системі RIES полягала у можливості генератора ключів знищити код відразу після відправлення його виборцям, чим могли скористатись хакери. Якщо цього не зробити, це може поставити під загрозу як таємність, так і справжність голосування.

Як наслідок почались дискусії у парламенті щодо можливості продовження використання інтернет-голосування на виборах. Крім того, незалежне розслідування виявило додаткові проблеми безпеки, пов'язані з кодом та можливістю захистити голосування.

Через це електронне голосування було заборонено в Нідерландах у 2007 році, але уряд вважав, що спроби необхідно продовжувати.

Вперше це збирались зробити у 2008 році під час виборів до Європарламенту для виборців за кордоном. Тоді визначили критерії, яким мають відповідати всі форми електронного голосування, однак запропонована система інтернет-голосування не відповідала їм. Головною проблемою була надійність використовуваної криптографічних ключів, які мали б зашифрувати дані та підпис виборця. На те, щоб якісно налаштувати цю систему не вистачало часу й уряд тоді вирішив відмовитись від інтернет-голосування [22, с.8].

У 2017 році Нідерланди вперше зібрались протестувати інтернет-голосування для виборців за кордоном. Пілотне випробування пройшло 15 березня перед голосування за нижню плату парламенту.

Після попереджень нідерландської розвідки чиновники Нідерландів серйозно поставилися до питання потенційного втручання Росії у їхні вибори. Але через їхню активну підготовку або через очевидну відсутність зусиль Росії щодо втручання, вибори пройшли успішно і без будь-якого помітного втручання. Водночас країна серйозно поставилась до можливості майбутнього використання голосування в інтернеті.

Опасіння додавав голландський референдум щодо торговельної угоди між Європейським Союзом (ЄС) та Україною, проведений нідерландськими проросійськими прихильниками. Він стався на фоні розслідування збиття рейсу МН17 на сході України. Місцеві проросійські сили в Нідерландах протистояли звинуваченням втручання в референдум [19, с.4].

Відтоді Служба загальної розвідки та безпеки (AIVD) почала стежити за російською хакерською групою CosyBear у середині 2014 року та попередила чиновників США про її діяльність.

У своїй щорічній доповіді за 2016 рік AIVD підкреслив зростання російської впливу на операції, спрямовані на економічний, політичний, науковий та сектори оборони. У доповіді зокрема згадуються кібератаки, спроби вербування людської розвідки, шпигунство, операції під фальшивим прапором та маніпулювання громадською думкою. У ньому зазначається, що «поширення дезінформації та

пропаганди відіграє важливу роль у прихованому політичному впливі. Він також приписує атаку на 100 урядових облікових записів електронної пошти. Офіцери голландської розвідки відкрито стверджували, що росіяни наполегливо намагалися «проникнути в комп'ютери державних установ і бізнесу». Через це у Нідерландах заборонили використання електронних машин для голосування та підрахунку голосів, а також інтернет голосування для усіх наступних виборах [19, с.6].

З 2006 року інтернет-голосування у Франції доступне для громадян, які проживають за кордоном. Приводом впровадження голосування в інтернеті стала низька явка на виборах. Щоб проголосувати в інтернеті, французькі виборці мали бути зареєстровані у консульському виборчому списку. Зареєструватися можна було онлайн або особисто у французьких консульствах та посольствах. Під час реєстрації виборці мали вказати свою поштову адресу, дійсну адресу електронної пошти та номер телефону, аби отримати логіни та паролі [25, с.6].

Голосування в інтереті було дозволене для усіх рівнів виборів, окрім президентських. Щоб проголосувати, потрібно зайти на портал, ввести ім'я користувача та пароля, отриманий за SMS та пройти CAPTCHA. Проголосувати можна з будь-якого пристроя, підключеного до інтернету. Безпеку системи забезпечує гомоморфне шифрування.

Критика інтернет-голосування у Франції полягала у технічних проблемах, з якими періодично зіштовхувались виборці. На прикладі 2014 року було важко відправити логіни та паролі виборцям, оскільки близько 25% зареєстрованих

виборців не надали адресу електронної пошти, тоді як інші у кількох країнах так і не отримали інформацію, надіслану поштою та SMS. По-друге, 6% інтернет-виборців (тобто близько 4630 громадян) звернулися до служби підтримки, бо зіткнулися з проблемами підключення. На додачу до цього з'явилась проблема з роботою сайту через зростання виборців, які підключились протягом останніх кількох годин до закінчення голосування [12, с.9].

