DOI: 10.6084/m9.figshare.9788438
УДК 004.771

Вишняков Володимир Михайлович
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки і комп'ютерної інженерії, *orcid.org/0000-0003-4668-712X*
Київський національний університет будівництва і архітектури, Київ
Комарницький Олег Олександрович
Головний спеціаліст департаменту інформаційно-комунікаційних технологій, *orcid.org/0000-0003-4830-919X*
Київська міська державна адміністрація, Київ
Жуковський Андрій Олександрович
Студент магістратури кафедри кібербезпеки і комп'ютерної інженерії, *orcid.org/0000-0002-9363-3469*
Київський національний університет будівництва і архітектури, Київ

МЕТОДИ КОНТРОЛЮ КЕРУВАННЯ СИСТЕМОЮ ІНТЕРНЕТ-ГОЛОСУВАННЯ

Анотація. *Дистанційне голосування через Інтернет надає суттєві переваги виборцям щодо зручності, мобільності та економії часу, але стримуючим фактором на шляху його впровадження є недовіра виборців через невпевненість у збереженні таємниці голосів та чесності підрахунку результатів волевиявлення. Зрозуміло, що персонал, який керує сервером підрахунку голосів, має найширші можливості для зловживань. Тому для підвищення рівня довіри громадян до системи дистанційного голосування є актуальною задача розроблення методів контролю, котрі б надавали беззаперечну впевненість у відсутності зловмисних або помилкових дій персоналу щодо керування системою Інтернет-голосування. Запропоновано методи, які дозволяють будь-якому користувачу мережі Інтернет контролювати дії персоналу щодо керування сервером підрахунку голосів, а також виявляти позаштатні проникнення до цього сервера під час функціонування. Завдяки впровадженню цих методів може бути доведена відсутність позаштатних дій щодо керування системою голосування, що дає змогу усунути підстави для недовіри до обслуговуючого персоналу, а також може бути виявлена та задокументована наявність порушень штатного режиму функціонування системи для подальшого детального аналізу причин та наслідків цих порушень.*

Ключові слова: дистанційне голосування через Інтернет; подолання недовіри виборців; збереження таємниці голосів; чесність підрахунку голосів; контроль керування сервером

Вступ

Дистанційне голосування через Інтернет (надалі ІГ) надає суттєві переваги виборцям щодо зручності, мобільності та економії часу, але стримуючим фактором на шляху його впровадження ІГ є недовіра виборців через невпевненість щодо збереження таємниці їх голосів та у чесності підрахунку результатів волевиявлення [1; 2]. Відомо, що для подолання недовіри необхідні переконливі методи контролю усіх тих процесів, які викликають сумніви. Ще на 52-й сесії Європейської комісії за демократію через право у жовтні 2002 року щодо систем електронного голосування було прийнято норму про забезпечення транспарентності в тому розумінні, що потрібно передбачати можливість перевірки нормального функціонування систем [3]. Замість терміну «транспарентність» часто вживають такі синоніми, як «відкритість» або «прозорість». Збільшення транспарентності відбувається також і у системах голосування з паперовими бюлетенями. Замість непрозорих скриньок з'явились прозорі урни та підвищено можливості контролю за дотриманням прийнятих міжнародних норм. В Росії було впроваджено відео спостереження на 46 тис. об'єктах виборчих комісій, що дозволяло будь-кому в режимі реального часу спостерігати в мережі Інтернет за процесом голосування та підрахунком голосів [4]. У Концепції розвитку електронної демократії в Україні [5], схваленою КМ України (08.11.2017 р. за № 797-р), серед основних базових принципів вказано на «підвищення рівня довіри людини, громадянина до інструментів електронної демократії та державних інституцій». Зрозуміло, що в системах ІГ найбільші можливості для фальсифікацій має персонал, який керує сервером підрахунку голосів виборців. Тому для забезпечення транспарентності систем ІГ треба так контролювати дії персоналу щодо управління сервером, щоб не було можливості приховати ці дії від контролерів. При цьому методи контролю повинні бути зрозумілими, а засоби доступними для усіх бажаючих. Оскільки транспарентність є тією властивістю, від напряму якої залежить рівень довіри людей, то на шляху розвитку електронної демократії

є актуальною задача розроблення методів контролю, які б надавали беззаперечну впевненість у відсутності зловмисних або помилкових дій щодо керування системою ІГ.

Аналіз досліджень і постановка завдання

Безпека систем голосування потребує виконання вимог, що мають протилежний характер, а саме слід забезпечувати таємність голосів та прозорість їх підрахунку. Мотивуючи вимогою таємності, розробники перших систем ІГ нехтували прозорістю. В роботі [6] відомий фахівець у галузі криптографії Брюс Шнайер поклав край подібним мотиваціям своєю заявою про те, що не слід вірити тим, хто пропонує зберігати в таємності програми з метою забезпечення безпеки, бо в даному випадку ця таємність не має нічого спільного з безпекою. Більш того, Брюс Шнайер стверджує, що відкритість програм сприяє покращенню їх безпечності через можливість широкого обговорення з метою вдосконалення. Вперше впровадили ІГ на загальнодержавному рівні в Естонії у жовтні 2005 року [7], але лише у 2013 році були опубліковані тексти програм [8]. Майже вісім років естонські виборці мали покладатись на довіру до розробників системи ІГ. Але відкритість програмного забезпечення ще не гарантує безпечність ІГ, бо залишаються загрози модифікації або підміни програм на сервері під час експлуатації. В роботі [9], де розглянуто усі можливі загрози щодо розкриття таємниці голосів та викривлення результатів волевиявлення в системі ІГ, показано, що єдиний користувач, який після нейтралізації більшості розглянутих загроз має можливість модифікації або підміни програм, це – адміністратор сервера.

