УДК 004.771

д.т.н., проф. **Чернишев Д.О.** (КНУБА)
д.т.н., проф. **Хлапонін Ю.І.** (КНУБА)
к.т.н., доц. **Вишняков В.М.** (КНУБА)

DOI: https://doi.org/10.17721/2519-481X/2020/68-10

ДОСВІД ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ В ЗАКЛАДІ ВИШОЇ ОСВІТИ

Важливою проблемою на шляху розвитку електронної демократії є забезпечення довіри громадян до електронних систем голосування. Хоч існує чимало фактів впровадження таких систем, але у кожному разі виборці повинні приймати на віру, що персонал, який обслуговує систему, буде чесно і безпомилково виконувати роботу. Іншими словами, жодна з цих систем не надає виборцям достатніх і зрозумілих доказів про те, що таємниця їх голосів не може бути порушена, а результати підрахунку голосів не можуть бути сфальсифіковані. Відомо, що беззаперечною довірою виборців користуються системи, у яких громадяни виконують аудит усіх тих процедур, де можливі прояви шахрайства. Зараз такі системи є, але у них не використовується електронне голосування. Мета цієї роботи полягає у доведенні та практичному підтвердженні можливості побудови системи таємного електронного голосування у публічній мережі Інтернет з доступними для виборців засобами проведення аудиту усіх тих процесів, які можуть викликати недовіру під час проведення голосування. Проаналізовані принципи побудови систем електронного голосування з точки зору можливості забезпечення довіри громадян за рахунок повної відкритості для аудиту обраних програмно-апаратних рішень. Саме з використанням таких рішень побудована система, яку впроваджено у Київському національному університеті будівництва і архітектури для проведення виборів представників студентства до Ради студентського самоврядування. Також ця система використовується для проведення таємних голосувань на засіданнях Вченої Ради Університету у режимі online. Важливим практичним результатом даного впровадження є усунення обтяжливої процедури ручного підрахунку голосів, що у випадку засідання, яке відбулося 16 жовтня 2020 року, де кількість бюлетенів була 53, хоч з 85 членів Вченої Ради прийняли участь у голосуванні 53 (шестеро проголосували паперовими бюлетенями), полегшення було відчутним, бо в урні було на 2491 бюлетень менше. Крім того, комп'ютерний підрахунок є миттєвим і безпомилковим, а наявність автоматизованого аудиту усуває можливість для будь-яких підробок програмного забезпечення або позаштатного втручання персоналу у роботу сервера. Головна перевага звичайно та, що створюються умови для захисту від розповсюдження вірусної хвороби і не треба припиняти діяльність Вчених Рад під час карантину.

Ключові слова: електронна демократія, таємне електронне голосування у мережі Інтернет, довіра громадян до систем електронного голосування, прозорість побудови систем електронного голосування, автоматизований аудит системи електронного голосування.

Вступ. Однією з основних проблем на шляху розвитку електронної демократії є створення систем голосування, які б заслуговували на абсолютну довіру з боку громадян. Хоч існують факти впровадження подібних систем на рівні держав, але у кожному разі виборці повинні приймати на віру, що персонал, який обслуговує систему, буде чесно і безпомилково виконувати роботу. Іншими словами, жодна з цих систем не надає виборцям достатніх і зрозумілих доказів про те, що таємниця їх голосів не може бути порушена, а результати підрахунку голосів не можуть бути сфальсифіковані. Відомо, що беззаперечною довірою виборців користуються системи, у яких громадяни виконують аудит усіх тих процедур, де можливі прояви шахрайства. Наприклад, у громадян Італії не виникає підозр щодо чесності проведення виборів [1]. Слід зауважити, що там мова йде про голосування паперовими бюлетенями, де завдяки призначенню випадкових виборців для участі у підрахунку голосів і широкому доступі спостерігачів для аудиту усіх тих процесів, де можуть бути вчинені порушення, не виникає підстав для недовіри.

Метою цієї роботи є доведення та практичне підтвердження можливості побудови системи таємного електронного голосування у публічній мережі Інтернет з доступними для

виборців засобами проведення аудиту усіх тих процесів, які можуть викликати недовіру під час проведення голосування.

Аналіз опублікованих робіт. Метою цього аналізу є висвітлення шляхів щодо забезпечення довіри громадян до систем електронного голосування. Актуальність такого аналізу пояснюється тим, що наявність недовіри є фактором, який здатен завдати значну шкоду розвитку електронної демократії у цілому.

Кожна з робіт, яку ми проаналізуємо, висвітлює певну властивість системи електронного голосування, яка може претендувати на 100% довіру з боку громадян. Хоч не кожен громадянин зможе розібратись в особливостях електронних систем, але у сучасному суспільстві вже існує значна кількість фахівців яким це доступно. Важливо, що їх кількість зростає рік від року.