Водночас голосування в інтернеті також викликало занепокоєння щодо безпеки та таємності голосування. У 2017 році виникнув скандал щодо можливих спроб російського втручання у вибори президента Франції в 2017. Тоді приводом для занепокоєнь стали атаки на президентську кампанію Еммануеля Макрона, які були аналогічними до кампанії колишньої кандидатки в президенти США від Демократичної партії Хіллари Клінтон. Французькі правоохоронні органи розпочали розслідування за фактом кібератаки на компанії «Advanced Persistent Threat 28» (APT28), «Fancy Bear» і «Pawn Storm», які були відомі співпрацею з Головним розвідувальним управлінням Росії [19, с. 15].

На той час Макрон фактично був єдиним кандидатом, який відкрито критикував Путіна. За 2 місяці до початку першого туру голосування партія «Національний фронт» отримала пряму фінансову допомогу з банку, пов'язаного з Кремлем. А тому очевидно, що Росія прагнула привести до влади проросійську кандидатку з євроскептичними поглядами та головну опонентку Макрона Марі Ле Пен. На той час Російська Федерація активно поширювала на національному т

та французькому інформаційному полі наративи про те, що Макрон нібито є агентом фінансових інтересів США і має нетрадиційну орієнтацію.

Пізніше французька розвідка отримала дані про підготовку Росією до хакерських атак на парламентські вибори, які мали б проходити того ж року, у тому числі за допомогою інтернету для виборців за кордоном. Через це Уряд Франції відмовився від інтернет-голосування, вибори за кордоном пройшли у традиційний спосіб [19, с.18].

Схожа до Франції відбулась й історія з Великобританією. Країна у тестовому режимі намагалась запровадити інтернет-голосуванняще у 2000-х роках. Тоді таким чином хотіли підвищити загальну явку на виборах. Інтернет-голосування було пілотовано в на місцевих виборах у містах Стратфорд-на-Ейвоні та Суідон на виборах у 2003 та 2007 роках. Проголосувати можна було як через комп'ютер, так і телефон, і кіоски для голосування [1, с. 14].

Для голосування розробили сайт, на якому виборці могли зареєструватись через номер телефону та паспортні дані. Після цього виборець отримував пароль та код доступу до кабінету для голосування. Щоб змінити свій вибір, людині потрібно було зателефонувати на гарячу лінію та повідомити про анулювання попередніх результатів, а тому система видавалась максимально незручною для звичайного виборця. Швидше за все саме це стало і причиною, чому загальна явка так і не збільшилась. У експерименті не описано, яку систему для безпеки використовувала країна на той час. Водочас безпека стала однією з причин відмови від ідеї інтернет-голосування на майбутніх виборах [9, с. 24].

У 2017 році перед оголошенням дострокових виборів прем'єр міністра Британії у країні знову почали говорити про можливість введення інтернет-голосування. Референдум про від'єднання Британії від ЄС та останні вибори показували постійну тенденцію до падіння явки а виборах. Тоді Росія активно проводила кампанії з дезінформації та залучала британських політиків до їх поширення. Серед таких — член Лейбористської партії Британії Джеремі Корбін, який активно був присутній на той час на російських ЗМІ, де транслював антиєвропейські та антинатівські ідеї.

Водночас були реальні опасіння влади щодо можливого втручання Росії у вибори. У 2016 році російські тролі поширювали фальшиві заяви про фальсифікацію голосів на референдумі про незалежність Шотландії 2014 року. А у 2016 році розвідка США дійшла висновку, що подібні російські «кампанії впливу» досі працюють у Сполученому Королівстві. Британські чиновники розраховували, що короткий проміжок часу між оголошенням і виборами обмежить можливості Москви розробити детальну схему фальсифікації виборів. Водночас розвідка попереджала про високу ймовірність спроб втрутитися у результати голосування за умов їх переведення у формат онлайн. Через це влада вирішила не ризикувати та відкласти питання використання інтернет-голосування на невизначений термін [19, с.26].

2.3. Інтернет-голосування у недемократичних державах: приклад Російської Федерації

Росія — це яскравий приклад, коли голосування фактично стає політичним інструментом. Країна має низький показник електоральної демократії та високий рівень недовіри до виборів й інституцій в цілому. Традиційні вибори неодноразово супроводжувались випадками примусового голосування, фальсифікацій, різних заборон для міжнародних спостерігачів та ЗМІ [4].