Зрозуміло, що, з метою гарантування відсутності порушень режиму функціонування системи ІГ, необхідно контролювати дії адміністратора, але у разі обмеженої кількості контролерів питання недовіри буде перекладено з адміністратора на контролерів. Дійсну довіру можна досягти у разі відсутності обмежень на кількість і особистість контролерів. У традиційних системах подібний контроль реалізують за допомогою масового спостереження у режимі реального часу через мережу відеокамер, які встановлюють в усіх тих місцях, де існує можливість зловживань. Для ІГ масовий контроль запропоновано в роботі [10] та описано в роботі [9], де представлено часову діаграму роботи сервера ІГ. Цю діаграму зображено на рис. 1, а послідовність дій адміністратора сервера під наглядом контролера показано на рис. 2.

Користувач з правами контролера, якого створює адміністратор після встановлення операційної системи, не може утворювати небезпечні ситуації для сервера виборчої дільниці (ВД), бо йому надають права доступу, які не дозволяють вносити будь-які зміни в штатну роботу сервера. При цьому користувачами-контролерами можуть стати будь-які особи без обмежень на їх кількість. Саме завдяки введенню цієї категорії користувачів система ІГ набуває прозорості, яка дає змогу впевнитись у неможливості приховувати порушення таємниці голосів та фальсифікацію їх підрахунку.

Слід зауважити, що цей контроль не потребує витрат з боку організаторів процесу голосування, бо його можуть виконувати громадські активісти та зацікавлені особи. Проведення такого контролю не залишає підстав для недовіри, бо всі елементи системи і дії персоналу, які можуть бути потенційно небезпечними, є відкритими для спостереження.

