ТЕМА 9. ЕЛЕКТРОННЕ ГОЛОСУВАННЯ

9.1. Сутність електронного голосування та його регулювання

Як складова електронної демократії, **е-голосування** (англ. e-voting) — є загальним терміном, що об'єднує кілька різних типів голосування, охоплюючи як процес здійснення голосування за допомогою електронних засобів, так і процес автоматичного підрахунку голосів за допомогою електронних пристроїв та спеціального програмного забезпечення.

Європейська комісія за демократію через право (http://www.venice.coe.int) – більш відома як *Венеціанська комісія*, оскільки вона збирається у Венеції – є дорадчим органом Ради Європи з конституційних питань.

Її роль полягає в тому, щоб надавати юридичні консультації своїм державам-членам і, зокрема, допомагати державам, які бажають привести свої правові та інституційні структури у відповідність з європейськими стандартами та міжнародним досвідом у сфері демократії, прав людини та правління закону.

Низка доповідей Венеціанської комісії присвячені проблемам відповідності віддаленого голосування (голосування поштою або електронне голосування) стандартам Ради Європи. Зокрема, ці доповіді містять попередження про необхідність вжиття додаткових заходів для мінімізації ризиків фальсифікацій та визначено *5 принципів*, що відображають засади європейської демократії та однаково придатні як для виборчих кампаній, так і для референдумів:

1. Універсальне право голосу: всі люди мають право голосу.
2. Рівні права голосу: кожен виборець має рівну кількість голосів.
3. Свобода права голосу.
4. Таємність права голосу.
5. Пряме право голосу.

На думку Венеціанської комісії, електронне голосування може використовуватися лише за умови, якщо:

- система є безпечною/захищеною і надійною;
- система є прозорою, тобто надає можливість перевірки щодо її функціонування;
- виборці мають нагоду отримати підтвердження свого вибору і виправити його у разі допущення помилки;
- для полегшення перерахунку голосів у разі конфліктної ситуації передбачається процедура роздрукування голосів.

Рада Європи [29] продовжує залишатися *єдиною організацією, яка встановлює міжурядові стандарти у сфері е-голосування*.

Комітет міністрів РЄ створив *Спеціальний комітет експертів з правових, операційних та технічних стандартів електронного голосування* (CAHVE), який складається з призначених урядом представників Держав-членів та організацій, котрі мають безпосередній досвід або спеціальні знання з е-голосування.

У 2004 році було схвалено Рекомендацію Rec(2004)11 щодо правових, операційних та технічних стандартів е-голосування, яка наразі залишається *єдиним джерелом* посилань на цю тему. Вона використовується в національній юриспруденції навіть у державах, які не є членами, а також іншими відповідними міжнародними суб'єктами.

У 2017 році було схвалено Рекомендацію CM/Rec(2017)5, яка розроблена для удосконалення Rec(2004)11 та стосується найбільш важливої частини виборчих технологій, а саме е-голосування, зокрема використання електронних засобів для подачі і підрахунку голосів. У цю категорію входять такі системи, як електронні виборчі машини (DRE), сканери для голосування, цифрові ручки та системи голосування в Інтернеті.

Мета Рекомендації CM/Rec(2017)5 - гармонізувати реалізацію принципів демократичних виборів і референдумів при використанні е-голосування, таким чином зміцнюючи довіру виборців до відповідного процесу голосування та схем е-голосування.

РЄ було розроблено 3 основних взаємодовнюючих документа, які регулюють електронне голосування:

1. Рекомендація CM/Rec(2017)5 Комітету міністрів державам-членам щодо стандартів електронного голосування.
2. Пояснювальний меморандум до Рекомендації CM/Rec(2017)5 Комітету міністрів державам-членам щодо стандартів електронного голосування.
3. Керівництво щодо імплементації положень Рекомендації CM/Rec(2017)5 щодо стандартів електронного голосування.

Показовим є те, що під час прийняття цієї рекомендації, Постійний представник Російської Федерації зазначив, що відповідно до статті 10.2c Регламенту засідань заступників міністрів він залишає за собою право свого уряду виконувати чи не виконувати рекомендацію.

17 березня 2020 року Центральна виборча комісія України створила *робочу групу для вивчення можливостей впровадження нових технологій у виборчий процес України*. До групи на чолі з членом ЦВК Сергієм Постівим входять до 20 представників Центральної виборчої комісії, Державного реєстру виборців, Міністерства цифрової трансформації України, представників правоохоронних та інших державних органів, експертів неурядові та міжнародні організації.

Робота групи зосереджена на кількох напрямках:

- міжнародний досвід використання нових технологій на виборах;
- цифрові рішення для управління виборами;
- електронна ідентифікація виборців;
- е-голосування, електронний підрахунок голосів та електронне підведення підсумків виборів;
- цифрові рішення для виборчої освіти та підвищення обізнаності громадськості.

Рада Європи надає свою експертну підтримку Центральній виборчій комісії України для того, щоб будь-яке цифрове рішення, яке розглядається для подальшого впровадження у українське виборче законодавство та практику, повністю відповідало міжнародним виборчим стандартам [52].

Національним інститутом стратегічних досліджень України в 2021 році була підготовлена аналітична записка щодо електронного

голосування та перспектив його впровадження в Україні [90], де зокрема зазначається при необхідність відповідального ставлення до ідеї втілення електронного голосування у контекст української виборчої системи, яке передбачає, що кроки з реалізації такої системи доцільно здійснювати лише у випадку, коли технічні, організаційні, правові умови в Україні відповідатимуть проголошеним Рекомендацією КМ Ради Європи CM/Rec(2017)5 щодо стандартів для е-голосування. На думку експертів, це потребує часу і може суттєво відтермінувати впровадження технології е-голосування.

9.2. Стандарти електронного голосування Ради Європи

Рекомендація CM/Rec(2017)5 з е-голосування має на меті [65]:

- надання виборцям можливості віддати свій голос не з виборчої дільниці на їхньому виборчому округі;
- сприяння проведенню голосування виборцем;
- сприяння участі у виборах і референдумах громадян, які мають право голосу та проживають або перебувають за кордоном;
- розширення доступу до процесу голосування для виборців з обмеженими можливостями або для тих, хто має інші труднощі з фізичною присутністю на виборчій дільниці та використанням наявних там пристроїв;
- збільшення явки виборців шляхом надання додаткових каналів голосування;
- приведення голосування у відповідність до нових подій у суспільстві та дедалі більшого використання нових технологій як засобу комунікації та громадської участі у прагненні до демократії;
- скорочення з часом загальних витрат для виборчих органів на проведення виборів чи референдуму;
- надання результатів голосування надійніше та швидше;
- надання електорату кращого обслуговування, пропонуючи різноманітні канали голосування.

Всі канали голосування, включаючи е- голосування, повинні відповідати принципам демократичних виборів і референдумів.

Е-голосування вже запроваджено з метою:

- збільшення явки виборців шляхом надання додаткових каналів голосування;
- приведення голосування у відповідність до нових подій у суспільстві та дедалі більшого використання нових технологій як засобу комунікації та громадської участі у прагненні до демократії;
- скорочення з часом загальних витрат для виборчих органів на проведення виборів чи референдуму;
- надання результатів голосування надійніше та швидше;
- надання електорату кращого обслуговування, пропонуючи різноманітні канали голосування.

СТАНДАРТИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

I. Загальне виборче право

1. Інтерфейс для виборців системи е-голосування повинен бути простим для розуміння та використання всіма виборцями.
2. Система е-голосування повинна бути розроблена, наскільки це можливо, для того, щоб люди з інвалідністю та особливими потребами могли голосувати самостійно.
3. Якщо канали дистанційного е-голосування не є загальнодоступними, вони є лише додатковим і необов'язковим засобом голосування.
4. Перед голосуванням за допомогою системи дистанційного електронного голосування необхідно чітко звернути увагу виборців на те, що електронні вибори, на яких вони подають своє рішення в електронному вигляді, є справжніми виборами чи референдумом.

II. Рівне виборче право

5. Вся офіційна інформація про голосування подається однаково, як у каналах голосування, так і між ними.

6. Якщо на одних і тих же виборах чи референдумі використовуються електронні та не електронні канали голосування, має бути безпечний і надійний метод для узагальнення всіх голосів та підрахунку результату.

7. Забезпечується унікальна ідентифікація виборців таким чином, щоб їх можна було безпомилково відрізнити від інших осіб.

8. Система е-голосування надає користувачеві доступ лише після автентифікації його/його як особи з правом голосу.

9. Система е-голосування забезпечує подачу, збереження в електронній скриньці та включення до результатів виборів лише відповідну кількість голосів на одного виборця.

III. Вільне виборче право

10. Система голосування чи будь-який неправомірний вплив не повинні впливати на намір виборця.

11. Забезпечується, щоб система електронного голосування представляла виборцю автентичний бюлетень та достовірну інформацію.

12. Спосіб, яким виборці керуються в процесі електронного голосування, не повинен спонукати їх проголосувати поспішно або без підтвердження.

13. Система електронного голосування надає виборцю можливість брати участь у виборах чи референдумі без надання виборцем переваги будь-якому з варіантів голосування.

14. Система електронного голосування повідомляє виборця, який проголосував, про недійсність голосування.

15. Виборець має бути в змозі переконатися, що його чи її намір точно відображено під час голосування і що запечатаний голос потрапив в електронну скриньку без змін. Будь-який неправомірний вплив, який змінив голосування, має бути виявлений.

16. Виборець отримує підтвердження системою про те, що голосування пройшло успішно і що вся процедура голосування завершена.

17. Система е-голосування повинна надавати надійні докази того, що кожен автентичний голос точно входить до відповідних результатів

виборів. Докази мають бути перевірені засобами, незалежними від системи е-голосування.

18. Система повинна надавати надійні докази того, що лише голоси виборців, які мають право голосу, були включені до відповідного остаточного результату. Докази мають бути перевірені засобами, незалежними від системи е-голосування.

IV. Таємне виборче право

19. Електронне голосування організовується таким чином, щоб забезпечити дотримання таємниці голосування на всіх етапах процедури голосування.

20. Система е-голосування обробляє та зберігає у міру необхідності лише персональні дані, необхідні для проведення електронних виборів.

21. Система е-голосування та будь-яка уповноважена сторона захищають дані аутентифікації, щоб неуповноважені сторони не могли зловживати, перехоплювати, змінювати або іншим чином отримувати інформацію про ці дані.

22. Списки виборців, які зберігаються в системі е-голосування або передаються за допомогою системи е-голосування, доступні лише уповноваженим особам.

23. Система е-голосування не надає виборцю підтвердження змісту поданого голосу для використання третіми особами.

24. Система е-голосування не дозволяє комусь розголошувати кількість голосів, поданих за будь-який варіант голосування до моменту закриття електронної скриньки для голосування. Ця інформація не підлягає розголошенню громадськості до закінчення періоду голосування.

25. Е-голосування забезпечує дотримання таємниці попереднього вибору, записаного та стертого виборцем до того, як він проголосував.

26. Процес е-голосування, зокрема етап підрахунку голосів, має бути організований таким чином, щоб неможливо було відновити

зв'язок між відданим голосом і виборцем. Голосування є і залишається анонімним.

V. Нормативно-організаційні вимоги

27. Держави-члени, які впроваджують електронне голосування, повинні робити це поступово та прогресивно.

28. Перед впровадженням електронного голосування держави-члени вносять необхідні зміни до відповідного законодавства.

29. Відповідне законодавство регулює обов'язки щодо функціонування систем електронного голосування та забезпечує контроль за ними органом управління виборами.

30. Будь-який спостерігач має можливість спостерігати за підрахунком голосів. Відповідальність за процес підрахунку голосів несе орган управління виборами.

VI. Прозорість і спостережливість

31. Держави-члени повинні бути прозорими в усіх аспектах е-голосування.

32. Громадськість, зокрема виборці, задовго до початку голосування інформується зрозумілою та простою мовою про:

- будь-які дії, які виборець може зробити, щоб взяти участь і проголосувати;
- правильне використання та функціонування системи е-голосування;
- графік е-голосування, включаючи всі етапи.

33. Компоненти системи електронного голосування розкриваються з метою перевірки та сертифікації.

34. Будь-який спостерігач, у межах, дозволених законом, має право спостерігати та коментувати електронні вибори, у тому числі підбивати результати.

35. Відкриті стандарти повинні використовуватися, щоб уможливити взаємодію різних технічних компонентів або послуг, отриманих з різних джерел.

VII. Підзвітність

36. Держави-члени розробляють технічні, оціночні та сертифікаційні вимоги та перевіряють, що вони повністю відображають відповідні правові та демократичні принципи. Держави-члени повинні оновлювати вимоги.

37. Перед запровадженням системи електронного голосування та через відповідні проміжки часу після цього, зокрема після будь-яких істотних змін у системі, незалежний компетентний орган оцінює відповідність системи електронного голосування та будь-якого ІКТ-компоненту з технічними вимогами. Це може мати форму офіційної сертифікації або іншого відповідного контролю.

38. Сертифікат або будь-який інший відповідний документ, що видається, повинні чітко ідентифікувати предмет оцінки та включати запобіжні заходи для запобігання його таємної чи ненавмисної модифікації.

39. Система е-голосування підлягає аудиту. Система аудиту повинна бути відкритою та всеохоплюючою та активно повідомляти про потенційні проблеми та загрози.

VIII. Надійність і безпека системи

40. Орган управління виборами несе відповідальність за дотримання всіх вимог навіть у разі збоїв і нападів. Відповідальність за доступність, надійність, зручність використання та безпеку системи е-голосування несе орган управління виборами.

41. До центральної інфраструктури, серверів і даних про вибори мають доступ лише уповноважені органом виборчого процесу особи. Призначення осіб, уповноважених здійснювати е-голосування, має бути чітко регламентовано.

42. Перед проведенням будь-яких е-виборів орган управління виборами повинен переконатися, що система е-голосування є справжньою та працює правильно.

43. Встановлюється порядок регулярного встановлення оновлених версій та виправлень усього відповідного програмного забезпечення.

44. Якщо голоси зберігаються або передаються поза контрольованим середовищем, голоси мають бути зашифровані.

45. Голоси та інформація про виборців зберігаються запечатаними до початку підрахунку голосів.

46. Виборчий орган повинен безпечно поводитися з усіма криптографічними матеріалами.