У Росії інтернет-голосування ввели, аби збільшити довіру до результатів голосування та залучити молодь. Очевидно, що збільшення частки протестного електорату не хвилювала чинну владу, адже з самого початку вибори не планували проводити прозоро.

Перші експерименти з впровадження технології інтернет-виборів провели у формі опитувань в 2008 році у Тульській області, у 2009 році у Володимирській, Волгоградській, Вологодській, Томській областях та Ханті-Мансійському автономному окрузі — Югре та у 2010 році в Московській області. Їх результати не впливали на результати виборів.

Вперше голосування в інтернеті провели у 2019 році до законодавчих органів влади та на виборах депутатів до Московської міської Думи VII скликання [7, с.3].

Нового сайту для голосування не розробляли, за платформу електронного голосування виступив офіційний сайт мера Москви. Для участі в інтернет-голосуванні потрібно було надіслати заявку на сайті mos.ru на включення до

Реєстру електронних виборців. Заявку можна подати за 45 днів до дня голосування. Під час електронного голосування виборець отримував SMS із кодом підтвердження на номер, зазначений у особистому кабінеті. Після правильного введення коду із SMS електронний бюлетень відкривався для голосування [7, с.6]

Безпеку системи мала б забезпечувати технологія блокчейн, однак під час вбудування можливості для голосування розробники в останній момент відмовилися від створення сервісу для перевірки виборцем правильності обліку голосу, а спостерігачі не отримали ключа для розшифровки голосів і повний доступ до коду системи [29, с.3].

Також підготовки до використання електронного голосування під час виборів до Мосміськдуми система не пройшла 4 тестування. Під час другого тестування системи було зафіксовано атаки хакерів. Між другим та третім тестуванням систему зламав французький криптограф. Також експерт та програміст Євген Федін виявив у кодї системи скрипт, що дозволяв вносити будь-які зміни до коду, аж до фальсифікування результатів голосування. Незважаючи на виявлені вразливості системи, було рішення про інтернет-голосування на виборах до Мосміськдуми не скасували.

Під час голосування явка на «електронних» дільницях перевищила 92% у всіх виборчих округах, де проводився експеримент. Загальна явка становила 21,77 %, що значно було значним відсотком для виборів такого масштабу [7, с.14].

У день голосування через збої системи виборцям не видавалися електронні бюлетені, статистика не оновлювалася. Співробітники кілька разів самостійно відключали і знову запускали систему, із 12 годин голосування система працювала лише 8 годин. Персональні дані виборців, які проголосували електронно, вже за тиждень після виборів змогли злити у мережу.

У всіх виборчих округах, які брали участь в експерименті, кількість відсотків виборців, які проголосували за самовисуванців, що згодом увійшли до фракції «Єдиної Росії», на «електронних» дільницях виявилася вищою, ніж на звичайних. У 30-му окрузі результати на «електронній» дільниці зовсім протилежні підсумкам виборів за паперовим голосуванням: за результатами електронного голосування перемогла кандидатка від «Єдиної Росії» Маргарита Русецька, тоді як на звичайних дільницях виграв незалежний кандидат Роман Юнеман [7, с. 20]. Попри провали, влада продовжила можливість застосування інтернет-голосування у 2021 року на виборах у Державну думу VIII скликання, під час яких експерти і дослідники відзначили низку порушень та можливих фальсифікацій [7, с. 22].

Один з експертів заявив, що на виборах до Держдуми у 2021 році була випробувана система електронного голосування, за допомогою якої можна отримувати будь-які вигідні владі результати. Незгода з результатами виборів, зроблених на основі електронного голосування, спонукала до проведення масових акцій протесту у жовтні 2021 року.

Після експерименту влада ухвалила закон, який дозволив використання інтернет-голосування на виборах усіх рівнів [7, с. 26]

Отже, з усіх проаналізованих країн інтернет-голосування дозволене на усіх рівнях виборів лише в Естонії. Інші країни використовували інтернет-голосування на окремих територіях найчастіше для голосування на місцевих виборах. У Канаді голосування в інтернеті дозволено лише для окремої категорії виборців, що мають фізичні або логістичні перешкоди для голосування на виборчій дільниці. Окремо Швейцарія, Естонія, Франція та Нідерланди дозволяють або дозволяли голосування для своїх громадян за кордоном.