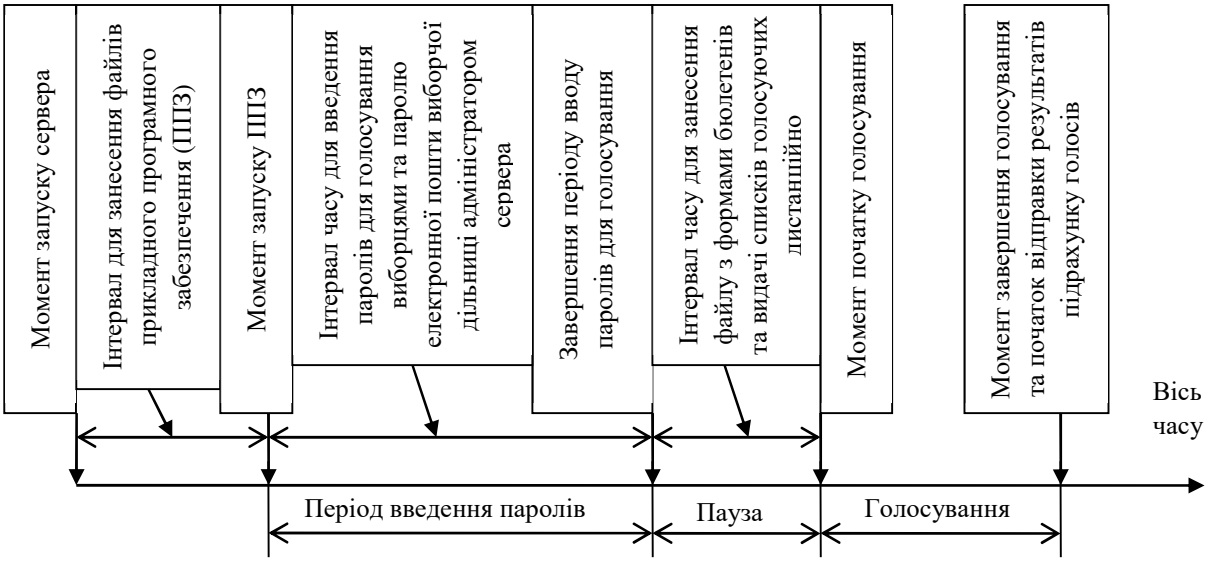

Рисунок 1 – Часова діаграма роботи сервера виборчої дільниці

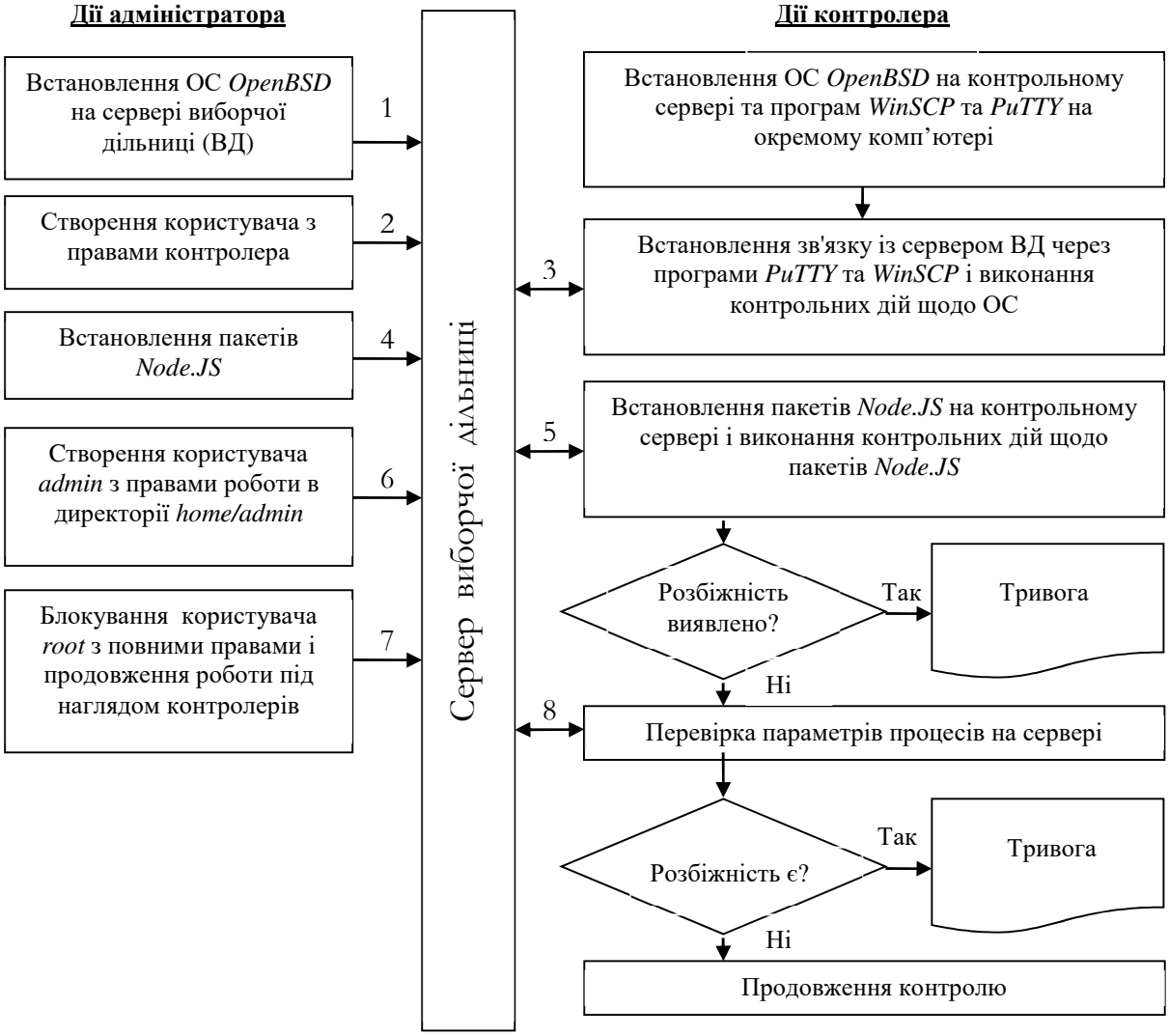

Рисунок 2 – Послідовність дій адміністратора сервера під наглядом контролера

Іншими словами, будь-яка спроба вчинення зловмисної дії у такій системі може бути виявлена та зафіксована контролюючими особами. Але для проведення такого контролю потрібні знання в галузі Інтернет-технологій і через це переважна більшість виборців не може самостійно виконувати процедури контролю, що описані в роботі [9]. Тому розроблення методів, які допомагали б контролювати дії адміністратора сервера ІГ не тільки фахівцям ІТ галузі, але й звичайним користувачам Інтернету, є актуальною, бо наявність таких методів сприяє зростанню довіри виборців до ІГ, що є позитивним фактором на шляху розвитку електронної демократії. Розроблення таких методів і є завданням цієї роботи.

Мета статті

Мета роботи полягає в підвищенні довіри виборців до системи ІГ за рахунок розроблення методів та програмних засобів, що надають можливість виборцям (особливо тим, хто не є фахівцями в галузі ІТ), власноруч контролювати дії персоналу щодо керування системою ІГ.

Виклад основного матеріалу

В роботі [9] представлено логічну модель захищеної системи дистанційного голосування , яку зображено на рис. 3, де все, що знаходиться в середині зовнішнього кола відповідає множині об'єктів сервера ІГ.

Операційна система сервера виборчої дільниці (після певних процедур налаштування) повинна дозволяти виконувати користувачам ті, і тільки ті дії, що є елементами множини Q, де Q являє собою об'єднання множин дій голосуючих виборців, адміністратора сервера та контролерів, які складають повну групу можливих дій користувачів:

$$Q = V \cup A \cup K, \qquad (1)$$

де V – множина дій голосуючих виборців; A – множина можливих (штатних і нештатних) дій адміністратора сервера; K – множина дій контролюючих осіб.