Перший крок у напрямку відкритості систем електронного голосування було зроблено відомим американським вченим Брюсом Шнайером, який у роботі [2] висловив рішучу заяву проти закритого програмного забезпечення машин для голосування. Він заявив: «Компанії, які виробляють ці машини, постійно стверджують, що вони повинні зберігати секретність свого програмного забезпечення з метою безпеки. Не вірте їм. У даному випадку секретність не має нічого спільного з безпекою.» Також у цій роботі Брюс Шнайер вказує на необхідність підвищення якості аудита програмного забезпечення систем електронного голосування і надає таку пораду щодо майбутніх розробок: «Якщо ми збираємось витрачати гроші на нові технології голосування, то є сенс витрачати їх на технології, які будуть спрощувати проблему, замість її ускладнення.» Фактично у цій роботі було закладено ідею створення простих і відкритих для аудиту систем електронного голосування, але ця ідея не була підтримана професійними розробниками, включаючи широко відому естонську систему електронного голосування [3]. Зрозуміло, що для професіоналів ідея спрощення не приваблива, бо це може негативно вплинути на їх фінансування. Як показує аналіз сучасних систем електронного голосування, їх продовжують ускладнювати [4]. Але ідею Брюса Шнайера було підтримано у студентській роботі «Відкрита система таємного голосування», яку опубліковано у 2014 у збірнику КНУБА (Київського національного університету будівництва і архітектури) [5]. У цій роботі обрано прості і досконалі рішення щодо забезпечення таємниці голосів виборців. По-перше, обрано серверну операційну систему *OpenBSD*, яка є єдиною сертифікованою в Україні для побудови систем захисту даних [6], а по-друге, для захисту персональних даних і голосів виборців обрано шифр Вернама, який забезпечує абсолютний захист даних від розкриття, що математично доведено в роботі [7]. Хоч використання цього шифру потребує виконання особливих умов, але перевагою є те, що виток даних під час передавання стає абсолютно неможливим, а це є важливою складовою для забезпечення довіри виборців. У таблиці надано перелік умов для абсолютного захисту даних під час передавання.

Таблиця

Умови забезпечення абсолютного захисту даних під час передавання

Умова	Опис виконання умови
Генерування випадкових бітових послідовностей (не псевдовипадкових)	Реалізовано метод генерування випадкових (не псевдовипадкових) бітів, який дозволяє генерувати випадкові послідовності на будь-якому комп'ютері, що описано у роботі [8].
Кожну випадкову бітову послідовність можна використовувати для шифрування тільки один раз	Для кожного сеансу зв'язку генеруються випадкові бітові послідовності незалежно одна від одної
Для обміну випадковими послідовностями бітів слід використовувати абсолютно захищений канал зв'язку	Обмін випадковими послідовностями бітів відбувається за алгоритмом Диффі- Хеллмана з такими параметрами, для яких у сучасних умовах не існує можливості розкриття даних.

У роботі [9] обґрунтовано вибір параметрів алгоритму Диффі-Хелмана для задачі електронного голосування, а у роботі [10] описано метод протидії атаці посередника, яка є можливою загрозою, у разі використання цього алгоритму.

Крім абсолютного захисту інформації від витоку під час передавання, для забезпечення 100% довіри щодо збереження таємниці голосів, слід також унеможливити виток інформації на сервері, де голоси розшифровуються і підраховуються. Це реалізовано завдяки операційній системі *OpenBSD*, яка дозволяє створювати захищену від будь-якого стороннього проникнення частину оперативної пам'яті, у якій підраховуються голоси. Ця технологія описана у роботі [11]. Таким чином, персональні дані виборців ніяк не можуть витікати зі сервера під час підрахунку голосів, бо їх розшифровка відбувається у захищеній частині оперативної пам'яті, де вони потрапляють на лічильник голосів, після чого ніякої інформації про те хто як голосував не залишається.

Крім збереження таємниці голосів для забезпечення повної довіри слід усунути можливість фальсифікації підрахунку голосів.

Зрозуміло, що у разі повної відкритості і багаторазового випробування програмного забезпечення, можна гарантувати відсутність помилок у підрахунку голосів, але не можна покладатись на чесність персоналу, який буде обслуговувати систему електронного голосування. Оскільки персонал, який зобов'язаний встановлювати і запускати програмне забезпечення, має можливість втручання у роботу сервера, то з метою недопущення з його боку позаштатних дій, у роботі [12] запропоновано проведення автоматизованого контролю усіх дій щодо управління сервером. При цьому кожен користувач мережі може проводити такий контроль. Але реалізація всього, що описано у перелічених роботах, може залишити привід для недовіри, бо потрібен ще контроль апаратних засобів, які розпізнають і підраховують голоси. У разі відсутності такого контролю може виникнути підозра, що зловмисник, з метою фальсифікації виборів, створив спеціалізоване обладнання, у якому закладено засоби імітації чесної роботи, а насправді є можливість втручання у процеси розпізнавання та підрахунку голосів. Усунути цю підозру дозволяє підхід, який описано у роботі [13], де запропоновано для серверів підрахунку голосів використовувати стандартні міні комп'ютери типу *Raspberry Pi* 3 з відкритим монтажем. При цьому, контролерам дозволено не тільки робити їх зовнішній огляд, але й підключати власні пристрої для копіювання файлів програмного забезпечення та виконання безпечних команд операційної системи. У таких умовах підробка серверного обладнання виходить за межі реальності через брак ресурсів для розміщення на цих міні комп'ютерах додаткового програмного забезпечення.

Усі перелічені технології реалізовані і надаються для голосування на серверах Державного підприємства ДНДІАСБ, яке є провайдером послуг у мережі Інтернет, про що свідчить інформація на їхньому сайті [14].

Електронне голосування у закладі вищої освіти. Згідно Плану заходів щодо реалізації Концепції розвитку електронної демократії в Україні на 2019-2020, який затверджено КМУ 12 червня 2019 р. №450-р із змінами, внесеними згідно з Постановою КМ № 123 від 05.02.2020 року, в закладах вищої освіти слід впроваджувати інструменти електронного голосування в діяльність органів студентського самоврядування [15]. Крім того, 15 липня 2020 року Урядом України внесено зміни до Порядку присудження наукових ступенів. Ці зміни дозволяють проведення засідань в дистанційному режимі з використанням сучасних засобів відео зв'язку, але голосування повинно залишатись таємним і відбуватись з використанням програмного забезпечення, яке обирає сама рада [16].