Поруч із інтернет-воєвизавленням майже всі країни використовували також паперове голосування. Лише у декількох муніципалітетах Канади вибори проводилися за допомогою інтернет- та телефонних бюлетенів.

Всі проаналізовані країни дозволяли голосування за допомогою власного комп'ютеру. Естонія, Швейцарія, Канада та Великобританія дозволяли також голосування у кіосках та з комп'ютера, розташованого у публічних місцях.

Для захисту голосування в Естонії використовують криптографічний алгоритм з відкритим ключем, Швейцарії — двоетапне шифрування, у Канаді та Австралії — шифрування, у Франції — гомоморфне шифрування, Нідерландах — хеш-технологію, у Росії — блокчейн.

Дослідження показало, що у всіх країнах інтернет-голосування значно не вплинуло на загальну явку.

Щодо загроз та проблем використання інтернет-голосування, то досліджувані країни стикались із технічними проблемами, пов'язаними із системою голосування та ідентифікації виборця (Франція, Австралія),

можливими загрозами безпеки та конфіденційності (Канада, Швейцарія, Росія), можливими атаками та зовнішнім втручанням у результати (Нідерланди, Британія та Франція), а також загрозами маніпуляцій результатами та внутрішнього втручання.

Висновки

Електронне голосування — це волевиявлення в контрольованому середовищі з використанням електронних засобів, яке характеризується особливим колом суб'єктів та існує у двох варіантах: з використанням машин прямого запису (directrecordingelectronicmachines – DRE) і у поєднанні електронного та паперового голосування, волевиявлення відсканують пристроєм для підрахунку голосів (Opticalscannerrecognition – OMR).

Інтернет-голосування розуміють в контексті електронного або як окремий вид голосування з використанням дистанційних електронних засобів, серед яких кіоски для голосування, телефони, персональні та публічні комп'ютери.

Інтернет-голосування на різних рівнях впроваджували 18 країн. З них 10 у тій чи іншій формі використовує інтернет-голосування до сьогодні. Як технологію найчастіше розроблені системи інтернет-голосування дозволяли використовувати комп'ютери, а як додатковий канал використовували кіоски для голосування.

Найчастіше для захисту голосування в інтернеті країни використовували криптографію, шифрування, блокчейн, РКІ, сліпий підпис, гомоморфне шифрування, рандомізовані бюлетені та хеш.

З усіх проаналізованих країн інтернет-голосування дозволене на усіх рівнях виборів лише в Естонії. Інші країни використовували інтернет-голосування на окремих територіях найчастіше для голосування на місцевих виборах.

Поруч з інтернет-воєвьявленням майже всі країни використовували також паперове голосування. Лише у декількох муніципалітетах Канади вибори проводилися за допомогою інтернет- та телефонних бюлетенів.

Дослідження показало, що у всіх країнах інтернет-голосування значно не вплинуло на загальну явку.

Щодо загроз та проблем використання інтернет-голосування, то досліджувані країни стикались із технічними проблемами, пов'язаними із системою голосування та ідентифікації виборця, можливими загрозами безпеки та конфіденційності, можливими атаками та зовнішнім втручанням у результати, а також загрозами маніпуляцій результатами та внутрішнього втручання.

З проаналізованого досвіду країн ми дішли висновку, що для успішного впровадження інтернет-голосування потрібні: сталі політичні інституції, довіра до влади та виборів, розвинене громадянське суспільство та правова держава, що дає можливість проводити чесні вибори та оскаржити їх результати в разі потреби, а також технології, які б дозволяли одночасно залучати якнайширші верстви населення (інклюзивні), зберігати таємницю голосування, перевірити результати та бути захищеними від зовнішнього втручання.

