МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Колективна монографія

Київ
Європейський університет
2023

УДК [004.056(53+55):003(26+27)]+621.643.8
А 43

Рекомендовано до друку Вченою радою ПВНЗ «Європейський університет» (протокол № 3 від 28.09.2022)

Рецензенти:
В.А. Лахно – доктор технічних наук, професор
(Національний університет біоресурсів і природокористування України)
М.Г. Медведєв – доктор технічних наук, професор
(Таврійський національний університет імені В. І. Вернадського)
О.А. Чемерис – доктор технічних наук, старший науковий співробітник
(Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України)

А 43 Актуальні питання забезпечення кібербезпеки та захисту інформації: колективна монографія / за заг. наук. ред. А.М. Давиденко, Київ: Європейський університет, 2023. – 204 с.

ISBN 978-966-301-259-9

Монографія є результатом тривалих наукових досліджень і пошуків авторів у напрямі обґрунтування сучасних концепцій, моделей, механізмів, проблем та перспектив розвитку наукових засад забезпечення кібербезпеки та захисту інформації України та світу; узагальнено та висвітлено організаційно-технологічні аспекти функціонування та захисту об'єктів критичної інфраструктури; наведено теоретичні засади та розроблено практичні рекомендації щодо безпеки комп'ютерних мереж та інтернет ресурсів в умовах сучасних впливів; проаналізовано проблеми й обґрунтовано перспективи розвитку криптографічних та стеганографічних методів захисту інформації.

До монографії увійшли матеріали доповідей учасників VIII Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», що проходила 2-5 лютого 2022 року на базі «Едельвейс» Європейського університету.

УДК [004.056(53+55)::003(26+27)]+621.643.8

ISBN 978-966-301-259-9

УДК 004.78

ДОКАЗ МОЖЛИВОСТІ ПОВНОЦІННОГО АУДИТУ СИСТЕМ ТАЄМНОГО ІНТЕРНЕТ ГОЛОСУВАННЯ

Хлапонін Ю.І.
завідуючий кафедрою кібербезпеки та комп'ютерної інженерії
Київський національний університет будівництва і архітектури
y.khlaponin@gmail.com

Вишняков В.М.
доцент кафедри кібербезпеки та комп'ютерної інженерії
Київський національний університет будівництва і архітектури
volodymyr.vyshniakov@gmail.com

Пригара М.П.
доцент кафедри технології машинобудування
ДВНЗ «Ужгородський національний університет»

Шпак О.І.
викладач кафедри програмного забезпечення систем
ДВНЗ «Ужгородський національний університет»

Анотація. Метою даного дослідження є довести можливість побудови системи таємного Інтернет голосування, в якій повноцінний аудит доступний для всіх виборців та їх довірених осіб. Під повноцінним слід розуміти такий аудит, при якому перевіряється все, що може викликати сумнів. На базі відкритого блоку серверів створено натурну модель системи для проведення експериментального голосування та розроблено детальну методику повноцінного аудиту. Експеримент може проводити будь-хто в будь-який момент за посиланням в Інтернеті. Таким чином, показано, що не лише при традиційних технологіях таємного голосування можливий повноцінний аудит, завдяки якому у виборців немає сумнівів щодо збереження таємниці свого голосування та чесності результатів. Для проведення повноцінного аудиту за описаною методикою не потрібно залучати висококваліфікованих спеціалістів, а цілком достатньо сучасної шкільної освіти, яка є обов'язковою у багатьох країнах.

1. Вступ.

Інтернет технології неухильно проникають і поглиблюються в процеси нашої діяльності. Проте на виборах представників влади, де вирішується доля багатьох громадян і цілих держав, впровадження нових технологій є

проблематичним. У країнах з розвиненою демократією, завдяки наявності аудиту, немає фальсифікацій на виборах, і вони не хочуть втрачати це досягнення при переході на нові технології. У рекомендаціях Ради ЄС щодо стандартів електронного голосування, прийнятих 14 червня 2017 року, у пункті 39 написано: «Система електронного голосування повинна підлягати аудиту. Система аудиту повинна бути відкритою та всеохоплюючою та активно повідомляти про потенційні проблеми та загрози». Якими б не були програмно-технічні засоби електронного голосування, але якщо для виборців вони являють собою «чорну скриньку», то усунути підозри у шахрайстві неможливо. Насправді, немає іншого способу забезпечити довіру виборців, як надати їм можливість провести повноцінний аудит. Під повноцінним аудитом слід розуміти такий, при якому перевіряється все, що може викликати сумніви. Мета дослідження – довести можливість побудови системи таємного Інтернет голосування, в якій повноцінний аудит доступний для всіх виборців та їх довірених осіб.

2. Постановка проблеми та задачі дослідження.

У роботі [1] висловлюється протест щодо он-лайн виборів представників влади через те, що аудит, який зазвичай проводять самі виборці, стає неможливим. Вказується, що в цьому випадку фахівці зможуть легко змінити результати голосування. У роботах з удосконалення систем Інтернет голосування можна виділити два напрями досліджень. Перший – це доробка естонської системи, яка не використовує технологію Blockchain, а другий – системи, що засновані на технології Blockchain. У роботі [2] були проаналізовані атаки на естонську систему, де було виявлено, що зловмисник може повторно голосувати за допомогою підробленого програмного забезпечення, і запропоновано більш безпечний протокол голосування. У роботі [3] для зміцнення довіри виборців пропонується проводити перевірку кіберризиків обізнаними користувачами. Однак питання аудиту апаратного та програмного забезпечення самими виборцями, для яких естонська система є «чорною скринькою», не зачіпаються. Для забезпечення довіри до систем голосування запропоновано та запатентовано використання технології Blockchain [4]. Дослідження в цьому напрямку тривають, що відображено в роботах [5–8], де вносяться пропозиції щодо покращення безпеки та анонімності виборців, а також протидії нечесності з боку кандидатів. Однак важко уявити собі широкодоступний аудит в системах за технологією Blockchain, оскільки ця технологія зрозуміла лише обмеженому колу фахівців. Таким чином, існує пробіл у дослідженнях Інтернет голосування з точки зору забезпечення широкодоступного аудиту виборцями. Зазначимо, що такий аудит є обов'язковим відповідно до пункту 39 рекомендацій Ради ЄС щодо стандартів електронного голосування [9]. Це дозволяє стверджувати, що доказ можливості побудови системи Інтернет голосування, в якій повноцінний аудит доступний