Судячи з Плану заходів Уряду України, бачимо, що таке важливе питання розвитку електронної демократії, як впровадження електронного голосування, покладено в першу чергу на заклади вищої освіти (ЗВО). Цей підхід суттєво відрізняється від того, який існував довгий час у інших країнах, де повністю покладались на професійних розробників і отримали потік критики через неможливість забезпечення довіри громадян, що описано у багатьох роботах дослідників, наприклад у цих [1, 4, 17]. При цьому, крім робіт наших студентів та аспірантів,

немає жодної, де було б вказано про можливість забезпечення беззаперечної довіри виборців до е-голосування.

Проблема забезпечення довіри полягає у тому, що люди тільки у разі можливості безперервного аудиту від початку голосування до закінчення підрахунку голосів можуть позбутися недовіри. Оскілки аудит цих систем потребує спеціальних знань, то для досягнення довіри необхідно набуття знань у галузі ІТ. Тому План Уряду щодо першочергового впровадження засобів е-голосування у ЗВО є доцільним, бо потрібні знання набуваються саме у закладах вищої та середньої освіти. Крім того, якщо студенти самі активують і створюють розробки, то програмно-технічні рішення будуть простішими і зрозумілішими, а це іде на користь досягненню довіри. Саме з цих міркувань було прийнято наше рішення щодо обрання засобів таємного дистанційного голосування.

Для систем таємного електронного голосування у ЗВО не всі вимоги відповідають тим, що існують на рівні держав. Тому треба було внести зміни у програмне забезпечення, яке запропоновано нашими фахівцями для виборів на державному рівні. Слід було доповнити систему можливістю управління періодами голосування під час засідань або зборів у режимі *online*. Для цього створено спеціальний інтерфейс, через який представник лічильної комісії або секретар засідання може керувати процесом голосування. Цей інтерфейс показано на рис. 1.

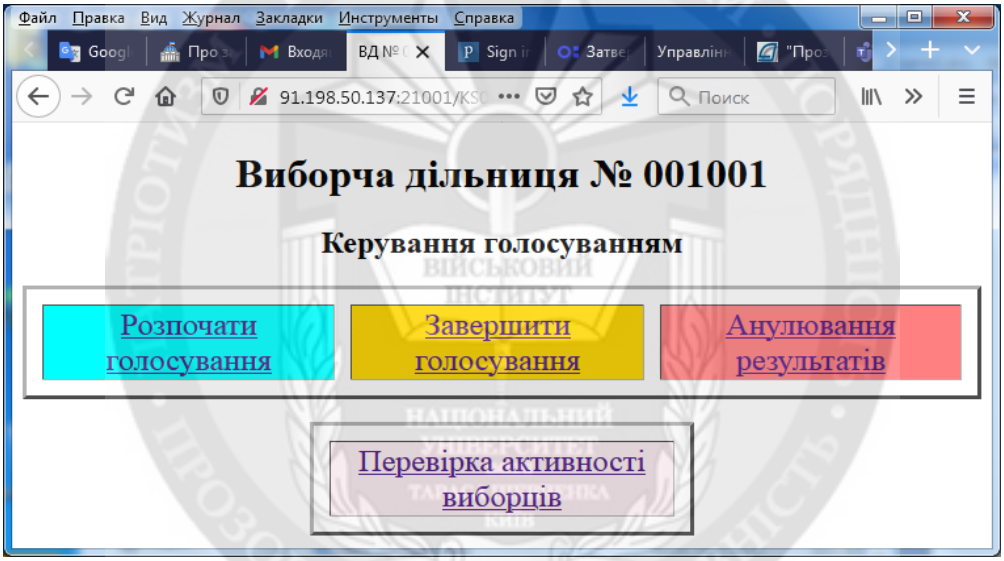

Рисунок 1 – Інтерфейс для управління процесом голосування

Через даний інтерфейс можна перевіряти активність виборців, що дозволяє у реальному часі дізнаватись хто вже проголосував. Це важливо у режимі *online*, бо можна нагадувати виборцям, які відволіклися, про необхідність проголосувати.

Поновлений інтерфейс виборців показано на рис. 2.