47. У разі виникнення інцидентів, які можуть загрожувати цілісності системи, особи, відповідальні за експлуатацію обладнання, негайно повідомляють про це орган управління виборами.

48. Достовірність, доступність і цілісність реєстрів виборців і списків кандидатів зберігаються. Джерело даних має бути перевірено. Необхідно дотримуватись положень щодо захисту даних.

49. Система електронного голосування визначає голоси, на які впливають порушення.

9.3. Досвід електронного голосування США

Е-голосування вже запроваджено США, Канаді, Бразилії, Індії, Бельгії, Австралії, Естонії, Південній Кореї.

У Великобританії, Німеччині, Франції, Іспанії, Португалії, Італії, Норвегії, Швейцарії, Росії, Казахстані, Японії, Китаї проводяться експерименти з його використання.

Цікавим є досвід електронного голосування в США, розпочинаючи з 2004 року все більше фіксується проблем, які виникають під час його використання.

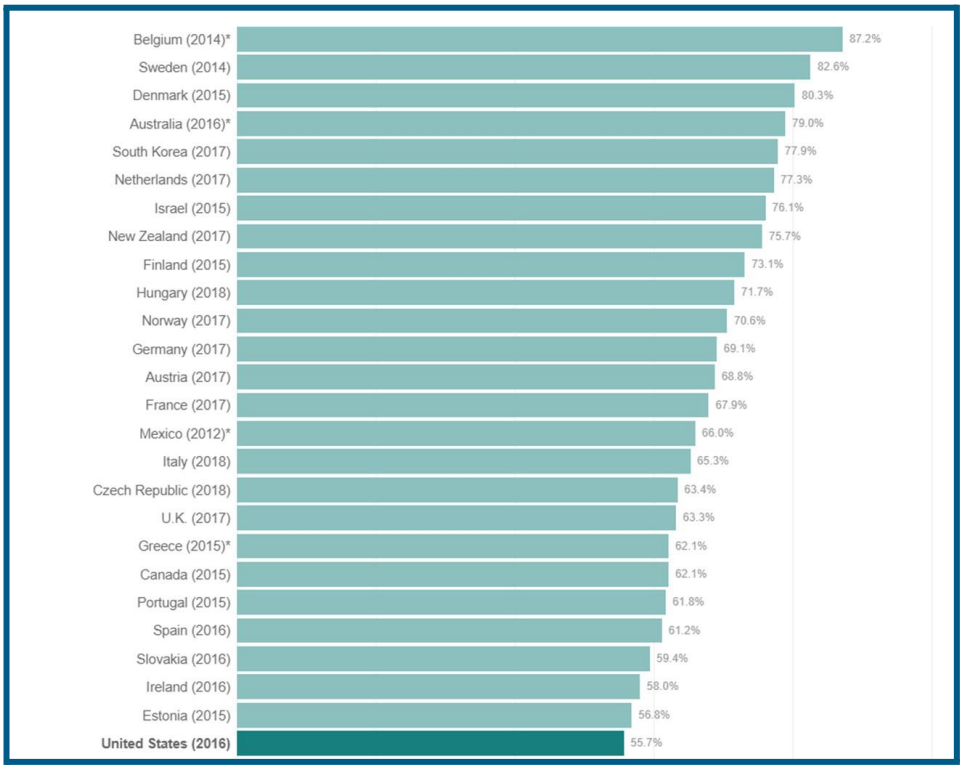

Рис. 7.3.1. Участь американських виборців у голосуванні

Загальна процедура е-голосування:

- Виборець отримує ключ електронного цифрового підпису.
- У день голосування з використанням комп'ютера, підключеного до Інтернет, виборець за допомогою відкритого ключа дістає доступ до сторінки зі своїми персональними даними і віртуального бюлетеня (списку кандидатів або партій) на спеціальному веб-сайті.
- Виборець вибирає одного з кандидатів або партійний список.
- Система пропонує підтвердження вибору, вказуючи номер, прізвище і ім'я кандидата (або політичну партію), відзначених виборцем.
- Виборець підтверджує свій вибір за допомогою закритого ключа електронного цифрового підпису.
- Система видає повідомлення про закінчення голосування

Види процедур е-голосування:

Віддалене голосування за допомогою Passport ID та інтернету.

Процес голосування: виборець під'єднує свою ID картку в картрідер, переходить на сайт ЦВК, логіниться за допомогою пін-коду та потрапляє до електронного бюлетеня, голосує та підтверджує піном свій вибір. Голос виборця вже опрацьовано, враховано та оприлюднено онлайн.

Фізичне голосування на дільницях з підрахунком за допомогою електронних урн.

Цей процес голосування схожий на традиційний, але кожен бюлетень вкидається не в прості пластикові урни, а в цифрову урну, яка підключена до інтернету та після зчитування бюлетеня система автоматично розпізнає голос і підраховує результати.

Голосування за допомогою спеціальних цифрових терміналів.

Спеціальні цифрові термінали - це комп'ютери з сенсорними екранами на зразок тих, де поповнюють мобільний рахунок. Такі термінали можуть бути багатофункціональні з можливістю авторизації через Passport ID-картку або за допомогою звичайного паспорту через надання спеціального номеру для голосування від членів комісії

Найпоширеніші матеріально-технічні засоби:

Vote-recording Technologies - заповнений бюлетень поміщають до виборчої машини, яка реєструє відображене на виборчому бюлетені чи іншій картці результат волевиявлення та здійснює автоматичний підрахунок результатів голосування.

Перфоровані карти (Punched Card) використовуються разом з машинами для голосування, які залишають отвір в перфокарті, що і становить процес голосування, після чого виборець опускає перфокарту до виборчої скрині.

Оптичне сканування (Optical Scan Marksense) передбачає здійснення виборчою машиною зчитування інформації оптичними засобами.

Електронна виборча система прямого запису (Direct-recording Electronic Voting System – DRE) – це голосування шляхом запису голосу

за допомогою електронного дисплея, забезпечене механічними або оптико-електронними компонентами, які можуть бути активовані виборцем; при цьому вибір виборця обробляється за допомогою комп'ютерної програми.

Рис. 7.3.2. Види технологій голосування в США

Основними видами технологій голосування [78] в США є:

- папір з ручним підрахунком,
- машини з механічним важелем,
- машини для перфокарт,
- відсканові паперові бюлетені
- електронні пристрої прямого запису

Механічні важільні машини в США вперше використані в 1890-х роках, керуються виборцем, який вказує на свій вибір, натискаючи важіль поруч із обраним кандидатом. Коли виборець заходить до виборчої машини, він або вона тягне за великий важіль, який тягне завісу навколо виборця, забезпечуючи конфіденційність. У машині є механізм блокування, який не дає виборцю переголосувати, тобто голосувати за більше, ніж дозволену кількість кандидатів. Після того, як виборець закінчив, виборець знову тягне за великий важіль, що призводить до збільшення лічильників, пов'язаних з його чи її вибором, на одиницю, і машина готується до наступного виборця.

Наприкінці дня виборів голоси підраховуються, відкриваючи апарат і читаючи цифри на лічильниках, пов’язані з усіма кандидатами. За законом, механічні важільні машини більше не можуть використовуватися на федеральних виборах.