для всіх виборців, є доцільним. Для досягнення цієї мети необхідно було вирішити наступні завдання:

- визначити блоки та процедури в системі голосування, які можуть викликати недовіру виборців;
- обрати принципи побудови системи таємного Інтернет голосування, де було б передбачена можливість проведення аудиту виборцями;
– розробити методологію для повноцінного аудиту системи голосування;
– виконати натурне моделювання системи таємного Інтернет голосування з аудитом за розробленою методикою.

3. Методи та засоби дослідження.

Для вирішення поставлених завдань використано теорію комп'ютерних мереж та криптографію. Також методом дослідження було натурне моделювання систем електронного голосування за використанням інструментів аудиту. Важливу роль у порівняльній апробації різних варіантів моделей та виборі найбільш вдалих технічних рішень відіграли студенти та викладачі трьох вищих навчальних закладів Києва. Провідну роль зайняв Київський національний університет будівництва та архітектури. Активну участь у дослідженні взяли студенти та викладачі Національного авіаційного університету та Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», а також співробітники НДІ автоматизованих систем у будівництві, які надали технічне забезпечення для досліджень та доступ до Інтернету.

4. Результати дослідження.

4.1. Визначення блоків і процедур, які можуть викликати недовіру виборців.

Побоювання виборців щодо порушення їхніх законних прав можуть бути пов'язані лише з двома такими випадками:

- розкриття таємниці голосу;
- фальсифікація підрахунку голосів.

Передача інформації під час Інтернет голосування здійснюється через канали загального доступу, де слід не довіряти всім блокам, які беруть участь у процесі передачі. За відсутності засобів захисту каналів зв'язку зловмисники можуть як розкривати голоси, так і підробляти дані, утворюючи атаку посередника (*MITM – Man in the middle*). Може проявлятися недовіра до серверного блоку, який приймає та підраховує голоси виборців, оскільки існує загроза зловмисного втручання обслуговуючого персоналу в роботу цього блоку. Також недовіру може викликати процедура відображення результатів підрахунку голосів. Крім перерахованих об'єктів, недовіру може викликати реєстр виборців, куди можна внести зайвих людей, замість яких голосуватимуть порушники. Як зазначено в [10], це легко визначити, опублікувавши дані про кількість виборців для кожної вулиці в межах виборчої дільниці, для кожного

будинку в межах вулиці та для кожної квартири в будинку. Тоді самі виборці знайдуть зайвих мешканців у своїх квартирах, зайві квартири у своїх будинках і зайві будинки на своїх вулицях без використання технічних засобів. При відкритому оприлюдненні результатів по кожній виборчій дільниці неможливо сфальсифікувати загальні результати голосування, оскільки будь-яку неточність легко виявити. Таким чином, визначено повний перелік блоків і процедур, які можуть викликати недовіру виборців під час Інтернет голосування.

4.2. Вибір принципів побудови системи голосування з можливістю проведення аудиту самими виборцями.

Для того, щоб повноцінний аудит могли провести самі виборці, усі технічні рішення системи голосування мають бути зрозумілими. Апаратне та програмне забезпечення, яке отримує та реєструє голоси, має бути відкрите для перевірки. Необхідно надати можливість громадянам залучати до перевірок своїх довірених спеціалістів. Важлива роль для демонстрації бездоганної роботи сервера голосування належить серверу аудиту, який виявляє та документує перешкоди в роботі сервера голосування. Схема підключення засобів для повноцінного аудиту системи голосування в Інтернеті з роботи [10], наведена на рисунку 1.

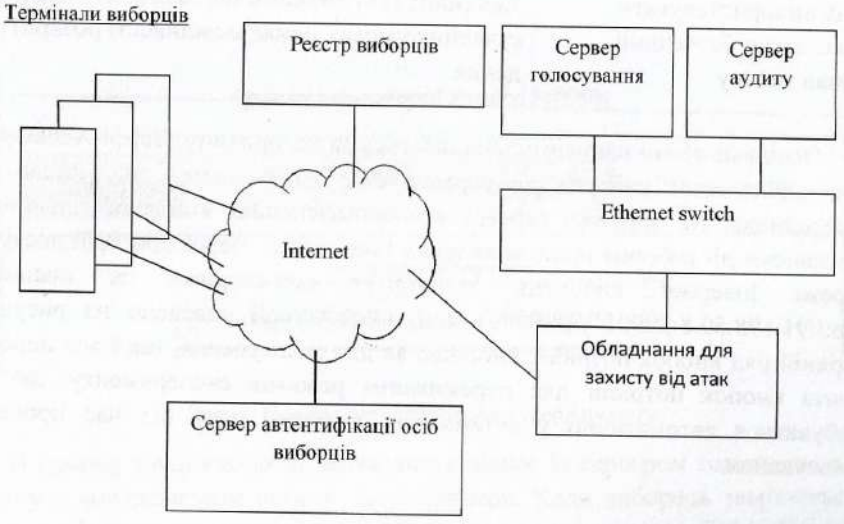

Рис. 1. Структурна схема системи Інтернет голосування.

У цій схемі сервери голосування та аудиту розміщено в одній мережі, що забезпечує надійність та швидкість проведення процедур аудиту. Виборці повинні переконатися, що їхні сеанси зв'язку з сервером голосування захищені від витоку та спотворення інформації. Для цієї мети можна використовувати технологію наскрізного шифрування, описану в [11]. Невелика кількість

інформації, яку виборець надсилає на сервер голосування (близько 60 байт), дозволяє використовувати шифр Вернама. Цей шифр надзвичайно простий для розуміння і для програмної реалізації, а його абсолютна безпечність математично доведена в роботі [12]. У таблиці 1 описані умови, які повинні бути виконані для абсолютного захисту переданих даних.