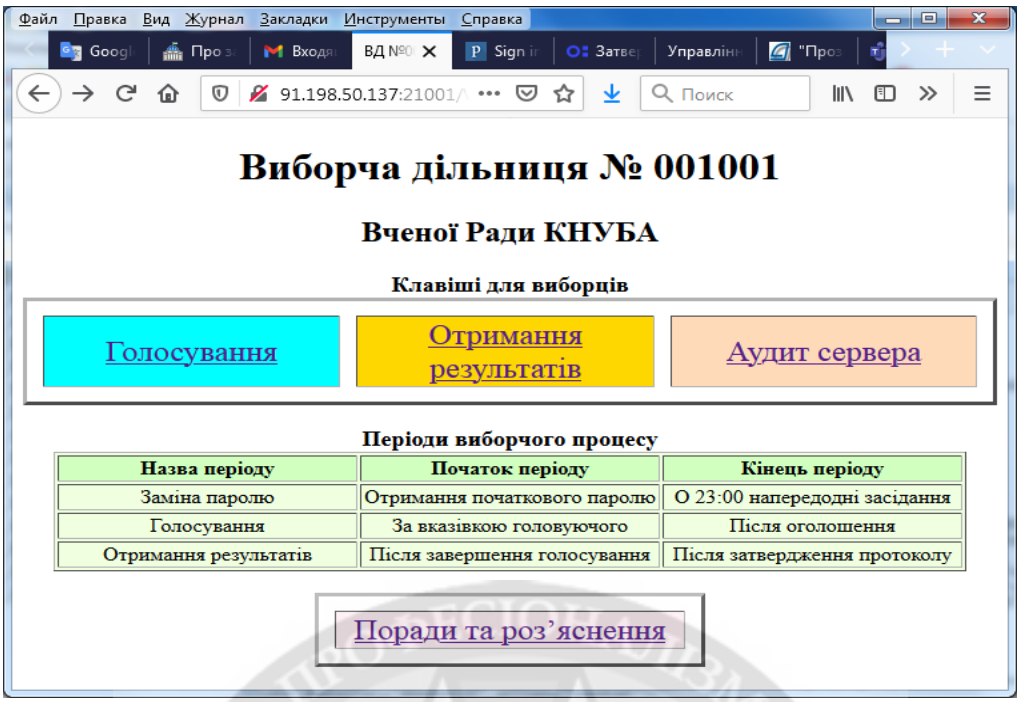

Рисунок 2 – Головний інтерфейс виборця

Вигляд бюлетенів для голосування на засіданні Вченої Ради показано на рис. 3, а сторінку з результатом голосування – на рис. 4.