Рис. 7.3.3. Механічні важільні машини в США

Пристрої для голосування за перфокартами були розроблені в 1960-х роках і спиралися на модифіковані картки Холлеріта для запису голосів. У найпоширенішому варіанті машини для перфокарт в тримач вставляється чиста карта з попередньою оцінкою. Тримач містить бюлетень для голосування та набір мішеней, які пов’язують кожен вибір із позицією удару на картці. Якщо виборець хоче проголосувати за кандидата використовує стилус, щоб змістити крапку (попередньо набраний шматок паперу) і створити дірку в картці, пов’язану з номером кандидата. Коли виборець закінчив, бере бюлетень і кладе його в урну. Наприкінці дня виборів виборчі бюлетені підраховуються за допомогою пристрою для зчитування карток, як правило, у центральному виборчому офісі.

Як і важільні машини, перфокарти більше не можна використовувати на федеральних виборах, хоча іноді вони все ще використовуються на виборах штатів і місцевих.

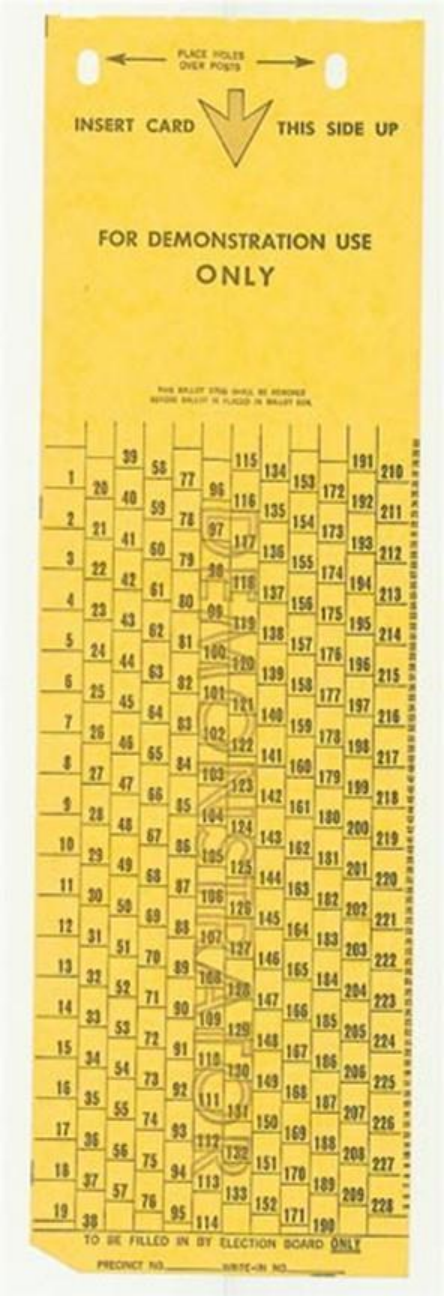

Рис. 7.3.4. Пристрої для голосування за перфокартами

Відсканові паперові бюлетені вперше були використані в 1960-х роках. Технологія, що використовується для оцінки стандартизованих тестів. Бюлетень маркується в приватній кабіні. Виборець використовує чорну ручку, щоб затемнити коло біля імені обраного кандидата. Потім кладе заповнений бюлетень у скриньку. Під час сканування на дільниці

сканер розташовується на виборчій скриньці, і бюлетень сканується під час його депонування, а голоси підраховуються наприкінці дня виборів шляхом виконання процедури на сканері дільничної комісії, яка роздруковує пов'язані з цим підсумки голосів. Загальні підсумки дільниці потім передаються в паперовому або електронному вигляді назад до центрального виборчого офісу.

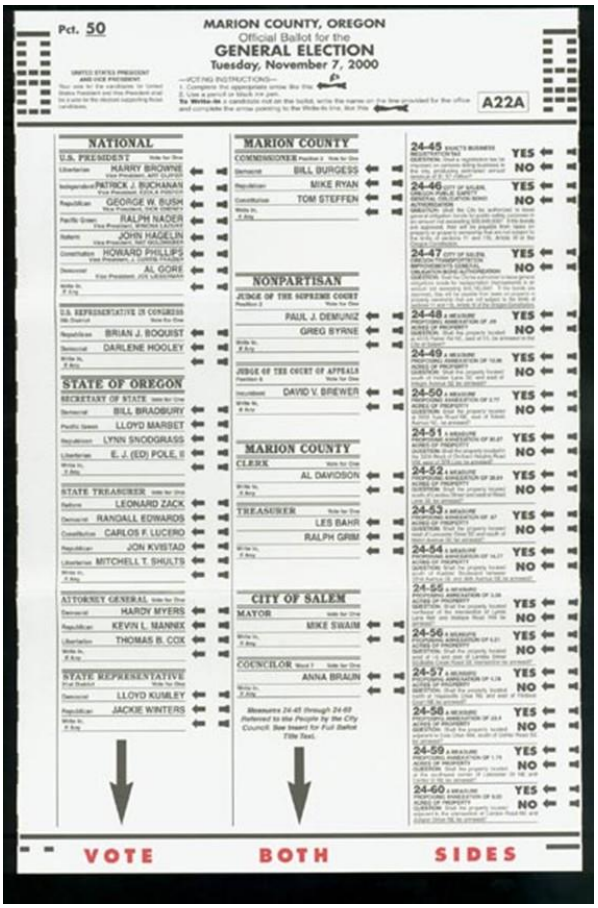

Рис. 7.3.5. Відсканові паперові бюлетені

Електронний прямий запис (DRE) - ця технологія коштувала 4 млрд. дол. і введена на виборчих дільницях в 42 штатах з 50. Вперше набули широкого застосування в 1970-х роках. Найперші DRE були, електронними версіями механічних важільних машин, з кнопками, які замінили важелі, а електричні накопичувачі замінювали механічні лічильники. Сьогодні DRE – це портативні комп'ютери, налаштовані на відображення варіантів голосування, а потім на електронний запис голосів. Вибір бюлетеня все частіше пропонується на сенсорному екрані комп'ютера, але деякі системи все ще покладаються на паперовий дисплей. Більшість сучасних DRE дозволяють виборцю вказати

голосування, натиснувши на сенсорний екран, хоча деякі системи покладаються на кнопки. Найперші DRE реєстрували голоси повністю за блоками внутрішньої пам’яті. Все частіше DRE також включають паперовий запис, який називається виборчим (або підданим перевірці) паперовим аудитом (VVPAT), який можна використовувати для перевірки або повторного підрахунку виборів.

