

ВІД РЕДАКЦІЙНОЇ КОЛЕГІЇ

неофіційний переклад

РЕКОМЕНДАЦІЇ Ради Європи № R (2004)11 від 30 вересня 2004 року

“ПРО ПРАВОВІ, ОРГАНІЗАЦІЙНІ ТА ТЕХНІЧНІ АСПЕКТИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ”

Комітет міністрів Ради Європи, згідно з положеннями статті 15(b) Статуту Ради Європи – Зважаючи на те, що завдання Ради Європи полягає у досягненні більшої єдності її держав-членів в справі захисту і просування ідеалів та принципів, що є їх загальним надбанням,

Підтверджуючи свою упевненість у тому, що представницька і пряма демократія є частиною суспільних цінностей і основою для участі громадян в політичному житті на рівні Європейського Союзу, а також на національному, регіональному і місцевому рівнях,

Визнаючи зобов'язання, узяті в рамках існуючих правових інструментів, і поважаючи інші міжнародні документи, а саме:

- Загальну декларацію прав людини;
- Міжнародний Пакт про цивільні і політичні права;
- Конвенцію про ліквідацію всіх форм расової дискримінації;
- Конвенцію про ліквідацію всіх форм дискримінації відносно жінок;
- Європейську Конвенцію про захист прав людини і основоположних свобод і зокрема Протоколу № 1 до неї;
- Європейську хартію місцевого самоврядування;
- Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації;
- Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних;
- Рекомендації Комітету міністрів про захист персональних даних в Інтернеті № R(1999)5;
- Документ Копенгагенської наради - конференції по людському вимірюванню ОБСЄ;
- Кодекс добросовісної практики у виборчих справах, прийнятий Радою за демократичні вибори Ради Європи і Європейською Комісією за демократію через право,

Пам'ятаючи про те, що виборче право є одним з основоположних принципів демократії і, отже, що процедури системи електронного голосування повинні відповідати принципам демократичних виборів і референдумів,

Визнаючи, той факт, що новітні інформаційні технології все більше використовують в повсякденному житті, держави-члени мають враховувати це в своїй демократичній практиці,

Відзначаючи, що участь у виборах і референдумах на місцевому, регіональному і національному рівнях в деяких державах-членах характеризується низькою явкою виборців, яка в окремих випадках має тенденцію знижуватися,

Відзначаючи, що деякі держави-члени вже використовують або розглядають можливість застосування електронного голосування в різних цілях, включаючи:

- надання виборцям можливості голосувати не тільки на виборчій дільниці свого виборчого округу, але і в іншому місці;
- забезпечення подачі голосу самим виборцем;
- забезпечення участі у виборах і референдумах всіх, що мають право голосувати, і, особливо громадян, що проживають або тимчасово знаходяться за кордоном;
- розширення доступу до виборчого процесу виборцям-інвалідам або тим, кому неможливо бути фізично присутнім на виборчій дільниці і використовувати засоби, що є там;
- підвищення явки виборців шляхом надання додаткових каналів для голосування;

- проведення процесу голосування в умовах нових суспільних реалій і підвищення застосування нових технологій як засобу зв'язку та громадянської активності;
- скорочення з часом витрат виборчих органів на проведення виборів або референдумів;
- підвищення оперативності і надійності при передачі результатів голосування;
- надання виборцям вищого рівня послуг в цілях зміцнення демократії шляхом пропозиції різноманітних каналів для голосування,

Усвідомлюючи занепокоєння щодо деяких проблем безпеки і надійності, які, можливо, властиві окремим системам електронного голосування,

Розуміючи, що тільки безпечні, надійні, ефективні, технічно витривалі, відкриті для незалежної перевірки і легко доступні для виборців системи електронного голосування зможуть укріпити суспільну довіру, яка є необхідною умовою електронного голосування,

Р е к о м е н д у є урядам держав-членів в тих випадках, коли вони вже використовують або розглядають можливість застосування електронного голосування, дотримуватися на підставі нижченаведеного параграфу (iv), положення нижченаведених параграфів з (i) по (iii), а також стандартів і вимог по правових, організаційних і технічних аспектах електронного голосування в тому вигляді, в якому вони висловлені в Додатках до цієї Рекомендації, а саме:

(i) Електронне голосування має будуватися на демократичних принципах та бути надійним і безпечним, як вибори та референдуми, що проводяться без застосування електронних засобів. Даний загальний принцип стосується всіх виборних питань, незалежно від того, згадані вони в Додатках чи ні.