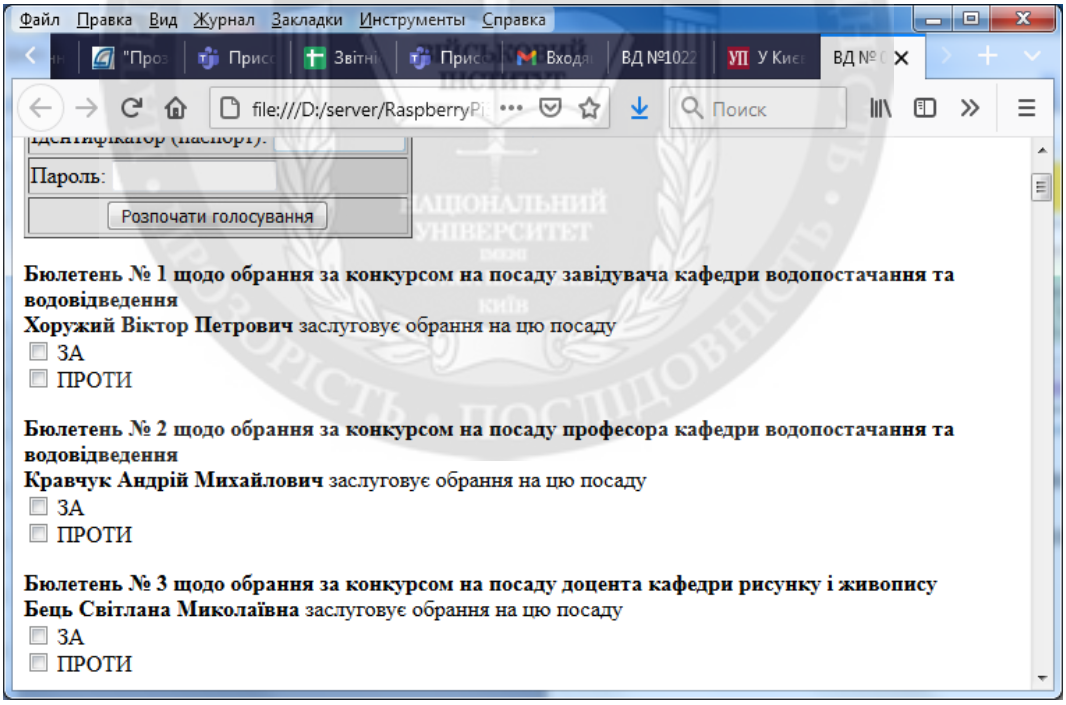

Рисунок 3 – Вигляд електронних бюлетенів на засіданні Вченої Ради

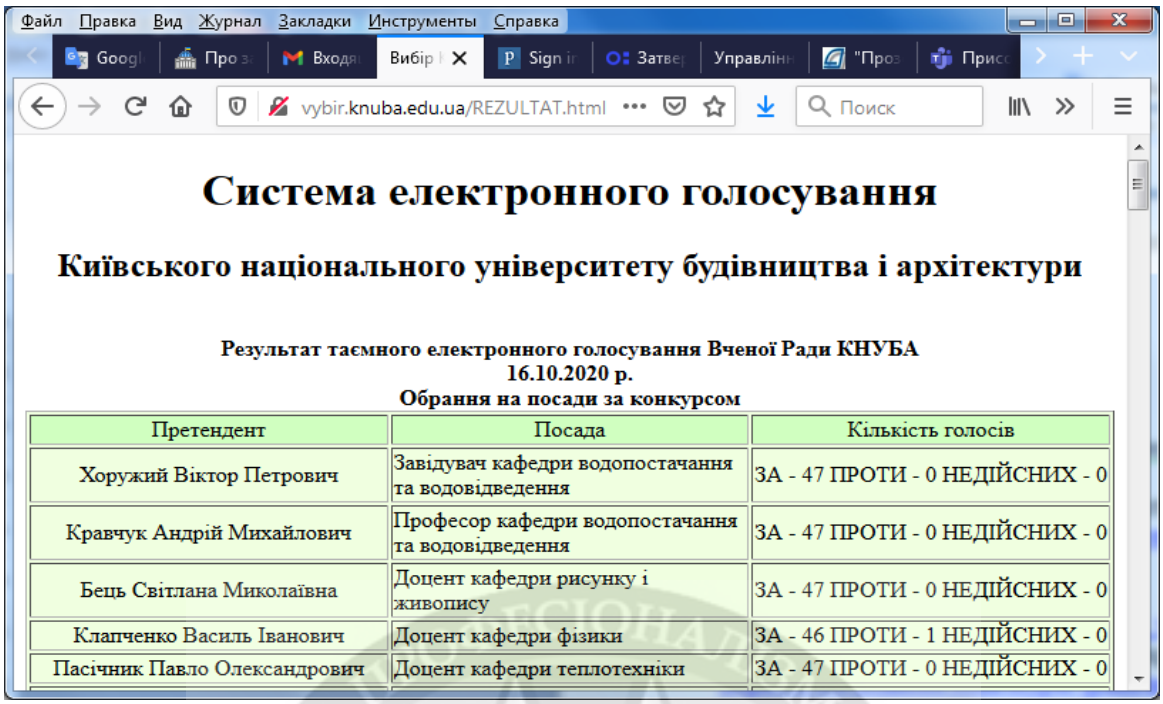

Рисунок 4 – Вигляд web сторінки з результатом голосування

Зміни у програмному забезпеченні з метою усунення зайвих перевірок, які не є доцільними у випадку проведення засідань або зборів у режимі *online*, були зроблені такі:

- усунено автентифікацію виборців по біологічним або іншим ознакам;
- усунено захист від впливу на виборців різними методами примусу.

При цьому в повному обсязі залишено такі властивості:

- абсолютну неможливість розкриття таємниці голосів;
- безперервний автоматизований контроль усіх програмно-апаратних засобів і процесів, які можуть стати приводом для недовіри виборців.

Слід зауважити, що аудит системи є доступним не тільки виборцям, а також і їх довіреним особам. Тому для проведення аудиту не обов'язково мати знання у галузі ІТ, а можна звернутись для цього до будь-яких фахівців.

Процедура підготовки до голосування полягає у тому, що реєстратор, якому адміністратор системи надає спеціальні повноваження, заповнює реєстр виборців по дільниці, яку він обслуговує. У цьому реєстрі, крім прізвища та ім'я слід вказати електронну пошту та унікальний ідентифікатор виборця, який є його початковим паролем. Ідентифікатори призначаються реєстратором за узгодженням з адміністратором таким чином, щоб не було повторень у межах установи. Для кожної групи голосуючих, наприклад, Вченої Ради, реєстр заповнюється одноразово, а перед кожним голосуванням слід лише вносити зміни та доповнення. Після занесення виборця до реєстру реєстратор відправляє йому повідомлення на електронну пошту. У цьому повідомленні надаються посилання для входу на web сторінку своєї виборчої дільниці та для заміни початкового паролю на свій постійний. Паролі виборці обирають і вводять самостійно від 8 до 16 символів на латинському регістрі. У будь-який момент до початку періоду голосування виборці можуть перевіряти та замінювати паролі. У разі, коли виборець не може пригадати пароль, реєстратор має можливість повернути йому початковий. Зауважимо, що реєстр виборців готується і зберігається на окремому комп'ютері, з якого на сервер голосування пересилається файл з паролями і ідентифікаторами у зашифрованому вигляді. Цей файл може пересилатись у відкритому вигляді, бо обраний шифр не підлягає розшифруванню. Таким чином на сервері голосування, де усі файли є відкритими для читання, не має персональних даних виборців, крім паролів і ідентифікаторів, які захищені шифром.

Процес голосування у переважній більшості випадків не викликає труднощів. Голосуючим, крім будь-якого пристрою з браузером і доступом до мережі Інтернет, нічого не потрібно. Усі процедури щодо управління системою голосування КНУБА, а також аудит серверів є у цілодобовому доступі за посиланням http://vybir.knuba.edu.ua/ через головну сторінку системи, що зображена на рис. 5, а сторінку для аудиту показано на рис. 6.