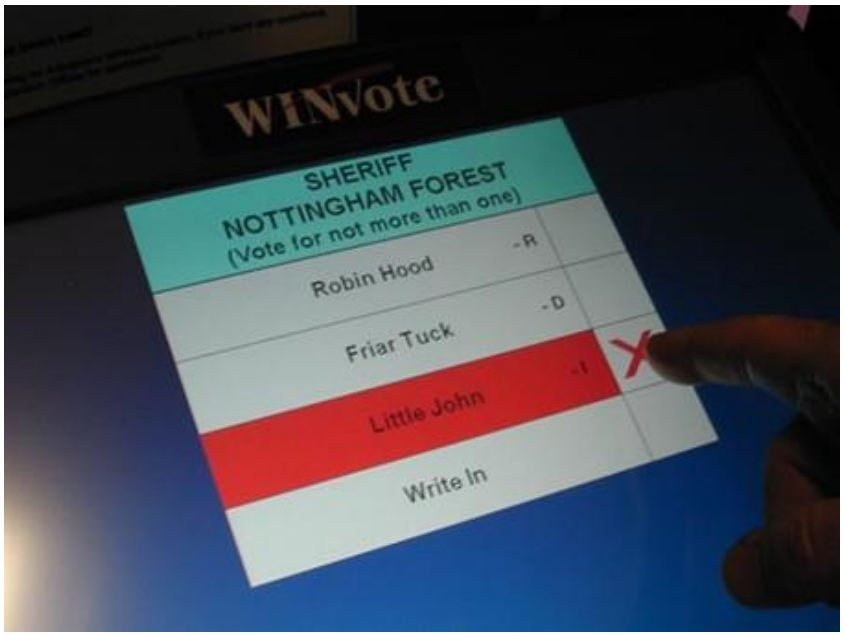

Рис. 7.3.6. Електронний прямий запис (DRE)

У США в останні роки використовуються такі типи обладнання для голосування:

- Системи для голосування з оптичним скануванням: виборці відзначають свої голоси, заповнюючи овал, квадрат або подібну форму на паперовому бюлетені. Паперові бюлетені скануються або на виборчій дільниці, або в центрі.
- Електронні системи прямого запису (DRE): системи DRE використовують комп'ютери, які записують голоси безпосередньо в пам'ять комп'ютера. Ці інтерфейси можуть включати сенсорні екрани, циферблати або механічні кнопки. Вибір виборця зберігається комп’ютером на картриджі або жорсткому диску. Деякі системи DRE також оснащені принтерами Voter-Verified Paper Audit Trail (VVPAT), які створюють паперові записи, які можна

зберегти для зведення в таблицю на випадок аудиту або повторного підрахунку.

- Пристрої та системи маркування бюлетенів (BMD): BMD "дозволяє електронне представлення виборчого бюлетеня, електронний вибір дійсних варіантів конкурсу та виготовлення паперового бюлетеня для голосування, який можна читати людиною, але не робить жодного іншого довготривалого запису вибору виборців». Спочатку використовувані в основному для розміщення виборців з обмеженими можливостями, BMD використовуються всіма виборцями в деяких місцях.

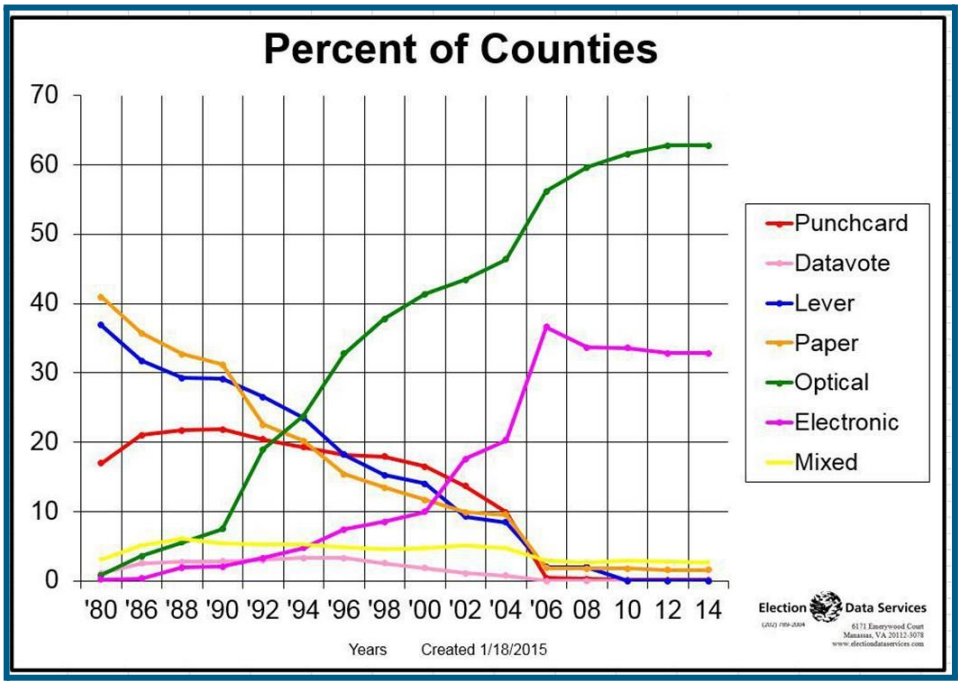

Рис. 7.3.7. Статистика голосувань за видами в США

9.4. Досвід електронного голосування в Естонії

Одним із лідерів щодо впровадження електронного голосування є Естонія. У 2005 році було прийнято Закон «Про електронні вибори», завдяки якому громадяни Естонії стали першими у світі, які в 2005 році проголосували на місцевих виборах в Інтернет-режимі (за допомогою ID-картки або мобільного-ID незалежно від того, перебувають вони вдома чи подорожують за кордоном). За допомогою цієї технології проголосувало 9 тисяч громадян (близько 2% від тих, хто прийняв участь у виборах). Станом на 2014 рік – кожен третій виборець

проголосував за допомогою інтернет-голосування. Вже вісім разів відбулося е-голосування в Естонії: на місцевих виборах у жовтні 2005 року, жовтні 2009 року і жовтні 2013 року; парламентських виборах у березні 2007 року, березні 2011 року та березні 2015 року; у виборах до Європейського парламенту у червні 2009 року та травні 2014 року.

На спеціальному веб-сайті (http://www.vvk.ee/valijale/e-haaletamine/) можна детально ознайомитися з електронним голосуванням в Естонії (Рис.7.4.1.).