Список використаної літератури

1. Антонов. Д. В. Международный опыт электронного голосования [Электронный ресурс] / JaroslavValerievichAntonov // Сборник конкурсных работ в области избирательного права и избирательного процесса выполненных студентами, аспирантами в 2010/2011 учебном году. М.: РЦОИТ.. – 2011. – Режим доступа до ресурсу: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290482.
2. Бобовський Є. О. «Метод цифрового голосування на основі технології блокчейн» [Электронный ресурс] / Євген Олександрович Бобовський // МАГІСТЕРСЬКА ДИСЕРТАЦІЯ на здобуття ступеня магістра за освітньо-науковою програмою «Комп'ютерні системи та мережі» зі спеціальності 123 «Комп'ютерна інженерія». – 2021. – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/41397/1/Bobovskiy_magistr.pdf.
3. Впровадження електронного голосування [Электронный ресурс] // The International Institute for Democracy and Electoral Assistance – Режим доступу до ресурсу: 3-Heights(TM) PDFSecurityShell 4.8.25.2 <http://www.pdf-tools.com>.
4. Все, що ви хотіли знати про електронне голосування [Электронный ресурс] // ОПОРА – Режим доступу до ресурсу: https://opora.ua/news/video/about_election/23346-q-a-vse-shcho-vi-khotili-znati-pro-elektronne-golosuvannia.
5. Электронное голосование по странам [Электронный ресурс] // ru.lknowledgr.cor – Режим доступу до ресурсу: <https://ru.knowledgr.com/21235681/ЭлектронноеГолосованиеПоСтранам>.
6. Солоненко О. ВИБОРЧІ ЦЕНЗИ: УМОВИ РЕАЛІЗАЦІЇ ВИБОРЧОГО ПРАВА [Электронный ресурс] / Олег Солоненко – Режим доступу до ресурсу: http://elar.naiu.kiev.ua/bitstream/123456789/13279/1/Проб.%20та%20стан%20дотр.%20захист._p17-18.pdf.
7. Токарева Е.А. Перспективы использования средств дистанционного голосования в РФ / Е.А. Токарева // Материалы Международного молодежного научного форума «ЛОМОНОСОВ-2011» / Отв. ред. А.И.

8. Турчин Я. Впровадження технології електронного голосування: світовий досвід та вітчизняні перспективи [Електронний ресурс] / Ярина Турчин – Режим доступу до ресурсу:
http://eprints.cdu.edu.ua/2382/1/Збірник_конф_ЧНУ_2019%20%281%29-55-64.pdf.
9. Круткий Д. Інтернет-голосування: виклики та рішення. Аналітична записка [Електронний ресурс] / DmytroKhutkyu. – 2020. – Режим доступу до ресурсу:
https://www.researchgate.net/publication/343917458_Internet-golosuvanna_vikliki_ta_risenna_Analiticna_zapiska.
10. Кохалик Х. Світовий досвід впровадження електронної демократії: проблеми та досягнення [Електронний ресурс] / Х. Кохалик – Режим доступу до ресурсу:
efdu_2015_42_20.pdf.
11. Навчальний посібник для членів дільничих виборчих комісій на місцевих виборах 25 жовтня 2020 року [Електронний ресурс] // ЦВК – Режим доступу до ресурсу: https://www.cvk.gov.ua/wp-content/uploads/2020/10/Posibnyk_DVK_web-s004.pdf.
12. Фоміна С. В. Поняття та ознаки голосування як стадії виборчого процесу в зарубіжних країнах [Електронний ресурс] / С. В. Фоміна – Режим доступу до ресурсу: <https://www.google.com/> http://www.irbis-nbu.gov.ua/cgi-bin/irbis_nbu/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&Z21ID=&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/znpkhnpu_pravo_2012_19_33.pdf.
13. Чупрін Р. В. Проектування виборчих систем: структура виборчого бюлетеня [Електронний ресурс] / Р. В. Чупрін – Режим доступу до ресурсу:
<http://politics.chdu.edu.ua/article/download/74347/69807>.
14. Чупрін В. Метод протидії незаконному впливу на виборців у системі Інтернет голосування [Електронний ресурс] / В. Чупрін, В. Вишняков, М. Пригара – Режим доступу до ресурсу: http://www.irbis-nbu.gov.ua/cgi-bin/irbis_nbu/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILEA=&2_S21STR=bezin_2017_23_1_3.