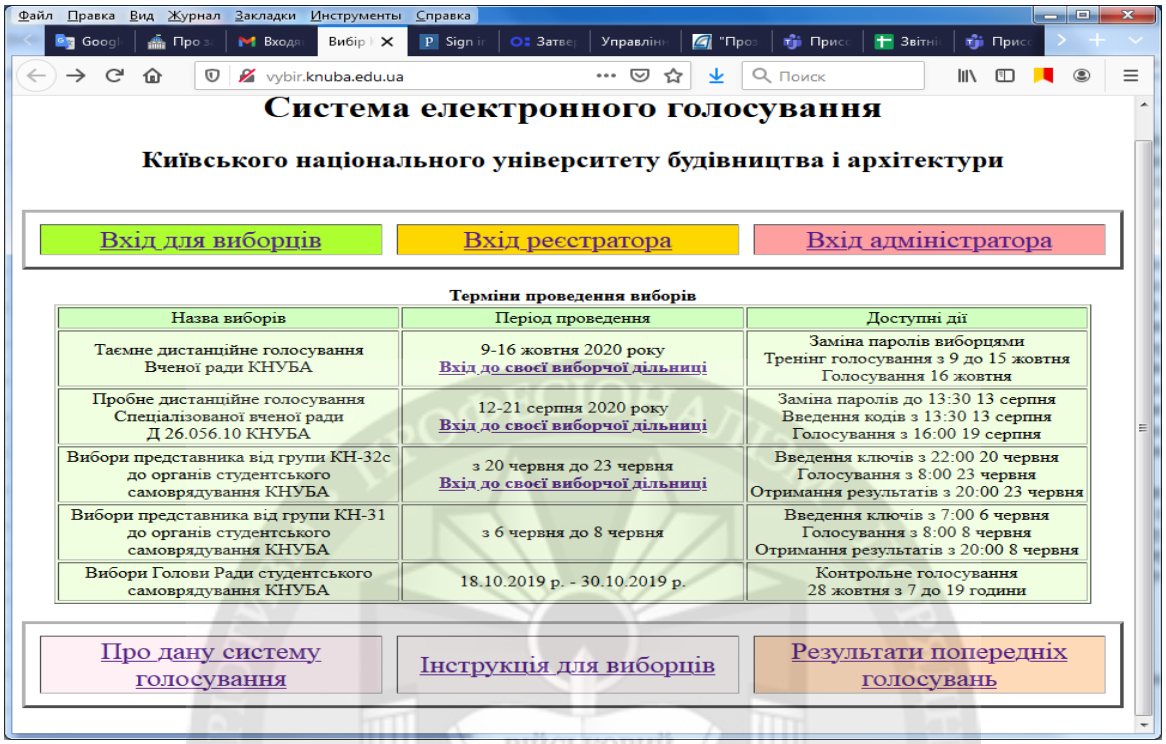

Рисунок 5 – Головна web сторінка Системи електронного голосування КНУБА

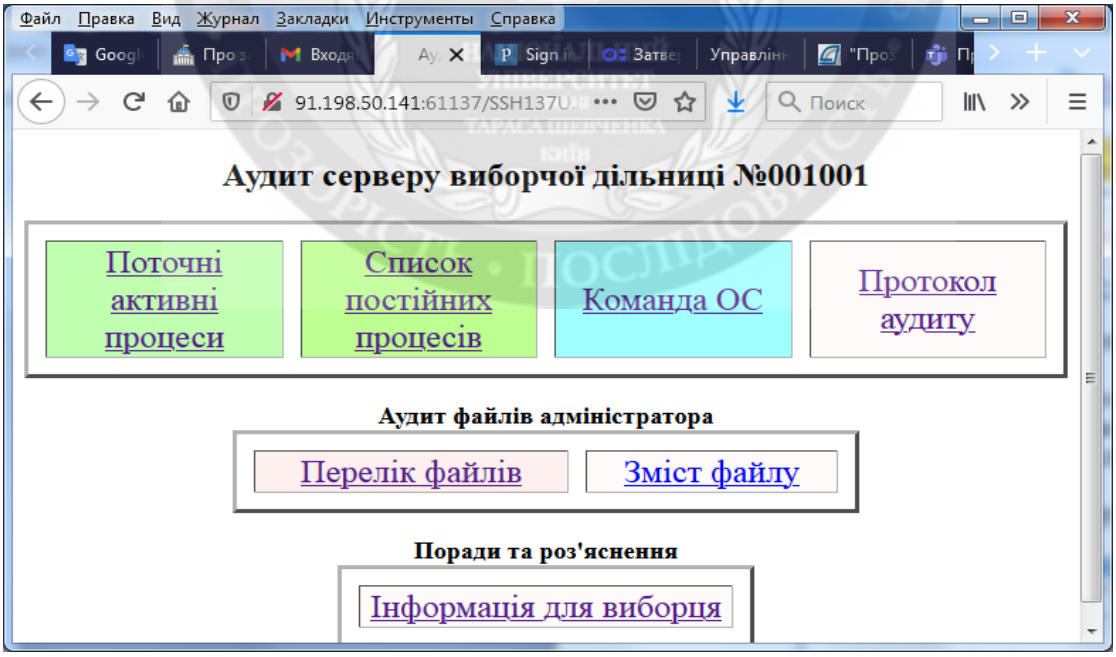

Рисунок 6 – Web сторінка для аудиту сервера Вченої Ради КНУБА

Важливою особливістю даної системи є повна відкритість і простота програмного забезпечення, яке створено з використанням лише двох широко відомих сучасних

комп’ютерних мов HTML і JavaScript. Це надає змогу її швидкого перетворення для різних застосувань, де необхідно збереження таємниці голосів і забезпечення захисту від шахрайства під час підрахунку.

Зовнішній вигляд серверного обладнання для голосування у режимі *online* представлено на рис. 7.

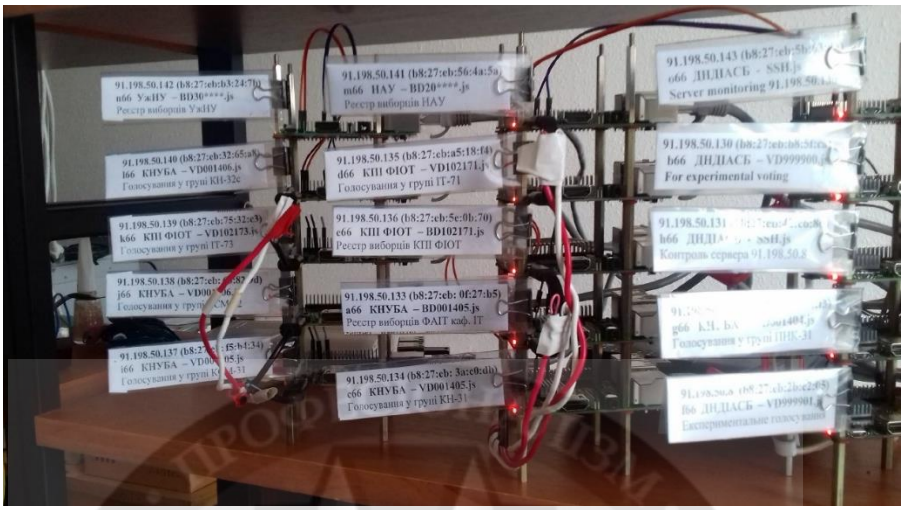

Рисунок 7 – Зовнішній вигляд серверного обладнання системи голосування

Для кожної виборчої дільниці за даною технологією *online* голосування призначається окремий сервер на міні комп’ютері типу *Raspberry Pi* 3 *B* з відкритим монтажем, що дозволяє аудиторам підключати свої контролюючі пристрої до потрібного сервера для повного контролю незалежно від інших серверів.