(ii) В ході практичного застосування цих Рекомендацій слід враховувати взаємопов'язаний зміст правових, організаційних і технічних аспектів електронного голосування в тому вигляді, в якому вони висловлені в Додатках.

(iii) Держави-члени повинні розглянути можливість перегляду відповідних частин свого національного законодавства у світлі положень цих Рекомендацій.

(iv) Разом з тим, принципи і положення, що містяться в Додатках, не вимагають від держав-членів зміни тих національних процедур голосування, які існували на момент ухвалення даної Рекомендації і які можуть продовжувати використовуватися цими державами-членами разом з системами електронного голосування до тих пір, поки дані національні процедури голосування відповідають всім принципам демократичних виборів і референдумів.

(v) Для того, щоб надати Раді Європи підстави для можливого подальшого удосконалення процесів електронного голосування, протягом найближчих двох років після ухвалення цих Рекомендацій Комітет міністрів рекомендує державам-членам:

- здійснювати нагляд за своєю політикою і досвідом відносно електронного голосування, особливо в частині виконання положень даної Рекомендації;

- надавати результати своїх спостережень в Секретаріат Рада Європи, яка направить їх державам-членам, і триматиме на контролі питання електронного голосування.

У Рекомендаціях нижченаведені терміни мають наступні значення:

- **аутентифікація** – представлення доказу достовірності особи або даних;

- **виборчий бюлетень** – юридично визнаний засіб, за допомогою якого виборець може зробити свій вибір серед наявних варіантів;

- **кандидат** – варіант вибору при голосуванні, що є особою і/або групою осіб і/або будь-якою політичною партією;

- **подача голосу** – розміщення голосу в ящик для голосування;

- **електронні вибори** або **електронні референдуми** – політичні вибори або референдуми, в яких на одній або більше стадіях застосовуються електронні засоби;

- **електронний ящик для голосування** – електронний засіб, в якому подані голоси зберігаються до початку їх підрахунку;

- **електронне голосування** – електронні вибори або електронний референдум, що включає застосування електронних засобів як мінімум при подачі голосів;

- **дистанційне електронне голосування** – електронне голосування, при якому подача голосу здійснюється за допомогою пристрою, непідконтрольного співробітнику виборчих органів;
- **опечатання** – захист інформації так, щоб її застосування або інтерпретація була неможлива без допомоги іншої інформації або засобів доступних тільки спеціально визначеним особам або органам влади;
- **голос** – вираз вибору серед наявних варіантів голосування;
- **виборець** – будь-яка особа, що має право проголосувати на виборах або референдумі;
- **канал для голосування** – спосіб, за допомогою якого виборець подає свій голос;
- **варіанти голосування** – набір варіантів, з якого робиться вибір за допомогою подачі голосу на виборах або референдумі;
- **список виборців** – список осіб, що мають право взяти участь в голосуванні (виборців).

Додаток 1

П р а в о в і с т а н д а р т и

А. Принципи

I. Загальне виборче право

1. Інтерфейс електронного голосування має бути зручним і зрозумілим виборцю.
2. Можливі реєстраційні вимоги при проведенні електронного голосування не повинні створювати перешкоду для участі виборця в електронному голосуванні.
3. Системи електронного голосування треба розробляти так, щоб максимально розширювати коло можливостей, що надаються подібними системами інвалідам.
4. При неможливості забезпечення загального доступу до каналів електронного голосування, їх використовують лише за бажанням виборця та як додатковий засіб голосування.