Таблиця 1.

Умови забезпечення абсолютного захисту даних під час передачі

Умова	Виконання умови
Отримання випадкових бітових послідовностей	Використовується метод отримання випадкових бітів, описаний у [13], який може бути застосовний на будь-якому комп'ютері.
Кожну випадкову послідовність можна використовувати один раз	Для кожного сеансу зв'язку їх випадкові бітові послідовності генеруються незалежно один від одного
Для передачі випадкових бітових послідовностей слід використовувати абсолютно безпечний канал зв'язку	Обмін випадковими бітовими послідовностями (ключами) відбувається за алгоритмом Діффі-Хеллмана [14] з такими параметрами, для яких у сучасних умовах немає можливості розкриття даних

Оскільки обмін ключами здійснюється за алгоритмом Діффі-Хеллмана, то при підключенні виборця до сервера слід переконатися, що немає атаки посередника. На прикладі сервера експериментальної виборчої дільниці далі розглянемо дії виборця щодо виявлення такої атаки. Через пристрій доступу до мережі Інтернет виборець завантажує веб-сторінку за посиланням http://91.198.50.8:29901/VD999901.html, вигляд якої наведено на рисунку 2. Верхній ряд кнопок потрібен виборцю як для голосування, так і для перевірки. Решта кнопок потрібні для перемикання режимів експерименту, що може відбуватися автоматично у встановлені моменти часу під час проведення голосування.

Рис. 2. Вигляд веб-сторінки виборчої дільниці.

Для проведення аудиту виборцю необхідно натиснути кнопку «Аудит сервера». При цьому веб-сторінка сервера аудиту відкриється в новому вікні, вигляд якого показано на рисунку 3.

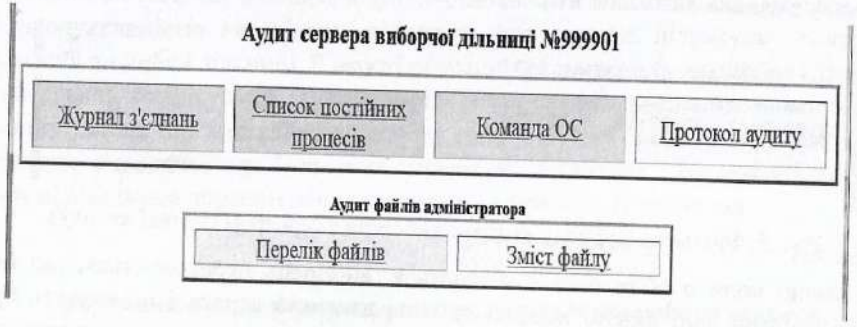

Рис. 3. Вигляд веб-сторінки сервера аудиту.

В одному вікні виборець може вести діалог із сервером голосування, а в іншому – контролювати роботу цього сервера. Коли виборець звертається до сервера, обмін кодовими словами відбувається за алгоритмом Діффі-Геллмана. Кожному такому з'єднанню присвоюється код, який є першими чотирма байтами кодового слова, надісланого виборцю сервером. Цей код (Код з'єднання) показано на рисунку 4 у діалоговому вікні виборця.

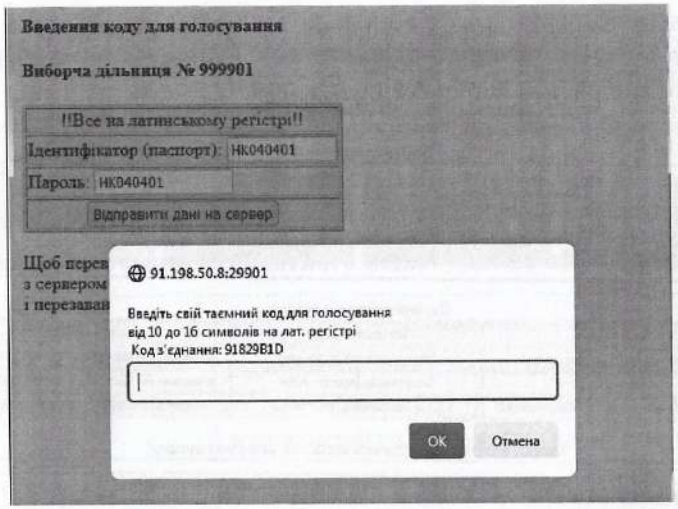

Рис. 4. Діалогове вікно з кодом з'єднання.

Для того, щоб переконатися у відсутності атаки посередника, виборцю достатньо у вікні аудиту, натиснувши клавішу «Журнал з'єднань», порівняти отриманий код (у цьому прикладі: 91829B1D) для порівняння з тим, що вказано в рядку журналу після дати та часу встановлення з'єднання з сервером. Фрагмент журналу з'єднань показано на рисунку 5.

```
cat /home/admin/CC999901.TXT

23.02.2022  22:27:19  91829B1D

a66$ exit
```

Рис. 5. Фрагмент журналу з'єднань виборців з сервером (у вікні аудиту).

Якщо коди в обох вікнах збігаються, виборець переконується, що його конфіденційні дані дійсно передаються на штатний сервер і не можуть бути дешифровані під час передачі. Оскільки задачі шифрування та підрахунку голосів не є складним, то обидва модулі програми JavaScript (клієнтський і серверний) легко перевіряються на коректність. Виборець може порівняти текст програми, що використовується, з тим, що опубліковано на сайті. Таке порівняння за допомогою стандартних інструментів займає кілька хвилин. Далі слід переконатися, що обробка даних сервером голосування не зазнала жодного позаштатного втручання. Завдяки відкритому блоку серверів, що показаний на рисунку 6, і вибору відомих апаратних і програмних засобів, такі підозри легко усуваються.