Також важливим практичним результатом є усунення обтяжливої процедури ручного підрахунку голосів, що у випадку засідання, яке відбулося 16 жовтня 2020 року, де кількість бюлетенів була 53, хоч з 85 членів Вченої Ради прийняли участь у голосуванні 53 (шестеро проголосували паперовими бюлетенями), полегшення було відчутним, бо в урні було на 2491 бюлетень менше. Крім того, комп’ютерний підрахунок є миттєвим і безпомилковим, а наявність автоматизованого аудиту усуває можливість для будь-яких підробок програмного забезпечення або позаштатного втручання персоналу у роботу сервера. Головна перевага звичайно та, що створюються умови для захисту від розповсюдження вірусної хвороби і не треба припиняти діяльність Вчених Рад під час карантину. З докладною інформацією щодо голосування на цьому засіданні Вченої Ради КНУБА у режимі *online* можна ознайомитись через наступне посилання http://www.knuba.edu.ua/?p=82428.

Висновки. Розглянуто принципи побудови та приклад впровадження системи таємного електронного голосування у закладі вищої освіти на засіданні Вченої Ради університету в режимі *online*.

Показано, що у цій системі забезпечено абсолютну таємницю голосів виборців за рахунок застосування досконалого методу шифрування під час пересилання даних по каналах мережі Інтернет та обробці даних у захищеній від будь-якого позаштатного втручання засобами операційної системи *OpenBSD* ділянці оперативної пам’яті сервера.

Описано можливості та методи проведення аудиту усіх програмних та апаратних засобів і процесів, які можуть викликати недовіру виборців під час проведення голосування, що дозволяє забезпечити повну довіру до даної системи за рахунок її 100% відкритості.

ЛІТЕРАТУРА:

1. Lombardi E. Electronic Vote & Democracy. May 2020. [Електронний ресурс] Режим доступу: http://www.electronic-vote.org.

2. Schneier B. What's Wrong With Electronic Voting Machines? November 2004. [Електронний ресурс] Режим доступу: https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html.

3. Electronic voting in Estonia. [Електронний ресурс] Режим доступу: https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia

4. Schneier B. Voatz Internet Voting App Is Insecure. March 15, 2020. [Електронний ресурс] Режим доступу: https://www.schneier.com/crypto-gram/archives/2020/0315.html

5. Вишняков В.М., Пригара М.П., Воронін О.В. Відкрита система таємного голосування. *Управління розвитком складних систем. Збірник наукових праць*, 2014, №20.- С. 110 – 115.

6. Первая и единственная UNIX-подобная защищённая операционная система в Украине. [Електронний ресурс] Режим доступу: https://www.atmnis.com

7. Shannon C. Communication Theory of Secrecy Systems. *Bell System Technical Journal*. 1949. 28 (4). Pp. 656-715.

8. Чуприн В.М. Генерування випадкових чисел штатними засобами хостів мережі Інтернет / В.М. Чуприн, В.М.Вишняков, М.П. Пригара // *Захист інформації*. – 2016. – Т. 18, №4. – С. 323-335.

9. Чуприн В.М., Вишняков В.М., Пригара М.П. Метод протидії незаконному впливу на виборців у системі Інтернет голосування. *Безпека інформації*. – 2017. – Том 23, №1. – С. 7–14.

10. Чуприн В.М., Вишняков В.М., Комарницький О.О., Метод протидії атакам посередника у транспарентній системі інтернет голосування, *Захист інформації, Ukrainian Information Security Research Journal*. - К.: НАУ, 2019. – Т.20. - №2. – С.172-182.

11. Чуприн В.М. Захист операційного середовища систем Інтернет голосування./ В.М. Чуприн, В.М.Вишняков, М.П. Пригара // *Захист інформації*. – 2017. – Т. 19, №1 – С. 56-66.

12. Вишняков В.М., Комарницький О.О., Жуковський А.О., Методи контролю керування системою Інтернет голосування, *Управління розвитком складних систем*. – 2019. - № 38 – С. 37-44.

13. Вышняков В.М., Комарницкий О.А. Транспарентные системы электронной демократии. Accent Graphics Communications & Publishing, Оттава, Канада. 2019. – 96 с.

14. Експериментальне голосування [Електронний ресурс] Режим доступу: http://www.asdev.com.ua/dndiasb/news/lates_news/eksperimentalne-golosuvannya.html

15. Про затвердження плану заходів щодо реалізації Концепції розвитку електронної демократії в Україні на 2019-2020 роки. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/405-2019-%D1%80/sp:max10#Text

16. Про внесення змін до Порядку присудження наукових ступенів. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/607-2020-%D0%BF#n8

17. Голубицкий С. Мутная технология. Уроки московских выборов на блокчейне. 30 сентября 2019 г [Електронний ресурс] Режим доступу: https://новаягazeta.ru/articles/2019/09/30/82175-mutnaya-tehn o logiya.

REFERENCES:

1. Lombardi, E. (2020) *Electronic Vote & Democracy*. Available at: http://www.electronic-vote.org (Accessed: 23 November 2020).

2. Schneier, B. (2004) *What's Wrong With Electronic Voting Machines?* Available at: https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html (Accessed: 23 November 2020).

3. 'Electronic voting in Estonia' *Wikipedia*. Available at https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia (Accessed: 23 November 2020).

4. Schneier, B. (2020) Voatz *Internet Voting App Is Insecure. March 15, 2020*. Available at: https://www.schneier.com/crypto-gram/archives/2020/0315.html (Accessed: 23 November 2020).