II. Рівне виборче право

5. При проведенні будь-яких виборів або референдумів необхідно попередити можливість подачі одним виборцем більше одного голосу в ящик для електронного голосування. Виборець повинен одержати можливість проголосувати тільки після того, як буде встановлено, що його/її голос ще не був поміщений в ящик для голосування.
6. Система електронного голосування не повинна допустити, щоб будь-який виборець міг подати голос за допомогою більш ніж одного каналу для голосування.
7. Кожний голос, поміщений в ящик для електронного голосування, має бути підрахований, а поданий на виборах або референдумі – включений в підрахунок тільки одноразово.
8. Там, де одночасно використовуються електронні і неелектронні канали для голосування, слід застосовувати безпечні і надійні методи підсумку голосів і встановлення правильного результату.

III. Вільне виборче право

9. Організація електронного голосування повинна забезпечити безпеку вільного формування і виразу думки виборця, а там, де це потрібне, і особистого здійснення виборчого права.
10. Процес, за допомогою якого виборці здійснюють електронне голосування, має бути таким, щоб запобігти можливості поспішного або необдуманого голосування.
11. У виборців має бути можливість змінити свій вибір на будь-якому етапі процесу електронного голосування до моменту подачі свого голосу або ж перервати саму процедуру без того, щоб їх попередній вибір був занесений в пам'ять системи або став доступний іншим особам.
12. Система електронного голосування має бути захищена від маніпулюючих дій на виборця в ході голосування.
13. Система електронного голосування повинна надати виборцю засіб для участі у виборах або референдумі, не створюючи при цьому у виборця будь-яких переваг відносно будь-яких варіантів вибору, наприклад, опускання паперового бюлетеня.

14. Система електронного голосування повинна чітко і ясно вказати виборцю на те, що його голос був успішно прийнятий, і що вся процедура голосування завершена.

15. Система електронного голосування повинна запобігти можливості зміни змісту поданого голосу після того, як він був поданий.

IV. Таємниця голосування

16. Електронне голосування слід організувати так, щоб на будь-якій стадії процедури голосування, особливо на стадії встановлення особи виборця, виключити все, що могло б порушити таємницю волевиявлення.

17. Система електронного голосування має гарантувати, що голоси, що знаходяться в ящику для електронного голосування, будуть підраховані і залишаться анонімними, та виключити можливість встановлення будь-якого зв'язку між поданим голосом і конкретним виборцем.

18. Система електронного голосування повинна бути сконструйована так, щоб очікуване число поданих голосів в будь-якому ящику для електронного голосування не давало можливості пов'язати одержаний результат з конкретними виборцями.

19. Під час електронної обробки даних необхідно вжити особливі заходи із недопущення використання та поширення інформації, яка веде порушенням таємниці голосування.

В. Процедурні захисні механізми

I. Прозорість

20. Держави-члени зобов'язані зробити кроки, спрямовані на те, щоб виборці розуміли особливості застосованої системи електронного голосування і відносилися до неї з довірою.

21. Інформація про роботу системи електронного голосування повинна знаходитися у відкритому доступі.

22. Виборці мають дістати можливість попрактикуватися у застосуванні нового способу електронного голосування до моменту проведення електронного голосування.

23. Будь-які спостерігачі, в тій мірі, в якій це допустимо згідно із законом, повинні мати нагоду бути присутнім і спостерігати за голосуванням для вироблення своїх зауважень з електронного голосування, включаючи встановлення його результатів.

II. Здійснення контролю і підзвітність

24. Компоненти системи електронного голосування мають бути доступні компетентним виборчим органам, в тій мірі, в якій це необхідне для здійснення контролю і акредитації.

25. Перед введенням в експлуатацію системи електронного голосування, а також після того, як її вводять до ладу, особливо після внесення в систему змін, незалежний орган, призначений виборчими органами, повинен проводити перевірку коректності роботи системи електронного голосування і наявності всіх необхідних заходів її захисту.

26. Необхідно передбачити можливість проведення перерахунку голосів. Інші функції системи електронного голосування, що можуть вплинути на правильність результатів підрахунку, повинні передбачати можливість перевірки їх роботи.