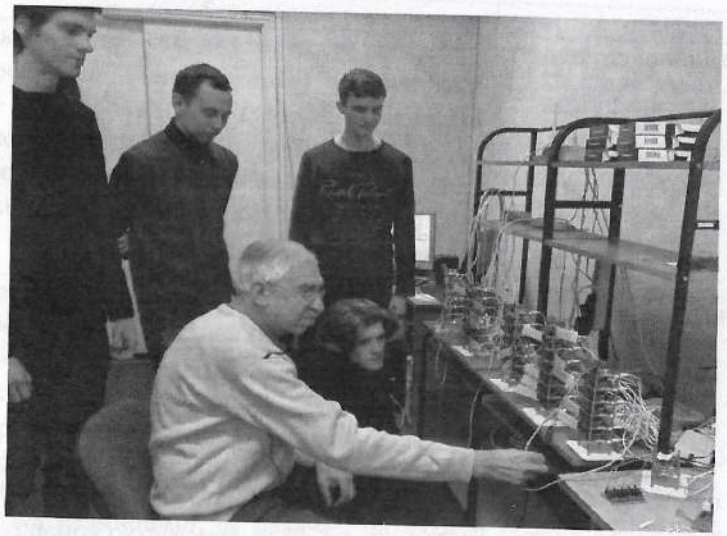

Рис. 6. Зовнішній вигляд відкритого блоку серверів.

У роботі [15] в якості апаратного забезпечення сервера голосування пропонується використовувати відомий міні-комп'ютер, наприклад Raspberry Pi 3 Model B. Цей комп'ютер має високу надійність, малу вартість, низьке енергоспоживання та підходить для відкритого монтажу. Він має характерний зовнішній вигляд, що дозволяє візуально визначити всі його складові елементи. За продуктивністю він цілком підходить для сервера підрахунку голосів у масштабі виборчої дільниці. В якості операційної системи було обрано OpenBSD мінімальної конфігурації. Такий вибір обумовлений високими вимогами до захисту даних, що покладено за основу розробки цієї системи, а також вона є повністю відкритою для будь-яких перевірок. У таблиці 2 зведені всі можливі види підозр щодо обробки даних сервером та способи їх усунення.

Таблиця 2.

Усунення підозр щодо порушення нормальної роботи сервера

Можлива підозра	Усунення підозри
1	2
Заміна сервера	Відкритість сервера для перевірки виборцями та їх довіреними особами. У разі претензій допускається заміна сумнівного сервера. Виборцям надається право підключити свою консоль до сервера для виконання команд перевірки. Після завантаження OpenBSD неможливо потайки змінити сервер.

1	2
Зміна операційної системи (ОС)	Виборцям надається право брати участь у завантаженні операційної системи за відкритою інструкцією. Після цього можна перевірити ОС через звичайний або власний сервер аудиту, ввівши команди, наприклад, sysctl, ps -aux, аж до копіювання всіх файлів ОС для перевірки.
Зміна прикладної програми	Файл прикладної програми (текст node.js) попередньо публікується на сайті виборчої системи. Адміністратор сервера розміщує копію цього файлу у своєму каталозі /home/admin/, а виборець копіює його через сервер аудиту для порівняння з опублікованим. Після запуску програми адміністратор створює звіт про свої дії за допомогою команди history > [report file name]. Виборець перевіряє звіт і порівнює час його створення з моментом запуску програми (команда ps -aux на сервері аудиту). Якщо файл з програмою був вірним до його запуску, то заміни не було.
Позаштатне втручання персоналу	Сервер аудиту реєструє появу всіх активних процесів, включаючи дії адміністратора. Після запуску програми та створення звіту ніхто не повинен заважати роботі сервера. Аудитор за допомогою клавіші «Протокол аудиту» перевіряє, чи немає записів після запуску програми, що свідчить про відсутність втручання у роботу сервера.

Зазначимо, що допуск виборців до перевірки серверного блоку та участі в установці ОС може бути дозволений у період до голосування, коли на сервері немає критичних даних. Тривалість цього періоду становить приблизно один місяць. Цього достатньо, щоб виборці переконалися, що на наявному обладнанні неможливо створити імітатор, який створював би видимість чесних виборів, а насправді допускав би фальсифікації. Не обов'язково, щоб кожен виборець перевіряв серверне обладнання, але бажано, щоб хтось із них скористався цим правом, оскільки важливо записати результат команди ps -aux, що показано на рисунку 7. Ця команда відображає стан усіх активних процесів сервера.


```
ps -aux
USER       PID %CPU %MEM   VSZ   RSS TT  STAT STARTED      TIME COMMAND
root     39820  1.8  0.4  1308  3432 ??  S     1:25PM    0:00.38 sshd: kontro
root         1  0.0  0.0   440   316 ??  S     8Jul21    9:53.69 /sbin/init
root     18788  0.0  0.1   724   832 ??  Ip    8Jul21    0:00.17 /sbin/slaacd
_slaacd  50295  0.0  0.1   724   572 ??  Ip    8Jul21    2:00.05 slaacd: engi
_slaacd  97395  0.0  0.1   728   600 ??  Ip    8Jul21    0:00.04 slaacd: fron
root     77435  0.0  0.2   812  1988 ??  IpU   8Jul21    0:00.43 syslogd: [pr
_syslogd 19541  0.0  0.1  1400  1308 ??  Sp    8Jul21   23:44.89 /usr/sbin/sy
root     88941  0.0  0.1   720   480 ??  IU    8Jul21    0:00.02 pflogd: [pri
_pflogd   1612  0.0  0.0   756   444 ??  Sp    8Jul21   23:32.26 pflogd: [run
_ntp     42631  0.0  0.3  1144  2352 ??  I<p   8Jul21    1:33.14 ntpd: ntp en
_ntp     50686  0.0  0.2  1060  2256 ??  Ip    8Jul21    0:00.46 ntpd: dns en
root     23582  0.0  0.1  1028  1328 ??  I<pU  8Jul21    0:01.13 /usr/sbin/nt
root     39763  0.0  0.1  1232  1320 ??  S     8Jul21  103:12.57 /usr/sbin/ss
root     42239  0.0  0.2  2000  1996 ??  Ip    8Jul21    0:02.26 /usr/sbin/sm
_smtpd   14805  0.0  0.4  1660  3432 ??  Ip    8Jul21    0:00.20 smtpd: klond
_smtpd   99816  0.0  0.4  1940  3736 ??  Ip    8Jul21    0:00.99 smtpd: contr
_smtpd   29763  0.0  0.4  1772  3676 ??  Ip    8Jul21    0:01.42 smtpd: looku
_smtpd   77896  0.0  0.4  2044  4128 ??  Ip    8Jul21    0:02.51 smtpd: pony
_smtpq   40229  0.0  0.4  1952  3728 ??  Ip    8Jul21    0:02.90 smtpd: queue
_smtpd   21890  0.0  0.4  1672  3532 ??  Ip    8Jul21    0:00.48 smtpd: sched
_sndiop  87793  0.0  0.1   560   764 ??  IpU   8Jul21    0:00.00 sndiod: help
_sndio   40541  0.0  0.1   588   684 ??  I<p   8Jul21    0:00.01 /usr/bin/snd
root     93843  0.0  0.1   736  1140 ??  Ip    8Jul21    1:50.46 /usr/sbin/cr
kontrol   9930  0.1  0.3  1232  2636 ??  S     1:25PM    0:00.03 sshd: kontro
admin    62604  0.0  5.6 220220 52632 p0- S     14Jul21  44:38.57 node --exper
kontrol  55491  0.0  0.1   500   660 p0  Sp    1:25PM    0:00.00 -ksh (ksh)
kontrol   1955  0.0  0.0   472   344 p0  R+pU/2 1:25PM    0:00.00 ps -aux
root     65197  0.0  0.2   464  1080 00  I+pU  8Jul21    0:00.04 /usr/libexec
b666 exit
```