5. Vyshniakov, V.M., Prygara, M.P. and Voronin O.V. (2014)," Vidkryta systema tayemnoho holosuvannya" [The system of secret ballot is open], Upravlinnya rozvytkom skladnykh system. Zbirnyk naukovyh prac', No. 20, pp. 110 – 115.

6. *First UNIX-like operating system in Ukraine*. (2017) Available at: https://www.atmnis.com . (Accessed: 23 November 2020).

7. Shannon, C. (1949) "Communication Theory of Secrecy Systems", Bell System Technical Journal, No. 28 (4), pp. 656–715.

8. Chupryn, V.M., Vyshniakov, V.M. and Prygara, M.P. (2016) Heneruvannya vypadkovykh chysel shtatnymy zasobamy khostiv merezhi Internet [Generation of random numbers by regular means of Internet hosts], Zakhyst informatsiyi, T. 18, No. 4, pp. 323-335.

9. Chupryn, V.M., Vyshniakov, V.M. and Prygara, M.P. (2017) Metod protydiyi nezakonnomu vplyvu na vybortsiv u systemi Internet holosuvannya [Method of counteracting illegal influence on voters in the Internet voting system], Bezpeka informatsiyi, T. 23 No. 1, pp. 7–14.

10. Chupryn, V.M., Vyshniakov, V.M. and Komarnitskiy, O.O. **(2019)** Metod protydiyi atakam poserednyka u transparentniy systemi internet holosuvannya [A method of counteracting the attacks of a mediator in a transparent Internet voting system], Zakhyst informatsiyi. *Ukrainian Information Security Research Journal*, T. 20, No. 2, pp. 172-182.

11. Chupryn, V.M., Vyshniakov, V.M. and Prygara, M.P. (2017) Zakhyst operatsiynoho seredovyshcha system Internet holosuvannya [Protection of the operating environment of Internet voting systems], Zakhyst informatsiyi, T. 19, No.14, pp. 56-66.

12. Vyshniakov, V.M., Komarnitskiy, O.O. and Zhukovs′kyy A.O. (2019) Metody kontrolyu keruvannya systemoyu Internet holosuvannya [Methods of control over the management of the Internet voting system], Upravlinnya rozvytkom skladnykh system. Zbirnyk naukovyh prac', No. 38, pp. 37-44.

13. Vyshniakov, V.M. and Komarnitskiy, O.O. (2019)**,** "Transparentnyye sistemy elektronnoy demokratii" [Transparent systems of e-democracy], Accent Graphics Communications & Publishing, Ottawa, Canada, 96 p.

14. *Eksperymental'ne holosuvannya.* (2020). Available at: http://www.asdev.com.ua/dndiasb/news/lates_news/eksperimentalne-golosuvannya.html. (Accessed: 23 November 2020)

15. *Pro zatverdzhennya planu zakhodiv shchodo realizatsiyi Kontseptsiyi rozvytku elektronnoyi demokratiyi v Ukrayini na 2019-2020 roky*. (2019). Available at: https://zakon.rada.gov.ua/laws/show/405-2019-%D1%80/sp:max10#Text. (Accessed: 23 November 2020)

16. *Pro vnesennya zmin do Poryadku prysudzhennya naukovykh stupeniv*. (2020). Available at: https://zakon.rada.gov.ua/laws/show/607-2020-%D0%BF#n8. (Accessed: 23 November 2020).

17. Golubitskiy, S. (2019). *Mutnaya tekhnologiya. Uroki moskovskikh vyborov na blokcheyne*. Available at: https://новаяgazeta.ru/articles/2019/09/30/82175-mutnaya-tehn o logiya. (Accessed: 23 November 2020).

Dr. Eng. Sc. Chernyshev D.O., Dr. Eng. Sc. Khlaponin Y.I., Ph.D. Vyshniakov V.M.

EXPERIENCE OF INTRODUCTION OF ELECTRONIC VOTING IN HIGHER EDUCATION INSTITUTIONS

An important problem on the way to the development of e-democracy is to ensure citizens' confidence in electronic voting systems. Although there are many cases of implementation of such systems, in all cases, voters must take it on faith that the personnel serving the system will honestly and accurately perform the work. In other words, none of these systems provide voters with sufficient and understandable evidence that the secret of their votes cannot be revealed and the results of the vote count cannot be falsified. It is known that the systems in which citizens perform audits of all those procedures where fraudulent manifestations are possible, enjoy the indisputable trust of voters. Now such systems exist, but they do not use electronic voting. The purpose of this work is to prove and practical confirmation of the possibility of building a system of secret electronic voting on the public Internet with means available to voters for auditing all those processes that may cause distrust during voting. The principles of constructing e-voting systems are analyzed from the point of view of the possibility of ensuring the trust of citizens through complete openness for auditing selected software and hardware solutions. It was with the use of such solutions that the system was built, which was implemented at the Kiev National University of Construction and Architecture for the election of student representatives to the Student Self-Government Council. Also, this system is used to conduct secret voting at meetings of the Academic Council of the University online. An important practical result of this implementation is the elimination of cumbersome manual counting procedures. In the case of the meeting that took place on October 16, 2020, where the number of ballots was 53, although 53 out of 85 members of the Academic Council took part in the vote (six voted with paper ballots), the relief was tangible, because there were 2,491 fewer ballots in the ballot box. In addition, computerized counting is instant and error-free, and the presence of automated auditing eliminates the possibility for any software tampering or unauthorized personnel interference with the server. The main advantage, of course, is that conditions are created to protect against the spread of a viral infection and there is no need to stop the activities of the Scientific Councils during quarantine.

Keywords: e-democracy, secret e-voting on the Internet, citizens' confidence in e-voting systems, transparency of building e-voting systems, automated audit of e-voting systems.