27. Система електронного голосування не повинна виключати можливості проведення часткового або повного повторного проведення виборів або референдумів.

III. Стійкість і захищеність

28. Державні органи держав-членів мають забезпечити надійність і безпеку системи електронного голосування.

29. Необхідно вжити всі можливі заходи по запобіганню можливості фальсифікації даних або несанкціонованого втручання в роботу системи протягом всього процесу голосування.

30. Система електронного голосування має передбачати заходи по підтримці доступності своїх послуг протягом всього процесу електронного голосування. Особливо вона повинна забезпечити стійкість до неполадок, збоїв або спроб блокування доступу до послуги.

31. Перед початком електронних виборів або референдумів відповідальний виборчий орган повинен провести перевірку системи електронного голосування і визначити її достовірність і нормальну працездатність.

32. Доступ до центральної інфраструктури, серверів і виборчих даних має бути тільки у осіб, уповноважених на це виборчим органом. Необхідно мати порядок надання таких прав доступу. Будь-які технічні роботи мають виконуватися бригадами мінімум з двох осіб. Склад бригад треба постійно змінювати. Слід прагнути проводити подібні роботи не у виборний період.

33. В той час, коли ящик для електронного голосування відкритий, будь-які санкціоновані дії, що впливають на систему, повинні проводитися бригадами як мінімум з двох осіб, по даних діях треба скласти звіт, і ці дії повинні контролюватися представниками компетентного виборчого органу, а також спостерігачами за виборами.

34. Система електронного голосування повинна підтримувати доступність і цілісність поданих голосів. Крім того, вона повинна забезпечувати конфіденційність поданих голосів і тримати їх в опечатаному вигляді до початку підрахунку голосів. При зберіганні або передачі за межі контрольованого середовища подані голоси повинні шифруватися.

35. Інформацію про виборців треба зберігати в опечатаному вигляді до тих пір, поки зберігається можливість встановлення зв'язків між ними. На певному етапі електронних виборів або референдумів персональні дані виборця мають відділятися від даних про його волевиявлення.

Додаток 2

Організаційні стандарти

I. Повідомлення

36. Національні правові норми, що регулюють проведення електронних виборів або референдумів, повинні чітко визначати тимчасові рамки відносно всіх їх етапів проведення як до, так і після виборів або референдумів.

37. Проміжок часу, протягом якого дозволено проводити електронне голосування, не слід починати до офіційного повідомлення про вибори або референдуми. Зокрема для дистанційного електронного голосування такий період повинен бути визначений і доведений до відомості громадськості задовго до початку голосування.

38. Задовго до початку голосування виборці мають бути проінформовані в дохідливій формі про те, яким чином буде організоване електронне голосування, а також про всі дії, які виборець повинен зробити, щоб взяти в ньому участь і проголосувати.

II. Виборці

39. Списки виборців мають регулярно обновлюватися. Виборець повинен мати можливість перевірити інформацію, що міститься про нього/неї в списку і зажадати внесення виправлень.

40. Слід запроваджувати електронний список виборців і механізм, що дозволяє здійснювати реєстрацію виборців в режимі он-лайн, а також, якщо це необхідно, і подачі заявок на використання системи електронного голосування. Якщо для участі в електронному голосуванні потрібне представлення окремої заяви і/або інших дій з боку виборця, слід розглянути можливість проведення даної процедури в електронній формі і, по можливості, в інтерактивному режимі.

41. Для тих випадків, коли період реєстрації виборця і період голосування співпадають за часом, слід передбачити відповідний механізм встановлення особи виборця.

III. Кандидати

42. Рекомендується запроваджувати застосування режиму он-лайн для реєстрації кандидатів.

43. Створений і відкритий для доступу в електронному вигляді список кандидатів повинен бути доступний для громадськості також за допомогою інших засобів.

IV. Голосування

44. Україй важливо, щоб система електронного голосування була побудована так, щоб не дозволити жодному виборцю проголосувати більше одного разу.

45. Дистанційне електронне голосування може починатися і/або закінчуватися до відкриття виборчих дільниць, але не може продовжуватися після завершення голосування.