Рис. 7. Результат виконання команди ps -aux у вікні сервера аудиту.

Якщо значення PID (рисунок 7) для процесів операційної системи залишаються незмінними, це означає, що сервер працює безперервно з часу, зазначеного в стовпці STARTED. У цьому випадку з 8 липня 2021 року. Оскільки кожен раз, коли запускають OpenBSD, для усіх, крім першого, процесів генеруються випадкові PID. Неможливо перезапустити сервер з тими самими PID. Сервер аудиту безперервно відстежує активні процеси за допомогою команди ps -aux кожні кілька секунд і викликає тривогу, якщо з'являється новий невідомий процес.

Таким чином, в описаній системі голосування виборці можуть провести повноцінний аудит і переконатися, що їхній голос не може бути розкритий зловмисником при передачі по каналах зв'язку та не було стороннього втручання в роботу сервера голосування.

4.3. Методика проведення повноцінного аудиту системи Інтернет голосування.

Відповідно до цієї методики аудит представлено у вигляді двох етапів: підготовчого та дистанційного. Передбачається, що серед виборців є ті, хто самостійно або із залученням довірених осіб візьмуть участь у підготовчому етапі аудиту на території провайдера Інтернету. Кількість таких виборців не обов'язково обмежувати. Завданням підготовчого етапу є перевірка обладнання сервера голосування з операційною системою на відповідність номенклатурі, а також перевірка працездатності дистанційного аудиту. Перш за все треба переконатись, що сервер дійсно працює на міні-комп'ютері Raspberry Pi 3 Model B. Це можна перевірити за зовнішнім виглядом, а також за допомогою команди sysctl hw, результат якої показаний на рисунку 8, де тип комп'ютера вказано як hw.product.

```
91.198.50.131:601
Авиабилеты  Яндекс  Начальная страница  Авн

 sysctl hw

hw.machine=arm64
hw.model=ARM Cortex-A53 r0p4
hw.ncpu=4
hw.byteorder=1234
hw.pagesize=4096
hw.disknames=sd0:89481f1157690de7
hw.diskcount=1
hw.sensors.bcmtemp0.temp0=32.71 degC
hw.product=Raspberry Pi 3 Model B Rev 1.2
hw.physmem=959225856
hw.usermem=959213568
hw.ncpufound=4
hw.allowpowerdown=1
hw.ncpuonline=4
b66$ exit
```

Рис. 8. Результат виконання команди sysctl hw.

Версію операційної системи можна визначити за допомогою команди uname -a. Для виконання команд необхідно підключити консоль, якою може бути будь-який комп'ютер з USB-портом. На рисунку 9 показано підключення консолі до Raspberry Pi 3 Model B.

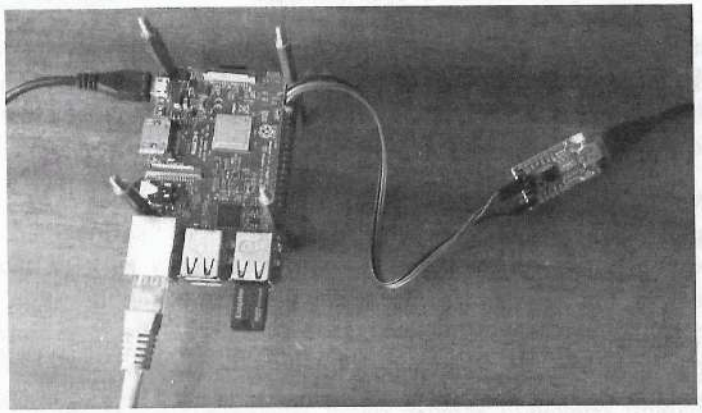

Рис. 9. Підключення консолі до міні-комп'ютера Raspberry Pi 3.