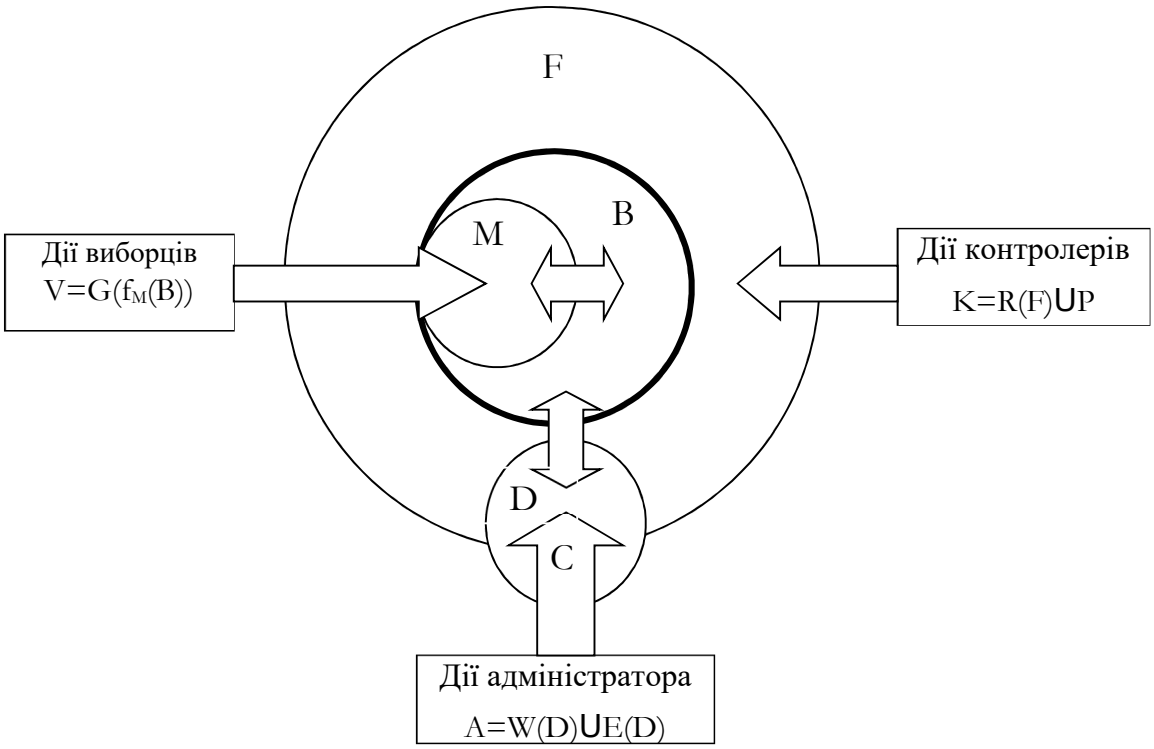

Рисунок 3 – Логічна модель захищеної системи дистанційного голосування

Слід зауважити, що таке поняття, як дії користувачів означає виключно успішно проведені транзакції щодо звернень до сервера.

Для об'єктів сервера прийнято такі позначення: F – множина всіх даних, що розміщенні у файловій системі сервера, включаючи файли з програмами готовими до виконання, а також з історією команд адміністратора; C – множина відображень команд адміністратора, причому $C \subset F$, $f : C \to A$, де f – функція відображення; D – множина файлів у тій директорії, до якої має доступ адміністратор; причому $D \subset F$; B – множина даних в оперативній пам'яті прикладної програми сервера; M – множина даних для моніторингу звернень виборців (ці дані використовує прикладна програма для авторизації голосуючих виборців), причому $M \subset B$.

Множини дій користувачів над переліченими об'єктами описують такі вирази:

$$V = \{G_1(f_M(B)), ..., G_n(f_M(B))\}, \quad (2)$$

де G_i – функція, яка відповідає і-му варіанту запиту виборця до сервера, $i = \overline{1, n}$; n – кількість варіантів запитів виборця до сервера (наприклад, голосування, отримання довідки про хід голосування тощо); f_M – функція моніторингу звернень голосуючих виборців до сервера,

$$A = W(D) \bigcup E(D), \quad (3)$$

де W – функція, яка відповідає множині дій (команд) адміністратора для приєднання файлів до множини D; E – функція, яка відповідає діям (командам) адміністратора щодо запуску на виконання файлів (програм) з множини D;

$$K = R(F) \bigcup P, \quad (4)$$

де R – функція, яка відповідає множині дій щодо доступу контролерів для ознайомлення з об'єктами множини F, причому $C \subset F$, $D \subset F$; P – множина дій контролера щодо перевірки статусу процесів на сервері та отримання інших відомостей, які можуть свідчити про порушення політики безпеки.

Як бачимо зі структури цієї системи ІГ, єдиний користувач, який має можливість виконання небезпечних дій на сервері, це – адміністратор сервера, бо будь-які дії виборців і контролерів не здатні надати їм такі права доступу, які б дозволяли утворити загрозу штатній роботі сервера. Адміністратору дозволено виконувати тільки дві дії, а саме, заносити файли в свою директорію і запускати на виконання файли з цієї директорії. При цьому будь-яка нештатна дія адміністратора може бути зафіксована контролерами, бо в нього не існує таких дій, які можна було б приховати від контролерів.