46. По кожному з каналів електронного голосування слід розробити і зробити доступними для виборця міри технічної підтримки і управління процедурою голосування. У випадку з дистанційним електронним голосуванням дані заходи повинні бути також доступні і по іншому, широко доступному каналу зв'язку.

47. Представлення варіантів голосування на екрані пристрою, що використовуються для електронного голосування, має бути неупередженим.

48. Електронний бюлетень, за допомогою якого здійснюється подача електронного голосу, не повинен містити ніякої іншої інформації про варіанти голосування окрім тих, які строго необхідні для подачі голосу.

49. Система електронного голосування не повинна виводити на дисплей інших повідомлень, які могли б вплинути на вибір виборця.

50. Перед подачею голосу за допомогою системи електронного голосування слід привернути увагу виборця до того, що електронні вибори або референдуми, на яких вони виказують своє рішення за допомогою електронних засобів, є реальними виборами або референдумами. При проведенні пробних випробувань системи необхідно звертати увагу учасників на той факт, що вони беруть участь не в реальних виборах або референдумах, а у проведенні випробувань одночасно з реальними виборами, та запропонувати їм проголосувати за допомогою тих каналів для голосування, які для цього визначені.

51. Система дистанційного електронного голосування не повинна надавати виборцю можливості отримання будь-якого підтвердження щодо змісту поданого їм голосу.

52. В умовах контрольованого середовища інформація про поданий голос (візуальна, аудіо) повинна зникати відразу, як він буде поданий. Якщо виборцю на виборчій дільниці видається паперове підтвердження участі в електронному голосуванні, він не повинен мати нагоди показати його будь-якій іншій особі або винести дане підтвердження за межі виборчої ділянки.

V. Результати

53. Система електронного голосування не повинна допускати розкриття даних про кількість голосів, відданих за той або інший варіант голосування до моменту закриття ящика для електронного голосування. Дану інформацію не слід доводити до відомості громадськості до тих пір, поки не завершиться встановлений період голосування.

54. Система електронного голосування повинна не допустити обробки інформації про подані голоси в рамках певним чином підібраних субблоків, що могло б призвести до розкриття волевиявлення окремих виборців.

55. Будь-яке декодування, що необхідно для підрахунку голосів, слід здійснити як щонайшвидше після завершення встановленого періоду голосування.

56. При проведенні підрахунку голосів представники виборчого органу повинні мати можливість взяти в ньому участь, а спостерігачі – спостерігати за його ходом.

57. Необхідно вести протокол підрахунку електронних голосів, що містить інформацію про час початку і закінчення підрахунку, а також прізвища присутніх при підрахунку осіб.

58. У випадку виникнення будь-якої неточності, що впливає на цілісність голосів, неправильні голоси мають бути перераховані окремо.

VI. Аудит

59. Система електронного голосування повинна піддаватися аудиту.

60. Висновки, одержані за наслідками аудиту, необхідно враховувати на майбутніх виборах і референдумах.

Додаток 3

Технічні вимоги

Розробку системи електронного голосування має здійснюватися враховуючи всебічну оцінку ризиків, пов'язаних з успішним проведенням конкретних виборів або референдумів. В сис-

темі електронного голосування повинна володіти належними і заснованими на даній оцінці ризиків механізмами захисту для боротьби з виявленими ризиками. Збої в наданні послуг або зниження їх ефективності повинні залишатися в заданих межах допустимого.

А. Доступність

61. Слід вжити заходи для того, щоб всі виборці могли використати відповідні програми і сервіси, і, якщо необхідно, забезпечити доступ до альтернативних способів голосування.

62. На всіх основних етапах процесу створення систем електронного голосування слід залучати користувачів до розробки їх дизайну, зокрема для того, щоб виявити можливі труднощі в їх застосуванні і перевірити простоту роботи з ними.

63. У тих випадках, коли це необхідно і можливо, слід безкоштовно надавати користувачам додаткові засоби, такі як, наприклад, спеціальні інтерфейси, або інші еквівалентні ресурси, такі як, наприклад, персональна допомога. Призначені для користувача засоби повинні, наскільки можливо, відповідати вимогам, висловленим в документі “Ініціатива по забезпеченню доступності Інтернету” (WAI).