Кабель живлення показаний ліворуч, а кабель до комутатора Ethernet – нижче. Ці і тільки ці два шнури повинні бути завжди підключені. Праворуч показаний кабель для підключення консолі через адаптер типу UART-USB. Перевірка підключення до Інтернету здійснюється командою ifconfig, результат якої наведено на рисунку 10.


```
 ifconfig

lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 32768
        index 2 priority 0 llprio 3
        groups: lo
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
        inet 127.0.0.1 netmask 0xff000000
enc0: flags=0<>
        index 1 priority 0 llprio 3
        groups: enc
        status: active
smsc0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        lladdr b8:27:eb:b8:5f:ca
        index 3 priority 0 llprio 3
        groups: egress
        media: Ethernet autoselect (100baseTX full-duplex)
        status: active
        inet 91.198.50.130 netmask 0xffffff00 broadcast 91.198.50.255
pflog0: flags=141<UP,RUNNING,PROMISC> mtu 33136
        index 4 priority 0 llprio 3
        groups: pflog
```

Рис. 10. Результат виконання команди ifconfig.

Ця команда показує статус використовуваних інтерфейсів, три з яких є сервісними (lo0, enc0, pflog0) і один (smsc0) для підключення до Інтернету. Ніякі інші інтерфейси з активним статусом не повинні бути виявлені. Якщо є сумніви в цілісності операційної системи, то потрібно скопіювати всі її файли для додаткової перевірки, яка детально описана в [15]. Ця перевірка полягає в завантаженні точно такої ж ОС за допомогою точно такого ж методу на іншому комп'ютері, а потім слід порівняти файли. Якщо результат порівняння позитивний, то в цілісності системи немає жодних сумнівів, оскільки змінити систему, залишивши всі її виконувані файли без змін, неможливо. Переконавшись, що ОС правильна, слід ввести через консоль команду ps -aux, результат якої було показано вище (рисунок 7). Усі результати виконання команд повинно зберігати для подальшого порівняння. Далі слід перевірити працездатність дистанційного аудиту. Для цього за допомогою будь-якого пристрою доступу до Інтернету за посиланням, опублікованим провайдером, необхідно відкрити веб-сторінку виборця. Потім, натиснувши клавішу аудиту, відкрити сторінку сервера аудиту, вигляд якої було показано вище (рисунок 3). Натиснувши клавішу введення команди ОС, слід ввести ті самі команди, які були введені через консоль, і перевірити результати. Для команди ifconfig результати повинні повністю збігатися, для команди sysctl hw може відрізнятися лише значення температури процесора, а для команди ps -aux значення PID всіх активних процесів ОС повинні збігатися. Ці результати мають бути опубліковані на сайті виборців. У разі недовіри до штатного сервера аудиту провайдер повинен допомогти виборцям встановити додатковий сервер аудиту. Принцип роботи сервера аудиту детально описано в [10]. Для доступу виборців до сервера аудиту рекомендовано використовувати протокол https, щоб нейтралізувати

атаку посередника. Наприкінці підготовчого етапу аудиту слід перевірити надходження запитів від виборців на сервер голосування за записами у файлі /home/admin/nohup.out. Для цього після запиту виборця на сервер голосування слід ввести через консоль команду cat /home/admin/nohup.out і перевірити адресу, яка буде відображатися в кінці файлу у вигляді: ADDR=217.66.97.56:63173. Ця адреса має відповідати реальній IP-адресі запиту виборця. Подальший аудит можна провести дистанційно. Для цього на веб-сторінці виборця слід натиснути клавішу аудиту, що відкриває голову веб-сторінку сервера аудиту. Далі, натиснувши клавішу «Команда ОС», слід виконати команди для порівняння, результати яких публікуються на сайті виборців. Крім того, виборці можуть перевірити вміст усіх файлів прикладного програмного забезпечення, що дає змогу порівняти тексти виконаних програм з опублікованими, а також звірити введені адміністратором команди у файлах звітів. Хоча ці перевірки дають змогу переконатися у відсутності маніпуляцій з апаратним та програмним забезпеченням сервера для голосування, їх недостатньо для повної переконливості у відсутності фальсифікацій. Найважливіші дві перевірки, які необхідно виконати в потрібний час, стосуються виявлення атаки посередника та маніпуляцій із сервером голосування. Першу з цих перевірок виборець має виконати під час діалогу з сервером голосування, оскільки атака посередника може бути здійснена в будь-який момент. Детальний опис цієї перевірки наведено вище (рисунки 4, 5). Другу з цих перевірок необхідно провести після отримання результатів голосування. Вона полягає у перегляді протоколу аудиту за допомогою клавіші «Протокол аудиту» (рисунок 3). Результати натискання цієї клавіші показані на рисунках 11, 12.

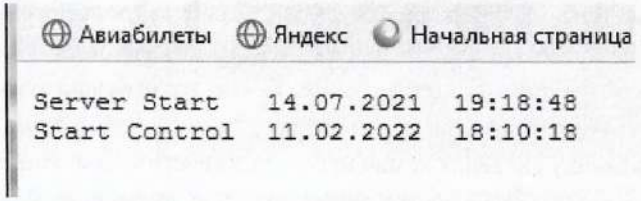

Рис. 11. Протокол аудиту, коли не було втручання у роботі сервера.

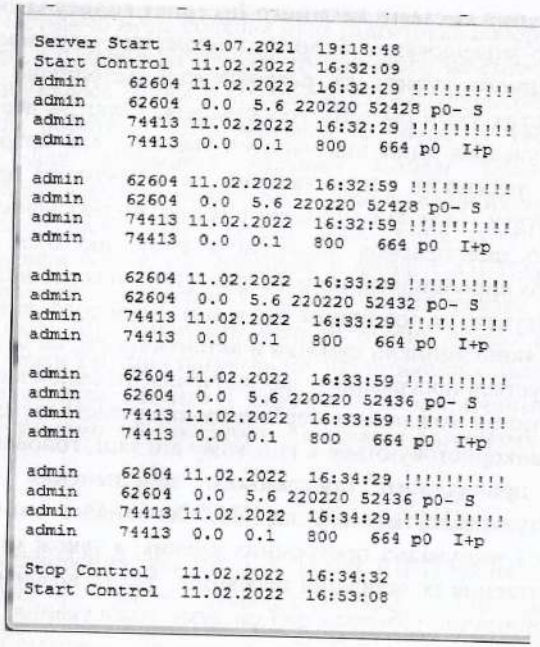

Рис. 12. Вигляд протоколу аудиту у разі втручання в роботу сервера на підготовчому етапі аудиту.