Розглянемо дії контролерів у різні періоди часу функціонування сервера та можливості отримання тих чи інших результатів контролю.

На початку функціонування сервера необхідно впевнитись у правильності встановленої операційної системи. Відомо, що ОС *OpenBSD* під назвою *BBOS* перевірена та сертифікована в Україні для систем

захисту інформації [11], а розробники цієї ОС своєю головною задачею обрали забезпечення захисту інформації. Тому правильність вибору цієї ОС не повинна викликати недовіру. Цю ОС можна вільно отримати з Інтернету або придбати на диску. Перевірка правильності ОС не є тривіальною задачею, бо для цього потрібно два комп'ютери та ще й вміння встановлювати ОС і порівнювати файли. Інтервал часу для цієї перевірки можна виділити зі значним запасом, наприклад, 3 – 4 тижні, щоб мати можливість оприлюднення та обговорення результатів на форумі контролерів, а також у разі виявлення порушень прийняти рішення щодо переустановлення ОС. Таку перевірку з позитивним результатом достатньо виконати 3 – 5 разів різними незалежними контролерами, щоб впевнитись у правильності встановленої ОС.

Після того як отримано підтвердження правильності встановленої ОС необхідно протягом усього подальшого часу функціонування системи ІГ постійно контролювати стан процесів на сервері для того, щоб уникнути таких явищ, як модифікація або підміна зловмисниками штатної ОС. Цю процедуру, а також усі наступні процедури контролю роботи системи ІГ за допомогою тих методів, які автори пропонують у цій статті, зможе виконувати будь-який користувач мережі Інтернет. Користуючись запропонованими методами, кожен бажаючий зможе впевнитись, що за весь час функціонування сервера не було змінено або модифіковано штатну ОС та інше штатне програмне забезпечення, а також усі дії персоналу щодо управління сервером системи ІГ виконувались точно за встановленим графіком.

Перший із запропонованих методів допомагає виявити відсутність позаштатних втручань в роботу сервера протягом усіх тих періодів часу, коли дії персоналу щодо керування сервером не передбачені, а також виявити моменти початку та інтервали часу виконання дій, що пов'язані з керуванням системою ІГ. Другий метод дає змогу впевнитись у тому, що дії персоналу в точності відповідали запланованим.

У першому методі використано особливість ОС *OpenBSD*, яка полягає в тому, що ідентифікатори усіх процесів (*PID*), крім першого, для якого *PID*=1, обираються випадково з ряду чисел від 2 до 32767. При цьому 20 значень перших *PID* залишаються незмінними від моменту запуску ОС до завершення функціонування сервера. Неможливо замінити чи зробити перезапуск ОС так, щоб залишити незмінними ці 20 значень *PID*. Процеси, які пов'язані з роботою контролерів і не можуть бути небезпечними для роботи сервера, мають характерні ознаки, а саме: значення *kontrol* у стовпчику *USER* або значення *sshd: kontrol* у стовпчику *COMMAND*. Все це можна побачити на рис. 4, де наведено результат виконання команди *ps -aux*.

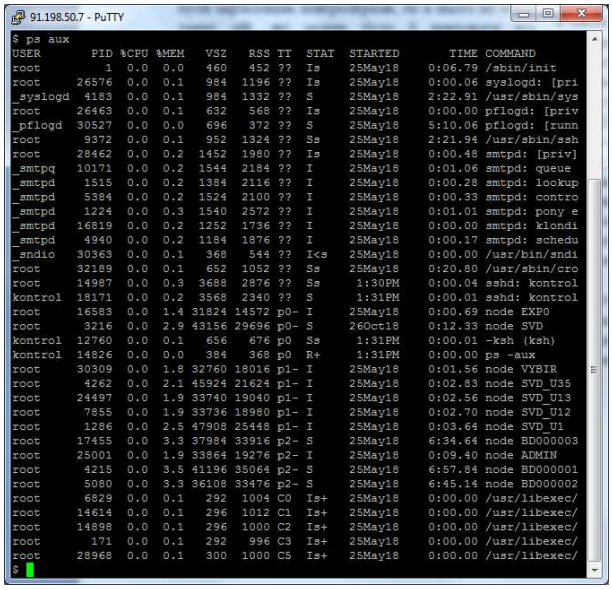

Рисунок 4 – Результат виконання команди ps –aux

Для того щоб будь-який користувач під ОС *Windows* міг реалізувати перший метод контролю створено програму з відкритим кодом на мові C#. Цю програму разом з інструкцією можна скачати тут http://www.asdev.com.ua/dndiasb/publications.html та перевірити на сервері за IP-адресою 91.198.50.7. На початку роботи програма завантажує з файлу PIDIGNOR.txt список *PID* постійно діючих в ОС процесів для ігнорування. Процеси контролерів програма ігнорує і не фіксує. У вікні програми друкуються, а також фіксуються у файлі *KRP.txt*, усі нештатні процеси та процеси адміністратора. На рис. 5 представлено вікно цієї програми.