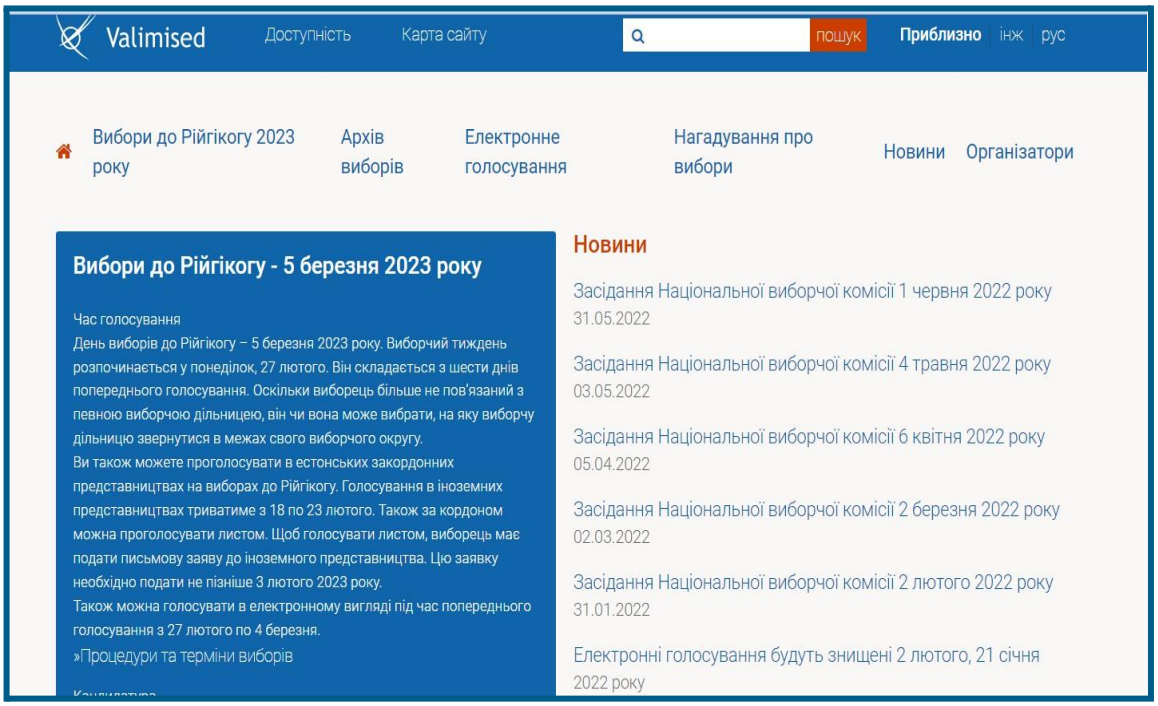

Рис. 7.4.1. Сайт з електронного голосування Естонії

Слід відзначити, що 7 грудня 2012 року Національною виборчою комісією Естонії було сформовано відокремлений виборчий орган - Комітет з електронного голосування (КЕГ), до основних обов'язків якого належать: підготовка та організація електронного голосування, з метою уникнення будь-яких випадків, які перешкоджають електронному голосуванню у відповідності до закону [15].

В 2017 році була запроваджена Система електронного голосування, заснована на загальних принципах електронного голосування. Однак ця структура є універсальною і застосовною до різних виборів. Загальна структура узагальнює вимоги до системи

електронного голосування, визначає учасників системи та описує їх діяльність та основні процеси електронного голосування, а також надає огляд можливостей для перевірки правильності системи та відповідності з основними вимогами.

Електронне голосування має декілька етапів *[15]*:

І. Підготовка.

Е-голосування організовується Державною виборчою службою (ДВС) у співпраці з Управлінням інформаційної системи (УІС). Перед початком голосування Державна виборча служба готує систему i-voting і оприлюднює заявку виборця, необхідну для голосування, на сайті «valimised.ee». ДВС налагоджує систему електронного голосування. УІС створює пару ключів для шифрування (відкритий ключ) і розблокування (приватний ключ) голосів. Одиниці приватного ключа розподіляються між членами ДВС і представниками КЕГ. Встановлюються програма-селектор і програма керування. Налаштована система перевіряється під час випробування. Проводяться вибіркові голосування, вибір виборців реєструється.

ІІ. Голосування на дільницях та електронне голосування

Виборці ідентифікують себе в системі електронного голосування за допомогою мобільного ідентифікатора, ID-картки або цифрового посвідчення особи. Селектор може перевірити справжність програми. Контрольні суми та інструкції щодо аутентифікації доступні на веб-сайті valimised.ee. Виборець підтверджує свій вибір цифровим підписом (після шифрування голосу) за допомогою програми виборця. Додаток для виборців відображає список кандидатів, серед яких виборець може зробити вибір. Виборець робить вибір. Програма виборця шифрує голос виборця відкритим ключем, а виборець підтверджує вибір цифровим підписом. Потім заявка для виборців надсилає голос колектору. Колектор — це серверна система, яка отримує електронні голоси. Колектором на виборах керує УІС. Кожен голос, отриманий Колекціонером, буде помічено часовою міткою сторонньої служби реєстрації. Це дає змогу перевірити наприкінці електронного голосування, що електронна урна, передана УІС, повна. Виборець може

використовувати програму керування смартфоном, щоб перевірити, чи його голос дійшов до збирача, і переконатися, що він зробив свій вибір. Виборець також може перевірити факт голосування повторно за допомогою електронного голосування (відображається вказівка, що ви вже проголосували), а також вказавши список виборців на виборчій дільниці.

III. Розгляд виборчих бюлетенів та електронного голосування

Якщо виборець не міг голосувати вільно та/або таємно або виборець не довіряє використаному комп'ютеру, виборець може змінити свій голос, проголосувавши повторно в електронному вигляді або за допомогою паперових бюлетенів протягом періоду електронного голосування.

Або останнє електронне голосування, або, якщо виборець також проголосував на виборчій дільниці, враховується паперовий бюлетень. Після закінчення е-голосування інкасатор передає до Державної виборчої служби електронну інформацію, записану на зовнішньому носії, зміст якої підписує представник інкасатора.

Після завершення е-голосування державна виборча служба перевіряє відповідність електронних голосів, що зберігаються в колекторі, з голосами, зафіксованими в службі реєстрації, та цілісність цифрових підписів голосів, а також електронних виборців. у списку виборців.

Після закінчення періоду електронного голосування УІС скасовує повторні голоси, а перед підрахунком електронних голосів (увечері дня виборів) УІС скасовує електронні голоси тих, хто проголосував паперовим бюлетенем.

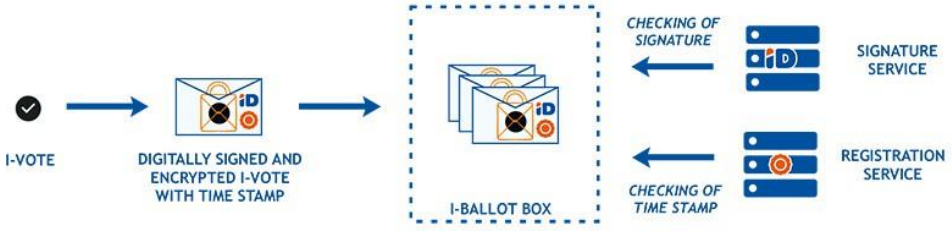

Рис. 7.4.2. Перевірка цілісності скриньки для голосування

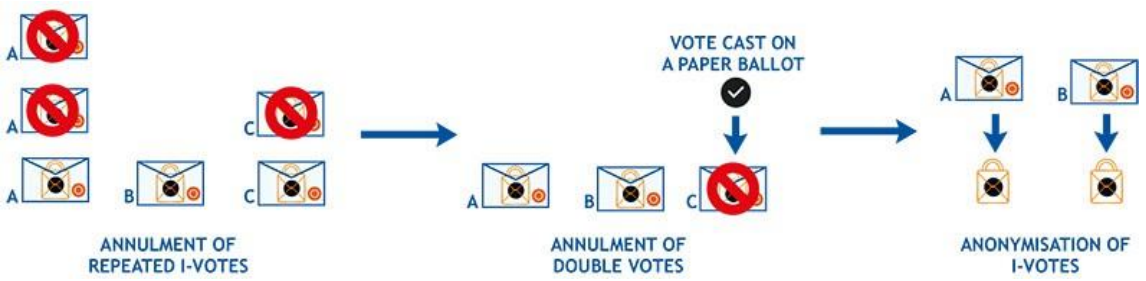

Рис. 7.4.3. Анулювання е-голосів

IV. Підрахунок голосів та перевірка результатів голосування

При читанні електронних голосів необхідно зберігати таємницю голосування виборця. Для цього при обробці персональні дані виборця (цифровий підпис) відокремлюються від електронного голосування.

Перед відкриттям електронного голосування зашифровані електронні голоси змішуються, щоб криптограми, які будуть зчитуватися, не можна було зіставити з криптограмами, які містяться в електронних голосах виборців.