Під час перевірки протоколу аудиту важливо звернути увагу на момент початку останнього контролю, після якого записів бути не повинно. Якщо увімкнути контроль на підготовчому етапі аудиту, то непотрібні записи потраплять у протокол (рисунок 12). Це може бути корисно для перевірки працездатності системи автоматичного аудиту.

Таким чином, шляхом проведення аудиту за представленою методикою можна виявити всі загрози, які викликають занепокоєння з боку виборців. Під час підготовчого етапу аудиту було підтверджено, що сервер голосування фактично реалізований на міні-комп'ютері Raspberry Pi 3 Model B під управлінням OpenBSD. Приховано замінити ці засоби неможливо, оскільки будь-яка спроба входу на сервер з правами адміністратора відразу реєструється сервером аудиту. Завдяки підготовчому етапу аудиту в умовах відкритого серверного блоку виборці можуть продовжити повноцінний аудит дистанційно до повного завершення роботи сервера для голосування. Завдяки етапу дистанційно аудиту виборці можуть переконатись, що програмне забезпечення не було підроблено і що не було стороннього втручання в роботу сервера. Це свідчить про те, що результати підрахунку голосів, опубліковані на сервері, не можуть бути сфальсифікованими.

4.4. Моделювання системи таємного Інтернет голосування.

Метою даного моделювання було підтвердження можливості практичної реалізації повноцінного аудиту за розробленою методикою та визначення якісних характеристик такої системи голосування. Перш за все зазначимо, що моделювання стосувалося лише тієї частини системи, яка потребувала аудиту для забезпечення таємності волевиявлення та відсутності шахрайства при визначенні результату. Основні принципи цього моделювання з точки зору вибору апаратного забезпечення полягали в тому, що було обрано засоби виключно масового виробництва, широко доступні, високої надійності та такі, що легко ідентифікувати за зовнішнім виглядом. Крім того, вони повинні бути недорогими, щоб, якщо виникли сумніви в автентичності, не було проблем із їх заміною. Що стосується програмного забезпечення, то основною вимогою була його повна відкритість і можливість перевірити відсутність шкідливих закладок. Для програм, які використовуються в готовому вигляді, головне – їх безпека, а для створеного прикладного програмного забезпечення – максимальна доступність і популярність мовних засобів. Особливою вимогою був вибір найбільш простих і зрозумілих програмних рішень, а також мінімізація обсягу програм для полегшення їх детальної перевірки. Усі ці вимоги були враховані під час вибору принципів побудови цієї системи голосування, про яку йдеться вище (п. 4.2). У моделі відкритого блоку серверів, показаній на рисунку 13, передбачено підключення консолі до кожного з серверів для контролю аудиторами.

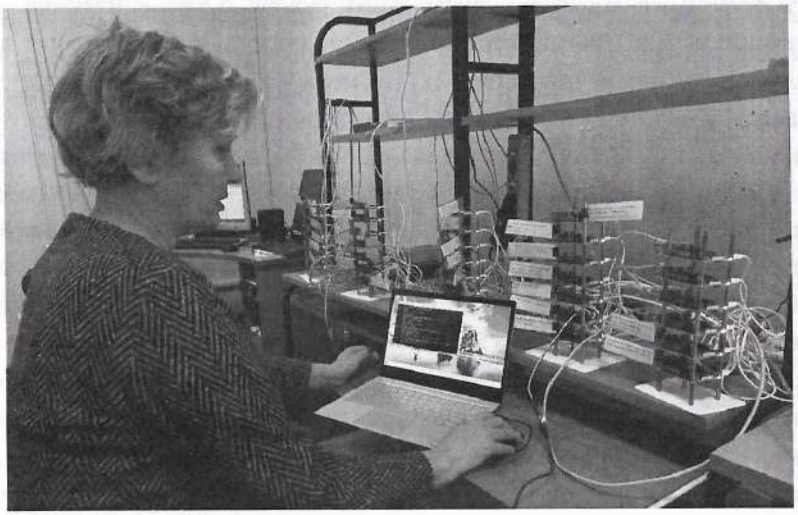

Рис. 13. Робота аудитора через консоль з відкритим блоком серверів.

Важливою частиною моделювання була підготовка виборців, які могли б не тільки голосувати, а й проводити аудит програмного забезпечення. Оскільки це моделювання відбувалось за участі студентів, які вже оволоділи комп'ютерними мовами в школі, робота з цією моделлю сприяла їх творчому розвитку. Найскладнішою для розуміння частини моделі були криптографічні перетворення, які засновані на обчисленні ступеню великих чисел за правилами операцій над полем Галуа $GF(2^{503})$. Для спрощення аудиту цей розрахунок реалізовано у вигляді блоку, розміщеного у файлі CRIPTO.js, що містить не більше 100 операторів JavaScript. Цей блок неодноразово перевірявся і не потребує перевірки. Дії, запрограмовані в цьому блоці, виконуються над символьними рядками з нулів і одиниць по 503 символи кожен. Криптографічні перетворення на стороні клієнта і сервера є симетричними і виконуються ідентичними програмами на JavaScript. Реалізація алгоритму Діффі-Хеллмана виглядає так:

$$C_C(C_S(q, X), Y) = C_S(C_C(q, Y), X), \qquad (1)$$

де C_C та C_S – перетворення, які виконує блок CRIPTO.js на стороні клієнта та сервера відповідно; q – рядок символів 010000... , що представляє собою примітивний елемент поля Галуа; X і Y – рядки випадкових символів (0, 1), які генеруються на стороні сервера та клієнта відповідно.