Таку програму найзручніше встановлювати на постійно діючому сервері з можливістю управління нею через web-інтерфейс і отриманням повідомлень від неї на електронну пошту або у вигляді СМС. У разі відсутності порушень штатної роботи сервера перше, що буде зафіксовано програмою, це процес, який є початком дій адміністратора щодо занесення файлів ППЗ на сервер. Момент появи цього процесу повинен бути наперед відомим, бо він узгоджується в часі з графіком проведення виборів. Використання цієї програми, а іншими словами першого методу контролю, дає змогу впевнитись у відсутності порушень штатної роботи сервера до початку вказаних дій адміністратора. Після цього слід дочекатись завершення дій адміністратора, про що буде свідчити зникнення процесу зі значенням *admin* у стовпчику *USER*, і задіяти другий метод контролю, який допомагає перевірити точність дій адміністратора та відсутність у цих діях зловмисних намірів. Для цього можна скористатись програмою *WinSCP*, яка є у вільному доступі, і дає змогу виявити у директорії *home/admin* появу трьох файлів ППЗ. Ретельної перевірки потребує тільки файл з програмою, яка є заздалегідь відкритою у вигляді

тексту на серверній мові *JavaScript* (розширення *js*). Ця програма призначена для управління сервером в автоматичному режимі від моменту її запуску до завершення роботи системи ІГ. Найсерйознішою загрозою у нашому випадку є заміна або модифікація цієї програми. Впевнитись у тому, що підготовлено для запуску на сервері саме штатну програму, а не якусь підробку, досить просто, бо файл з програмою повинен бути розповсюдженим заздалегідь і потрібна лише елементарна перевірка на ідентичність. Задача зловмисника, який хоче сфальсифікувати результат виборів або розкрити таємницю голосів, потребує заміни штатного файлу з програмою перед її запуском на підроблений, а після запуску повернення на місце штатного файлу. Все це треба зробити так швидко, щоб контролери не встигли зафіксувати. Інших можливостей для заподіяння подібної шкоди у персонала, який керує системою ІГ, в даній операційній системі не існує. Щоб впевнитись у відсутності реалізації описаної загрози необхідно перевірити і зафіксувати в режимі реального часу такі події:

1. Початок процедури управління сервером;
2. Запуск штатної програми на виконання;
3. Завершення сеансу управління сервером;
4. Відсутність будь-яких дій, які б мали змогу спричинити загрозу протягом цього сеансу.

За допомогою першого методу контролю із точністю до встановленого значення інтервалу між запитами (на рис. 5 він дорівнює 10 секунд) можна без сумнівів забезпечити перевірку по перших трьох пунктах, але це не надає гарантій щодо виконання четвертого пункту. Для отримання таких гарантій автори пропонують, щоб адміністратор обов'язково через одну-дві хвилини після запуску програми виконував додаткову дію до завершення сеансу, а саме команду *history > history*. В результаті такої команди у файл *home/admin/history* будуть занесені усі команди, які були введені під час цього сеансу управління сервером. У разі, якщо у цьому файлі буде виявлено тільки один рядок змісту: *nohup node* <ім'я прикладної програми>, то можна після ще декількох простих перевірок впевнитись у тому, що ніяких небезпечних дій під час запуску програми не було виконано. Розглянемо докладніше послідовність перевірок під час запуску серверної програми з використанням запропонованих методів. Слід перевірити, щоб момент запуску серверної програми з точністю до хвилини збігався із запланованим, бо від цього моменту автоматично визначаються наступні інтервали часу, включаючи період голосування. Цей момент буде зафіксовано у рядку робочого вікна програми та у файлі *KRP.txt*. Цей рядок у полі *USER* буде мати значення *admin*, а у полі *COMMAND* – *node* <ім'я програми>. Процес, який супроводжує дії адміністратора, також буде мати значення *admin* у полі *USER*, а його поява на 1–5 хвилин випереджатиме момент запуску програми. Цей процес повинен зникнути за 1–2 хвилини після запуску програми. Залишається перевірити, щоб після запуску програми і виконання команди *history > history* адміністратор не виконував зловмисних дій, які були описані вище. Для цього достатньо перевірити значення *PID* для процесу серверної програми. Це значення повинно залишатись незмінним після завершення процедури управління. Далі у файлі *KRP.txt* буде фіксуватись тільки один процес виконання прикладної програми, який не повинен припинятись чи замінюватись до повного завершення циклу роботи системи ІГ. У разі позитивних результатів перевірок обома методами, які запропоновані у цій статті, можна гарантувати точність виконання персоналом усіх потрібних штатних дій та неможливість порушення таємниці голосів або викривлення результатів підрахунку, бо в обраній операційній системі не існує шляхів для непоміченого контролюючими особами заподіяння шкоди під час керування роботою системи ІГ.