64. При розробці нових засобів слід надавати увагу їх сумісності з вже існуючими засобами, включаючи ті, в яких застосовані технології для людей з фізичними недоліками.

65. Презентація варіантів голосування має враховувати особливості конкретного виборця.

В. Сумісність

66. Для забезпечення сумісності технічних компонентів або сервісів системи електронного голосування слід використовувати відкриті стандарти.

67. В даний час “Стандарт мови виділення для виборчих систем” (EML) є саме таким відкритим стандартом і його слід якнайширше застосовуватися у всіх майбутніх прикладних системах електронного голосування для забезпечення їх сумісності. Рішення про терміни упровадження EML повинно ухвалювати державами-членами. Версія стандарту мови EML, діюча на момент ухвалення цієї Рекомендації, і вся супутня документація доступні на Інтернет-сайті Ради Європи.

68. У тих випадках, коли до виборів або референдумів пред'являються особливі вимоги, необхідна адаптація для їх врахування. Це дозволить розширити або скоротити інформаційні потоки при одночасному збереженні сумісності із загальною версією стандарту EML. З цією метою рекомендується використання мов із структурованою схемою і шаблонних мов.

С. Робота систем (для центральної інфраструктури і клієнтських пристроїв, що працюють в контрольованому середовищі)

69. Компетентні виборчі органи повинні опублікувати офіційний список програмного забезпечення, що використовується в електронному голосуванні або референдумі. Держави-члени можуть виключати із списку дані, які впливають на їх захист. Як мінімум, слід перерахувати використовуване програмне забезпечення, його версії, дати інсталяції і дати його короткий опис. Слід розробити процедуру регулярної установки оновлених версій і виправлень для відповідних програмних засобів захисту. Необхідно забезпечити можливість проведення у будь-який час перевірки захищеності устаткування для голосування.

70. Відповідальні за справну роботу устаткування повинні мати план дій в надзвичайних ситуаціях. Будь-яка резервна система повинна відповідати тим же стандартам і вимогам, що і основна система.

71. Слід створювати і постійно мати достатні резерви для забезпечення безперебійного ходу голосування. Відповідні фахівці повинні бути готові приступити до роботи згідно порядку, розробленому компетентними виборчими органами.

72. Відповідальні за устаткування повинні мати чіткий порядок дій, який би забезпечив те, щоб устаткування і його робота відповідали встановленим вимогам протягом всього періоду голосування. Резервні служби повинні регулярно одержувати дані моніторингу.

73. Перед кожними виборами або референдумами слід проводити перевірку наявного устаткування відповідно до протоколу, складеного компетентними виборчими органами. Мета перевірки устаткування полягає в тому, щоб встановити його відповідність технічній специфікації. Результати перевірки повинні бути доведені до компетентних виборчих органів.

74. Будь-які технічні роботи повинні супроводжуватися стандартною перевіркою на внесення змін в систему. Про всі істотні зміни в ключовому устаткуванні необхідно повідомляти.

75. Устаткування для електронних виборів або референдумів треба розташовувати в безпечній зоні, де протягом всього періоду їх проведення забезпечується охорона від будь-якого втручання в їх роботу. На час проведення виборів або референдумів слід мати план евакуації на випадок стихійного лиха. Більш того, необхідно забезпечити надійне зберігання даних, що залишаються в системі після виборів або референдумів.

76. У разі виникнення нештатних ситуацій, що можуть поставити під загрозу цілісність систем, особи, що відповідають за роботу устаткування, повинні негайно сповістити про це компетентні виборчі органи, які вживатимуть необхідні заходи для усунення наслідків виниклої ситуації. Ступінь серйозності нештатної ситуації, що вимагає доповіді, повинна бути визначена наперед відповідними виборчими органами.