Змішування відбувається в два етапи:

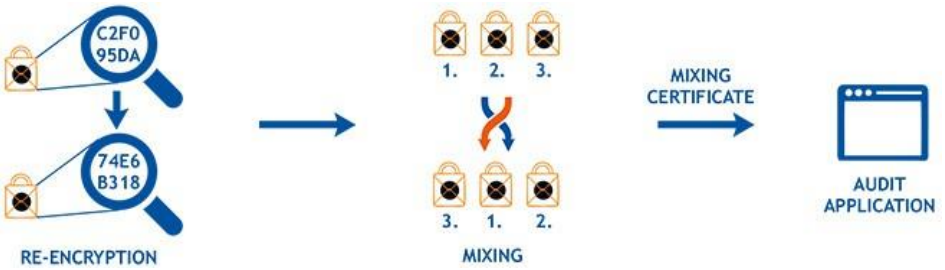

Рис. 7.4.4. Змішування е-голосів

1. Голоси мають бути зашифрованими. Для цього використовується окрема програма для змішування Verificatum.

   Для кожного зашифрованого голосу створюється нова криптограма. При цьому втрачається зв’язок між оригінальним електронним голосом і зашифрованою криптограмою (їхні криптограми тепер інші).

2. Зашифровані голоси будуть скрембловані, і зв'язок між вихідними голосами та порядком зашифрованих голосів буде втрачено.

Нарешті, на правильність змішування видається сертифікат змішування, який можна перевірити за допомогою аудиторської програми. Оскільки змішані голоси порівнюються з вхідними, які є незмішаними криптограмами, це робиться в контрольованому (закритому) середовищі.

Після змішування неможливо довести, що голос, зашифрований програмою виборця, при відкритті є розшифрованим голосом, оскільки криптограми різн і змішані. Це гарантує, що голосування зберігається в таємниці, а результати можуть бути ідентифіковані, а також перевірені публічно.

Читаний вибір є анонімним і не може бути повернений виборцю. Голоси розшифровуються за допомогою приватного ключа, доступ до якого ділиться між членами ДВС (7) та представниками КЕГ (2). Щоб розблокувати голоси, має бути принаймні 5 власників ключів. Після змішування відкриваються змішані голоси та підраховуються результати.

Рис. 7.4.5. Підрахунок е-голосів

Після закінчення підрахунку голосів видається довідка про читання про правильність відкриття електронних голосів, яку можна перевірити за допомогою аудиторської програми. Квитанція про прочитання дозволяє перевірити, що відкритий голос і криптограма пов’язані відкритим ключем.

Для перевірки доказів аудитору потрібен результат, змішані голоси та відкритий ключ.

Оскільки криптограми введених голосів були змішаними, а результат (або результат голосування) є відкритим, перевірку можна виконувати без обмежень, не боячись конфіденційності. Вихідний код програми аудиту можна безкоштовно завантажити та компілювати, щоб усі спостерігачі могли перевірити читання.

Голова Державної виборчої служби підписує результати електронного голосування після перевірки доброчесності. Достовірність та цілісність результатів виборів можна перевірити за допомогою файлу підпису, створеного під час підрахунку голосів за допомогою відкритого ключа.

Спостерігачі та аудитор можуть використовувати інструкції для контролю за ходом процедур електронного голосування. Аудитори повинні записати всі номери використаних наклейок.

Аудитор і, за бажанням, спостерігачі можуть за допомогою програми аудиту перевірити правильність підрахунку голосів за допомогою підтвердження читання.

Програма аудиту є загальнодоступною, і будь-хто може її скомпілювати (або написати власну програму).

Усі операції електронного голосування є публічними, електронний доступ до системи сервера голосування (Collector) обмежено з міркувань безпеки. Тут перевіряється цілісність даних (цілісність електронної урни та перевірка цілісності електронного голосування).

Результат голосування буде перевірено наступного дня під час другої перевірки цілісності електронного голосування.

Державна виборча служба зберігає електронні голоси не менше одного місяця з дня виборів. Після цього, але не до остаточного вирішення виборчих скарг, УІС знищить електронні голосування, персональні дані виборців, що містяться в системі електронного голосування, та ключ для відкриття електронного голосування.

Для е-голосування використовується застосунок е-голосування, проголосувати в якому можна на вибір, використовуючи для голосування ID-картку чи Mobile-ID.

Голосувати можна в публічних точках доступу до Інтернету, обладнаних комп'ютерами, які мають зчитувачі ID-карт.

Щоб уникнути ризиків, пов'язаних із безпекою комп'ютера, для е-голосування слід використовувати комп'ютер, який належить особисто виборцю або надійному адміністратору.

Щоб отримати SIM-карту Mobile ID, необхідно укласти договір про надання послуг у свого мобільного оператора.

Електронну заяву на отримання сертифікатів Mobile ID з державною гарантією необхідно подати на веб-сторінці Департаменту поліції та прикордонної охорони.

Голосувати за допомогою лише мобільного телефону неможливо.

Для голосування необхідно мати комп'ютер з підключенням до Інтернету. Але Mobile ID можна використовувати для ідентифікації особи та надання цифрового підпису. Мобільний телефон також необхідний для перевірки е-голосу, він допомагає підтвердити, чи правильно поводився комп'ютер під час е-голосування.

Система е-голосування дозволяє повторно голосувати. У разі повторного голосування зараховується лише останній поданий голос. Для повторного голосування необхідно запустити програму для виборців, дотримуючись наведених вище інструкцій. Система визначає, що виборець вже проголосував, і запитує підтвердження, що ви проголосуєте знову.

Якщо виборець голосував електронно кілька разів, його повторні «е-голоси» анулюються. Підставою для анулювання є час голосування; враховується останній за часом голосування. Е-голосування триває до 20:00 суботи виборчого тижня. Якщо виборець також проголосує бюлетенем на виборчій дільниці, його е-голос не враховується, а дійсним буде лише голос, поданий у паперовому бюлетені. З 2021 року

виборець може змінити свій е-голос, проголосувавши бюлетенем на виборчій дільниці до вечора дня виборів. Віддавши свій е-голос, виборець може перевірити за допомогою смартфона, чи враховано його.