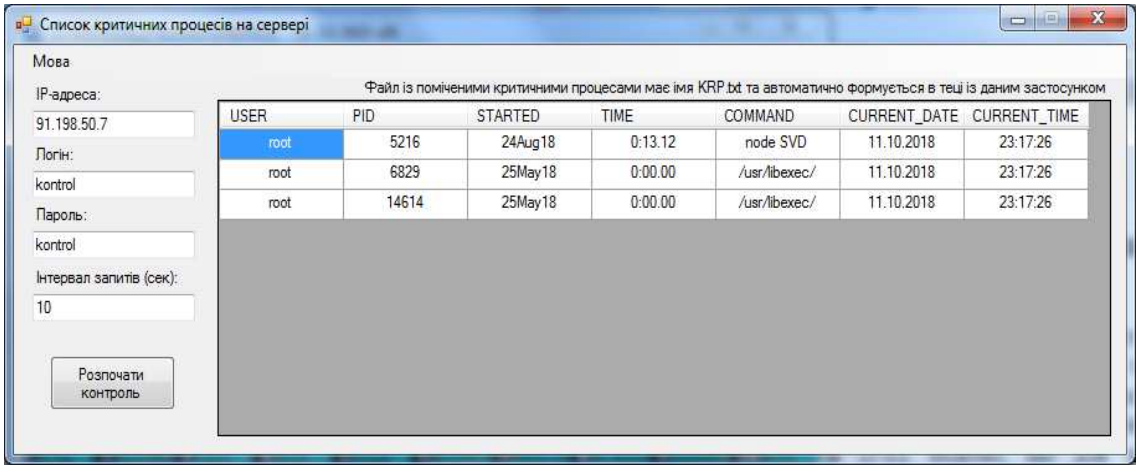

Рисунок 5 – Робоче вікно програми для контролю керування роботою системи ІГ

Висновки

Недостатня прозорість систем голосування через Інтернет є суттєвим стримуючим фактором їх впровадження, який породжує недовіру виборців через невпевненість щодо збереження таємниці голосів та/або у чесному підрахунку результатів волевиявлення.

У статті проаналізована можливість утворення загроз щодо розкриття таємниці голосів і фальсифікації результатів підрахунку з боку персоналу, який керує роботою відкритої для контролю системою таємного голосування в мережі Інтернет, та запропоновано методи, які дають змогу контролюючим особам виявити та зафіксувати дії персоналу, який керує сервером підрахунку голосів, і довести відсутність у цих діях зловмисних намірів щодо порушення штатного режиму роботи системи Інтернет-голосування.

Запропоновані у цій статті методи контролю керування системою Інтернет–голосування засновані на виконанні простих і доступних широкому колу користувачів Інтернету процедур, що надає можливість усунення підстав для недовіри з боку виборців через недостатність знань у галузі ІТ.

Список літератури

1. *Lessons from the EVOTE 2014 Internation Conferens [Electronic source] – Available at: http://e-lected.blogspot.com/search?updated-min=2014-01-01 T0 0:00:00-08:00&updated-max=2015-01-01T00:00:00-08:00& max-results=50.*
2. *Lombardi E. Electronic Vote & Democracy [Electronic source] – http://www.electronic-vote.org*
3. *Свод рекомендуемых норм при проведении выборов [Electronic source] – https://online.zakon.kz/Document/?doc_id=30926744#pos=16;-47*
4. *В ЦИК рассказали, где 18 марта можно посмотреть трансляции с участков и из ТИКов [Електронний ресурс] – https://rg.ru/2018/03/16/v-cik-rasskazali-gde-18-marta-mozhno-posmotret-transliacii-s-uchastkov-i-iz-tikov.html*
5. *Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації [Електронний ресурс] – http://zakon.rada.gov.ua/laws/show/98-2018-%D1%80/paran2#n2*
6. *Schneier B. What's Wrong With Electronic Voting Machines? https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html*
7. *Электронное голосование в Эстонии [Електронний ресурс] – http://ru.wikipedia.org/wiki/Электронное_голосование_в_Эстонии*
8. *E-hääletamise tarkvara [Electronic source] – https://github.com/vvk-ehk/evalimine*
9. *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.*
10. *Вишняков В.М., Пригара М.П., Воронін О.В. Відкрита система таємного голосування // Управління розвитком складних систем. – 2014. – Вип. 20. – С. 110 – 115.*
11. *Первая и единственная UNIX-подобная защищённая операционная система в Украине [Електронний ресурс] – https://www.atmnis.com*

Стаття надійшла до редколегії 18.03.2019

Вышняков Владимир Михайлович
Кандидат технических наук, доцент, доцент кафедры кибербезопасности и компьютерной инженерии, *orcid.org/0000-0003-4668-712X*
Киевский национальный университет строительства и архитектуры, Киев
Комарницкий Олег Александрович
Главный специалист департамента информационно-коммуникационных технологий, *orcid.org/0000-0003-4830-919X*
Киевская городская государственная администрация, Киев
Жуковский Андрей Александрович
Студент магистратуры кафедры кибербезопасности и компьютерной инженерии, *orcid.org/0000-0002-9363-3469*
Киевский национальный университет строительства и архитектуры, Киев

МЕТОДЫ КОНТРОЛЯ УПРАВЛЕНИЯ СИСТЕМОЙ ИНТЕРНЕТ–ГОЛОСОВАНИЯ

Аннотация. *Дистанционное голосование через Интернет предоставляет существенные преимущества избирателям по удобству, мобильности и экономии времени, но сдерживающим фактором на пути его внедрения является недоверие избирателей из-за неуверенности в сохранении тайны голосов и честности подсчета результатов волеизъявления. Понятно, что персонал, который управляет сервером подсчета голосов, имеет широкие возможности для злоупотреблений. Поэтому для повышения уровня доверия граждан к системе дистанционного голосования актуальным является разработка методов контроля, которые бы обеспечивали безоговорочную уверенность в отсутствии вредоносных или ошибочных действий персонала по управлению системой Интернет–голосования. В статье предложены методы, которые позволяют любому пользователю сети Интернет контролировать действия персонала по управлению сервером подсчета голосов, а также выявлять нештатные проникновения к этому серверу*