D. Безпека

I. Загальні вимоги (що відносяться до періоду до голосування, періоду голосування і періоду після голосування)

77. Необхідно вжити технічні і організаційні заходи для того, щоб не допустити безповоротні втрати даних у разі збою або будь-якої помилки, які можуть негативно позначитися на роботі всієї системи електронного голосування.

78. Система електронного голосування повинна забезпечувати захист персональних даних, що відносяться до приватних осіб. Необхідно забезпечити конфіденційність списків виборців, що зберігаються і передаються виборчою системою.

79. Для того, щоб забезпечити гарантовану роботу компонентів системи електронного голосування відповідно до заданих технічних специфікацій і доступність її сервісів, система повинна проводити регулярне тестування своєї роботи.

80. Залежно від категорії або функції користувача, система електронного голосування повинна обмежувати можливість доступу до своїх послуг тим набором послуг, які закріплені за даною категорією або функцією користувача. Перш ніж користувач дістане можливість роботи в системі, необхідно провести його аутентифікацію.

81. Система електронного голосування повинна забезпечити захист даних аутентифікації з тим, щоб неправомочні особи не могли зловживати нею, перехоплювати, змінювати або будь-яким іншим способом цілком або частково одержати інформацію про дані аутентифікації. При застосуванні систем в неконтрольованих приміщеннях доцільно проводити аутентифікацію з застосуванням засобів шифрування даних.

82. Слід забезпечити проведення безпомилкової ідентифікації виборців і кандидатів (унікальної ідентифікації).

83. Системи електронного голосування повинні генерувати надійні і достатньо повні дані для забезпечення проведення спостережень за виборами. Слід забезпечити можливість точного визначення часу появи даних для спостереження. Необхідно підтримувати автентичність, доступність і цілісність даних.

84. Система електронного голосування повинна мати надійні і синхронізовані між собою лічильники часу. Правильність роботи лічильника часу повинна забезпечити установку тимчасових відміток для аудиторських процесів і даних спостережень, а також дотримання тимчасових обмежень на реєстрацію, висунення кандидатів, голосування або підрахунок голосів.

85. Виборчі органи несуть загальну відповідальність за дотримання цих вимог з безпеки, що підлягає оцінці з боку незалежних органів.

II. Вимоги на етапах до голосування (для даних, що будуть використані на етапі голосування)

86. Слід забезпечити автентичність, доступність і цілісність списків кандидатів і списків виборців. Необхідно проводити аутентифікацію джерел надходження даних. При цьому слід врахувати вжиті заходи по захисту даних.

87. Факт того, що висунення кандидата і, якщо це потрібне згідно із законом, рішення кандидата і/або компетентного виборчого органу про згоду з висуненням, були здійснені у встановлені терміни, має бути документально підтверджений.

88. Факт проведення реєстрації виборців у встановлені терміни повинен бути документально підтверджений.

III. Вимоги на етапі голосування (для даних, що будуть використані на етапі після голосування)

89. Необхідно забезпечити цілісність даних, отриманих по завершенню етапу до голосування (списки кандидатів і виборців). Слід проводити аутентифікацію джерел надходження даних.

90. Слід зробити все необхідне, щоб система електронного голосування видавала виборцю автентичний бюлетень. У ситуації дистанційного електронного голосування виборець повинен бути проінформований про наявні механізми перевірки встановлення каналу зв'язку з офіційним сервером і автентичності запропонованого бюлетеня.

91. Факт того, що голос був поданий у встановлений термін, має бути документально підтверджений.

92. Необхідно вжити заходи для того, щоб захистити системи, що використовуються виборцями для голосування, від будь-якого впливу, який міг би вплинути на рішення виборця.

93. Вся залишкова інформація щодо рішення виборця або екранне його відображення повинні бути знищені відразу після того, як виборець проголосував. При дистанційному електронному голосуванні виборець повинен бути проінформований про порядок видалення, де це можливо, результатів голосування з пристрою, який використовувався для голосування.

94. На початку система електронного голосування повинна перевірити правомочність виборця взяти участь в голосуванні. Система електронного голосування повинна провести аутентифікацію виборця і забезпечити подачу і занесення в пам'ять ящика для електронного голосування цієї кількості голосів, яка приходить на одного виборця.