Оскільки перетворення C_C та C_S однакові, і вираз (1) в арифметичному еквіваленті має вигляд:

$$(q^X)^Y = (q^Y)^X, \qquad (2)$$

то справедливість рівності (1) не викликає сумніву. Це означає, що на стороні сервера і клієнта утворюються однакові послідовності з 503 випадкових символів 0 і 1. Дані для шифрування перетворюються в рядки символів 0 і 1, а потім до кожного символу за модулем 2 додається поточний символ із випадкової послідовності. Для розшифрування на стороні одержувача виконується точно таке ж перетворення, оскільки шифр Вернама симетричний.

Таким чином, моделювання показало, що аудит системи, включаючи найскладнішу для розуміння частину програмного забезпечення, доступний для осіб лише зі шкільною освітою. Саме для цього покоління створюються нові системи голосування, в яких завдяки широко доступному повноцінному аудиту, усуваються необґрунтовані підозри щодо можливого шахрайства.

5. Обговорення результатів створення відкритого блоку серверів.

При традиційній технології голосування, як зазначено в [1], завдяки повноцінному аудиту у виборців не виникає підозр у шахрайстві. Однак при таких же технологічних можливостях в інших країнах вибори можуть закінчитися скандалами. Це свідчить про те, що якщо в суспільстві не визріла потреба в чесному голосуванні, то умови для повноцінного аудиту не будуть створені або його результати будуть проігноровані. У цій роботі показано, що у

разі Інтернет голосування, завдяки відкритому блоку серверів, стає можливим проведення повноцінного аудиту. Для цього достатньо, щоб виборці дотримувалися методики, що представлена в цій роботі, але це не означає, що результати перевірки не можна буде ігнорувати. Іншими словами, ці дослідження доводять, що запровадження Інтернет голосування можна здійснити, не втрачаючи можливості в повноцінному аудиті, у чому до проведення цих досліджень могли виникнути сумніви.

6. Висновки.

1. Виходячи з того, що побоювання виборців пов'язані лише з розкриттям таємниці їх голосів та можливою фальсифікацією підрахунку, визначено блоки та процедури в системі Інтернет голосування, які можуть викликати недовіру виборців.

2. Вибрано принципи побудови системи таємного голосування в Інтернеті на основі використання відкритого серверного блоку, що забезпечує можливість проведення повноцінного аудиту не лише самими виборцями, а й будь-якими їх довіреними особами.

3. Розроблено методику проведення повноцінного аудиту системи Інтернет голосування. Завдяки цій методиці такий аудит не вимагає залучення фахівців високого рівня, а для цього цілком достатньо сучасної шкільної освіти.

4. Створено модель системи таємного Інтернет голосування, що включає засоби проведення аудиту за розробленою методикою. Завдяки цій моделі показано, що немає проблем з вибором апаратного та програмного забезпечення для здійснення повноцінного аудиту в системах таємного Інтернет голосування. Для експериментального голосування модель доступна в Інтернеті за адресою http://91.198.50.8:29901/VD999901.html.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lombardi, E. (2022) Electronic Vote & Democracy. Retrieved from http://www.electronic-vote.org.

2. Ajish, S., Anil Kumar, K. S. (2020) Secure I-Voting System with Modified Voting and Verification Protocol. Advances in Electrical and Computer Technologies. https://www.springerprofessional.de/en/secure-i-voting-system-with-modified-voting-and-verification-pro/18356152?searchResult=7.Ajish&searchBackButton=true.

3. Solvak, M. (2020) Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, October 6–9, 2020, pp 213-228. https://link.springer.com/chapter/10.1007/978-3-030-60347-2_14.

4. Patent US 2017/0109955 A1 Blockchain Electronic Voting System And Method Apr. 20, 2017.

5. Ibrahim, M., Ravindran, K., Lee, H., Farooqui, O., Mahmoud, Q.H. (2021) An Electronic Voting System using Blockchain and Fingerprint Authentication. 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C). https://www.computer.org/csdl/proceedings-article/icsa-c/2021/391000a123/1tuzQj20SwE.

6. Alvi, S.T., Uddin, M.N., Islam, L., Ahamed, S. (2020) From Conventional Voting to Blockchain Voting: Categorization of Different Voting Mechanisms. 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020 vol. 1, pp. 1-6. https://www.computer.org/csdl/proceedings-article/sti/2020/09350399/1rgGtTphP3i.

7. Fernandes, A., Garg, K., Agrawal, A., Bhatia, A. (2021) Decentralized Online Voting using Blockchain and Secret Contracts. International Conference on Information Networking (ICOIN), 2021, vol. 1, pp. 582-587. https://www.computer.org/csdl/proceedings-article/icoin/2021/09333966/1qTrSPKAJ7W.

8. Schneier, B. (2020) Voatz Internet Voting App Is Insecure. March 15. Retrieved from https://www.schneier.com/crypto-gram/archives/2020/0315.html.

9. Recommendation CM/Rec(2017) of the Committee of Ministers to member States on standards for e-voting.
https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f

10. Khlaponin, Y., Vyshniakov, V., Ternavska, V., Selyukov, O., Komarnytsyi, O. (2021) Development of audit and data protection principles in electronic voting systems. Eastern-European Journal of Enterprise Technologies, 2021, № 4/2 (112). 47–57. http://journals.uran.ua/eejet/article/view/238259/237901 DOI: 10.15587/1729-4061.2021.238259.

11. Вишняков, В.М., Пригара, М.П., Воронін О.В. (2014) Відкрита система таємного голосування, Управління розвитком складних систем, 2014, №20, С. 110 – 115. http://urss.knuba.edu.ua/files/zbirnyk-20/22.pdf.

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

13. Chupryn, V., Vyshniakov, V., Prygara, M. (2016) Generation of random numbers by regular means of Internet hosts. Ukrainian Information Security Research Journal V. 18, №4. – 323-335.

14. Diffie, W., Hellman, M.E. (1976) New Direction in Cryptography. *IEEE Transactions on Information Theory.* 1976. v.IT-22, n.6. Pp. 644-654.

15. Вишняков, В.М., Комарницький, О.А. (2019) Транспарентні системи електронної демократії. Accent Graphics Communications & Publishing , Ottawa, Canada.