в процессе его функционирования. Благодаря внедрению этих методов может быть доказано отсутствие внештатных действий по управлению системой голосования, что позволяет устранить основания для недоверия к обслуживающему персоналу, а также могут быть обнаружены и документированы нарушения штатного режима функционирования системы для дальнейшего детального анализа причин и последствий этих нарушений.

Ключевые слова: дистанционное голосование через Интернет; преодоление недоверия избирателей; сохранение тайны голосов; честность подсчета голосов; контроль управления сервером

Vyshniakov Volodymyr
PhD in engineering, associate professor, Department of Cyber Security and Computer Engineering, *orcid.org/0000-0003-4668-712X*
Kyiv National University of Construction and Architecture, Kyiv
Komarnitskiy Oleg
Chief Specialist, Department of Information and Communication Technologies, *orcid.org/0000-0003-4830-919X*
Kyiv City State Administration, Kyiv
Zhukovskyi Andrii
Master level student at the department of cyber security and Computer Engineering of the majority, *orcid.org/0000-0002-9363-3469*
Kyiv National University of Construction and Architecture, Kyiv

METHODS OF CONTROL OF SYSTEM MANAGEMENT ON THE INTERNET VOTING

Abstract. *Remote voting via the Internet provides significant advantages for voters in terms of convenience, mobility, and time savings, but a constraint on its implementation is the distrust of voters due to uncertainty in keeping secrets and fairness in the counting of voting results. It is clear that the staff that manages the counting server has ample opportunities for abuse. Therefore, in order to increase the level of citizens' confidence in the remote voting system, the challenge is to develop control methods that would provide unconditional confidence in the absence of malicious or erroneous actions of personnel in managing the Internet voting system. This article proposes methods that allow any Internet user to control the actions of personnel managing a vote counting server, as well as to identify abnormal penetrations to this server during its operation. Thanks to the introduction of these methods, the absence of abnormal actions to manage the voting system can be proved, which allows to eliminate the grounds for distrust of the service personnel, as well as violations of the normal operation of the system can be detected and documented for further detailed analysis of the causes and consequences of these violations. The methods of control of Internet voting system offered in this article are based on the implementation of simple and accessible to the wide circle of Internet users of the procedures, which provides an opportunity to eliminate the grounds for distrust by voters due to lack of knowledge in the field of IT.*

Keywords: remote voting via the Internet; overcoming voter mistrust; keeping secrets of voices; honesty; control server management

References

1. Lessons from the EVOTE 2014 Internation Conferens [Electronic source] – Available at: http://e-lected. blogspot.com/ search?updated-min=2014-01-01 T0 0:00:00-08:00&updated-max=2015-01-01T00:00:00-08:00& max-results=50.

2. Lombardi E. Electronic Vote & Democracy [Electronic source] – http://www.electronic-vote.org

3. Code of recommended standards for elections [Electronic source] – https://online.zakon.kz/Document/?doc_id=30926744#pos=16;-47

4. The CEC was told where on March 18 you can watch broadcasts from polling stations and from TECs. [Electronic source] – https://rg.ru/2018/03/16/v-cik-rasskazali-gde-18-marta-mozhno-posmotret-transliacii-s-uchastkov-i-iz-tikov.html

5. About the conceptualization of the development of e-democracy in Ukraine and the plan of calling for real estate. [Electronic source] – http://zakon.rada.gov.ua/laws/show/98-2018-%D1%80/paran2#n2

6. Schneier B. What's Wrong With Electronic Voting Machines? https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html

7. E-voting in Estonia [Electronic source] – https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia

8. E-hääletamise tarkvara [Electronic source] – https://github.com/vvk-ehk/evalimine

9. Chuprin, V.M., Vyshniakov, V.M., Prygara, M.P. (2017). Defence of operating environment of the systems the Internet voting. Information security, 1, 56- 66.

10. Vyshniakov, V.M., Prygara, M.P., Voronin, O.V. (2014). Open secret ballot system. Management of Development of Complex Systems, 20, 110-115.

11. The first and only UNIX-like protected operating system in Ukraine [Electronic source] – https://www.atmnis.com

---

Посилання на публікацію

APA *Vyshniakov, Volodymyr, Komarnitskiy, Oleg & Zhukovskyi, Andrii. (2019). Methods of control of system management on the Internet voting. Management of Development of Complex Systems, 38, 37 – 44, dx.doi.org\10.6084/m9.figshare.9788438.*

ДСТУ *Вишняков, В. М. Методи контролю керування системою Інтернет-голосування / В.М. Вишняков, О.О. Комарницький, А.О. Жуковський // Управління розвитком складних систем. – 2019. – № 38. – С. 37 – 44, dx.doi.org\10.6084/m9.figshare.9788438.*