95. Система електронного голосування повинна забезпечити, щоб вибір виборця був точно відображений при голосуванні і цей голос поступив в ящик для електронного голосування.

96. Після завершення голосування жоден виборець не повинен мати доступ до системи електронного голосування. Разом з тим, прийом електронних голосів ящиком для електронного голосування системи повинен продовжуватися протягом ще деякого періоду часу, достатнього для компенсації затримок при проходженні повідомлень по каналу електронного голосування.

IV. Вимоги на етапах після голосування

97. Необхідно підтримувати цілісність даних, одержаних після закінчення голосування (голоси, списки виборців, кандидатів) та проводити аутентифікацію джерел надходження даних.

98. Процес підрахунку голосів повинен забезпечити точний підрахунок голосів. Результат підрахунку голосів має бути відтворюваним.

99. Система голосування повинна забезпечити доступність і цілісність ящика для електронного голосування і результату підрахунку голосів стільки часу, скільки це необхідно.

E. Аудит

I. Загальні вимоги

100. Система аудиту повинна розроблятися і упроваджуватися як складова частина системи електронного голосування. Аудиторські засоби мають бути на різних рівнях системи: локальному, прикладному і технічному.

101. Наскрізний аудит системи електронного голосування містити ведення облікових записів, забезпечення засобів моніторингу та засобів перевірки. Для виконання даних вимог повинні використовуватися ті аудиторські системи, які перераховані нижче в підрозділах II – V.

II. Ведення облікових записів

102. Аудиторська система має бути відкритою і всебічною та активно повідомляти про потенційні проблеми і загрози.

103. Аудиторська система повинна вести облік часу, подій і дій, включаючи інформацію: що відноситься до голосування, зокрема кількість: виборців, які мають право на голосування; поданих голосів; бюлетенів визнаних недійсними; підрахунків і перерахунку голосів. про атаки на систему електронного голосування і її комунікаційну інфраструктуру; про системні збої, несправності та інші недоліки в системі.

III. Моніторинг

104. Аудиторська система повинна забезпечувати можливість нагляду за ходом виборів або референдумів, а також можливість перевірки відповідності одержаних результатів і вживаних процедур вимогам відповідних правових норм.

105. Розголошення аудиторської інформації неправомочним особам є неприпустимо.

106. Аудиторська система повинна забезпечити збереження анонімності виборця.

IV. Здійснення контролю

107. Аудиторська система повинна забезпечити можливість перехресної перевірки, підтверджувати коректність роботи системи електронного голосування і точності одержаних результатів, щоб знайти випадки махінацій з боку виборців і довести, що всі підраховані голоси є дійсними та всі голоси підраховані.

108. Аудиторська система повинна здійснювати перевірку електронних виборів на предмет їх відповідності правовим нормам. Мета цього – переконливо показати, що одержані результати є точним віддзеркаленням автентичних волевиявлень.

109. Аудиторська система повинна бути захищена проти будь-яких атак, які могли б порушити її роботу, викликати зміну або втрату записів, що зберігаються в ній.

110. Держави-члени повинні вжити достатні заходи для забезпечення конфіденційності будь-якої інформації, одержаної будь-якою особою в ході виконання нею задач аудиту.

F. Акредитація

111. Держави-члени мають запровадити процес акредитації, який би дозволив проводити тестування і сертифікацію будь-якого компоненту інформаційних і комунікаційних технологій на предмет його відповідності технічним вимогам, запропонованих в цих Рекомендаціях.

112. З метою розширення міжнародної співпраці і запобігання дублювання в роботі, держави-члени повинні розглянути можливість приєднання своїх національних агентств до відповідних міжнародних угод про обопільне визнання сертифікатів відповідності, таких як, наприклад, Європейська співпраця за акредитацію (EA), Міжнародна співпраця по акредитації лабораторних випробувань (ILAC), Міжнародний акредитаційний форум (IAF).

Комітет міністрів РЄ – //www.coe.fr/cm

~~~~~ \* \* \* ~~~~~