15. A Model for Direct Recording Electronic Voting Systems [Электронный ресурс] // ASTER OF INFORMATION TECHNOLOGY in the SCHOOL OF INFORMATION TECHNOLOGY of the FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY University of Pretoria – Режим доступа до ресурсу:
<https://repository.up.ac.za/bitstream/handle/2263/28041/dissertation.pdf?sequence=1&isAllowed=y>.
16. Barcodes in the Election Industry [Электронный ресурс] // ELECTION SYSTEMS & SOFTWARE – Режим доступа до ресурсу:
<https://www.nass.org/sites/default/files/2019-07/Election-Systems-Software-White-Paper-NASS-Summer19.pdf>.
17. Eric A. Fischer. The Direct Recording Electronic Voting Machine (DRE) Controversy: FAQs and Misperceptions [Электронный ресурс] / Eric A. Fischer, Kevin J. Coleman // Congressional Research Service ~ The Library of Congress – Режим доступа до ресурсу: <https://www.files.ethz.ch/isn/141781/60725.pdf>.
18. Erik Miguel de Elias. Optical Mark Recognition: Advances, Dificulties, and Limitations [Электронный ресурс] / Erik Miguel de Elias, Paulo Marcelo Tasinafo // SN Computer Science. – 2021. – Режим доступа до ресурсу: <https://link.springer.com/content/pdf/10.1007/s42979-021-00760-z.pdf>.
19. Erik Brattberg and Tim Maurer. Five European Experiences With Russian Election Interference [Электронный ресурс] / Erik Brattberg and Tim Maurer // Carnegie Endowment for International Peace. – 2018. – Режим доступа до ресурсу: <http://www.jstor.com/stable/resrep21009.6>.
20. European Parliamentary and local Elections (Pilots) Act 2004 // Режим доступа: www.legislation.gov.uk.
21. Goodman N. Internet Voting in Sub-national Elections: Policy Learning in Canada and Australia [Электронный ресурс] / N. Goodman, S. Rodney. – 2017. – Режим доступа до ресурсу: <https://sci-hub.se/> <https://twin.sci-hub.se/6380/88a9e14fa686ce9ce7696d0725d80d56/goodman2017.pdf?download=true>.

22. Germann, M., & Serdült, U. Internet voting and turnout: Evidence from Switzerland. Electoral Studies [Электронный ресурс] / Germann, M., & Serdült, U. – 2017. – Режим доступа до ресурсу: <https://sci-hub.se/10.1016/j.electstud.2017.03.001>
23. Jacobs B. Electronic Voting in the Netherlands: from early Adoption to early Abolishment* [Электронный ресурс] / B. Jacobs, W. Pieters – Режим доступа до ресурсу: <http://www.cs.ru.nl/B.Jacobs/PAPERS/E-votingHistory.pdf>.
24. Leontine Loeber. E-voting in the Netherlands; past, current, future? [Электронный ресурс] / Leontine Loeber. – 2016. – Режим доступа до ресурсу: <https://www.researchgate.net/> https://www.researchgate.net/profile/Leontine-Loeber/publication/301547849_E-voting_in_the_Netherlands_past_current_future/links/5718956e08aed43f632215dc/E-voting-in-the-Netherlands-past-current-future.pdf?origin=publication_detail.
25. Mr. Sanjay Kumar. ANALYSIS OF ELECTRONIC VOTING SYSTEM IN VARIOUS COUNTRIES [Электронный ресурс] / Mr. Sanjay Kumar, Dr. Ekta Walia // Department of Computer Engineering, M. M. University, Mullana (Ambala) 133207, India. – 5. – Режим доступа до ресурсу: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.5626&rep=rep1&type=pdf>.
26. Newindianexpress.com. From EVMs to Blockchain-based e-voting? [Электронный ресурс] / Newindianexpress.com – Режим доступа до ресурсу: <https://www.newindianexpress.com/opinions/2021/apr/26/from-evms-to-blockchain-based-e-voting-2294834.html>.
27. Robert K. New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper? [Электронный ресурс] / K. Robert, D. David, L. Krivonosova // Public Money & Management – Режим доступа до ресурсу: <https://www.tandfonline.com/doi/pdf/10.1080/09540962.2020.1732027>.
28. Uwe Serdult. Fifteen years of internet voting in Switzerland [History, Governance and Use] [Электронный ресурс] / Uwe Serdult, Micha Germann, Fernando Mendez – Режим доступа до ресурсу: <https://ieeexplore.ieee.org/abstract/document/7114482>.

29. Which Countries Are Casting Votes Using Blockchain? [Электронный ресурс] // TheHackerNoonNewsletter – Режим доступа до ресурсу: <https://hackernoon.com/which-countries-are-casting-voting-using-blockchain-s33j34ab>.