Таблиця 7.4.1. Система електронного голосування в Естонії

Вибори до Європарламенту 2019	155521	73	155448	н/д	2555
Вибори	Е-виборці	Е-голосування Скасовано (замінено паперовими бюлетенями)	е-голоси підраховані	е-голоси недійсні (недійсні через нестандартний голос)	Кілька голосів І (замінено на е-голос)
Парламентські вибори 2019	247232	191	247041	н/д	6340
Місцеві вибори 2017	186034	163	185871	н/д	4527
Парламентські вибори 2015 року	176491	162	176329	1	4593
Вибори до Європарламенту 2014	103151	46	103105	1	2019
Місцеві вибори 2013	133808	146	133662	1	3045
Парламентські вибори 2011 року	140846	82	140764	н/д	4384
Місцеві вибори 2009 року	104413	100	104313	н/д	2373
Вибори до Європарламенту 2009 року	58669	55	58614	н/д	910
Парламентські вибори 2007 року	30275	32	30243	н/д	789
Місцеві вибори 2005 р	9317	30	9287	н/д	364

Стать	Чоловіки	Жінки
Вибори до Європарламенту 2019	71152	84369
Парламентські вибори 2019	112538	134694
Місцеві вибори 2017	87987	98047
Парламентські вибори 2015 року	83560	92931
Вибори до Європарламенту 2014	50000	53151
Місцеві вибори 2013	63963	69845
Парламентські вибори 2011 року	65396	75450
Місцеві вибори 2009 року	49343	55070
Вибори до Європарламенту 2009 року	28879	29735
Парламентські вибори 2007 року	15681	14594
Місцеві вибори 2005 р	5061	4256

Рис. 7.4.6. Е-виборці за статтю

9.5. Ризики та загрози при впровадженні е-голосування

Поєднання Інтернету та голосування це жахлива ідея, на думку представника спільноти кібербезпеки Сенатора Рон Уайден, штат Джорджія, яку він висловив у 2019 р: «Я вважаю, що це найгірше, що ви можете зробити з точки зору безпеки виборів в Америці, якщо не брати до уваги розміщення американських виборчих урн на московській вулиці».

Фахівці з кібербезпеки виокремили та описали низку **загроз**, які виникають або можуть виникнути під час електронного голосування, а саме [68]:

Електронний лист, який хтось із Вашингтона, округ Колумбія, надсилає комусь із усього міста, може передаватись через сервери в Далласі чи Мумбаї чи навіть через ворожі країни, такі як Росія, причому кожна зупинка надає можливість хакеру втрутитися в нього.

Навіть якби можна було б вимагати, щоб електронні виборчі бюлетені проходили через сервери лише в США, не існує жодного методу для забезпечення безпеки на кожному сервері на цьому шляху. Це все одно, що довірити FedEx доставку посилок, які повинні були пройти через склади з не замкненими дверима, відкритими вікнами та без камер безпеки.

Найефективнішим способом захисту даних на цих цифрових шляхах є наскрізне шифрування, яке скрембує вміст так, що він здається незрозумілим нікому, крім відправника чи одержувача. Експерти з питань безпеки голосування вважають, що це також перспективний інструмент для захисту виборчих бюлетенів, і Microsoft навіть створила безкоштовне програмне забезпечення, яке дозволить виборцям перевірити, чи правильно підраховані їхні зашифровані бюлетені.

Але програмне забезпечення, яке є новим і все ще тестується, працює лише на машинах для голосування, якими люди користуються особисто. Дослідники не з'ясували, як використовувати наскрізне шифрування в інтернет-голосуванні.

Пристрої людей вже можуть бути скомпрометовані - досить важко захистити бюлетень, коли він проходить через Інтернет, але те, що насправді не дає експертам спати вночі, це думка про те, що пересічні американці використовують свої комп'ютери або телефони для голосування.

Пристрої, підключені до Інтернету, переповнені шкідливим програмним забезпеченням, яке може безшумно маніпулювати своєю хост-машиною для безлічі цілей. За словами Джо Кінірі, головного науковця виборчої технічної компанії Free & Fair: «Середня Windows-машина, яку ми бачимо у світі сьогодні, безсумнівно, має певну форму шкідливого програмного забезпечення» [68].

Однією з проблем безпеки є «ботнети» - «армії шкідливих комп'ютерів, які хакери створюють, заражаючи орди погано захищених машин і наказуючи їм поширювати спам, шкідливе програмне забезпечення та інші цифрові загрози. Якби інтернет-голосування набуло широкого поширення, хакери могли б розбагатіти, здаючи в оренду свої бот-мережі людям, які хотіли підсадити зловмисне програмне забезпечення, що підмінює голоси».

Деякі ботнети містять мільйони комп'ютерів-зомбі. «Чи цього достатньо, щоб підмінити результати виборів?» — Ден Воллах, професор інформатики в Університеті Райса [68].

Що можуть зробити зловмисники?

- розміщення шкідливого програмного забезпечення на телефоні, планшеті чи комп'ютері виборця, щоб змінити бюлетень після його заповнення;
- впровадження шкідливого коду на виборчі веб-сайти, які отримують виборчі бюлетені, змінюючи декілька бюлетенів одночасно;
- підробка системи маршрутизації в Інтернеті, щоб вона направляла виборчі бюлетені через ворожий сервер, який змінює виборчі бюлетені, перш ніж відправити їх до виборчого офісу;
- обсадження виборчого сайту сміттєвим рухом, уповільнення або блокування його, щоб бюлетені не пройшли;
- підкуп довіреного співробітника виборчого офісу або його постачальника технологій, який може втрутитися в систему зсередини.

Чотири федеральні агенції, включаючи DHS і ФБР, виклали ці ризики в нещодавньому бюлетені для керівників виборів штатів [66] (Рис. 7.5.1.).

Технологія	Як це працює	Небезпека	ризику
Електронна доставка	Виборець отримує цифрову копію чистого бюлетеня електронною поштою або завантаження.	Хакер може підробити бюлетень до того, як він досягне виборця, наприклад, видаливши кандидата.	Низька
Маркування електронних бюлетенів	Виборець може заповнити бюлетень за допомогою телефону, комп'ютера або планшета, але все одно має надіслати його поштою або особисто.	Хтось міг би втрутитися в електронний вибір таким чином, що виборець не помічає перед голосуванням.	Помірний
Повернення електронного бюлетеня	Виборець повертає заповнений бюлетень онлайн. Західна Вірджинія, Делавер і Нью-Джерсі прийняли це для деяких виборців на цьогорічних виборах, включаючи людей з обмеженими можливостями.	Багато, включаючи ризик масової зміни голосів зловмисником.	Високий

Рис. 7.5.1. Ризики електронного голосування

У 2003 році при аналізі системи е-голосування програмного забезпечення в Університеті Джона Хопкінса виявили численні вразливості безпеки в системах електронного голосування. Дослідження було засноване на програмному забезпеченні, яке використовується в системах Diebold AccuVote-TS по всій країні. Як зазначив професор Ден Уолл в 2004 р.: "Дизайн і проектування системи була на диво паскудної і наївною."

При реалізованих електронних технологіях у виборця в США немає абсолютно ніякої можливості упевнитися, що голос, відданий через сенсорний екран за кандидата А, не приписаний машиною кандидату Б.

Девід Діллл, професор інформатики Стенфордського університету вважає, що важко одержати безпосередню інформацію про те, що саме відбувається в ході сертифікаційного процесу.

Бев Харріс вже не перший рік веде за допомогою друзів приватне розслідування. Підсумком роботи стала книга «Вибори з чорним ящиком: підробка голосування в 21 столітті» [43].

Питання для самоконтролю:

1. *Яка сутність електронного голосування?*
2. *Яка роль Венеціанської комісії щодо питань електронного голосування?*
3. *Охарактеризуйте основні стандарти електронного голосування, затверджені Радою Європи?*
4. *Назвіть етапи загальної процедури е-голосування в США?*
5. *Які є основні види технологій голосування в США?*
6. *Який є спеціальний сайт, де висвітлюються результати електронного голосування в Естонії?*
7. *Назвіть основні етапи процедури е-голосування в Естонії?*
8. *Які основні ризики та загрози впровадження системи е-голосування?*
9. *Які найбільші пересторогі є у фахівців з кібербезпеки щодо електронного голосування?*