© Chupryn V., Vyshniakov V., Prygara M. Method of guaranteeing the security of the vote in the Internet voting system // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 1, p. 7-14.

DOI: 10.18372/2225-5036.23.11547

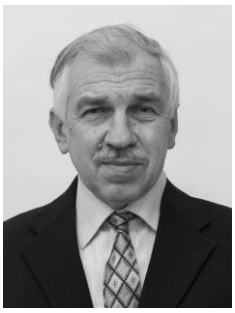
МЕТОД ПРОТИДІЇ НЕЗАКОННОМУ ВПЛИВУ НА ВИБОРЦІВ У СИСТЕМІ ІНТЕРНЕТ ГОЛОСУВАННЯ

Володимир Чуприн[1], Володимир Вишняков[1], Михайло Пригара[2]

[1]*Національний авіаційний університет, Україна*
[2]*Ужгородський національний університет, Україна*

ЧУПРИН Володимир Михайлович, к.т.н.

Рік та місце народження: 1946 рік, м. Киштим, Челябінська область, РФРСР.
Освіта: Київський інститут інженерів цивільної авіації, 1969 рік.
Посада: професор кафедри телекомунікаційних систем з 2002 року.
Наукові інтереси: захист інформації в телекомунікаційних системах.
Публікації: більше 50 наукових публікацій, серед яких монографії, підручники, навчальні посібники, наукові статті та патенти на винаходи.
E-mail: vladimir@ndiasb.kiev.ua



ВИШНЯКОВ Володимир Михайлович, к.т.н.

Рік та місце народження: 1946 рік, м. Київ, Україна.
Освіта: Київський політехнічний інститут, 1969 рік.
Посада: доцент кафедри телекомунікаційних систем з 2015 року.
Наукові інтереси: інформаційні технології, захист інформації.
Публікації: більше 70 наукових публікацій, серед яких навчальні посібники, наукові статті, авторські свідоцтва та патенти на винаходи.
E-mail: volodymyr.vyshniakov@gmail.com

ПРИГАРА Михайло Петрович

Рік та місце народження: 1987 рік, м. Мукачево, Закарпатська область, Україна.
Освіта: Київський національний університет будівництва і архітеуктури, 2010 рік.
Посада: викладач кафедри програмного забезпечення систем з 2016 року.
Наукові інтереси: інформаційні технології, захист інформації, розподілені системи.
Публікації: більше 10 наукових публікацій, серед яких наукові статті, матеріали та тези доповідей на конференціях.
E-mail: misha_prigara@ukr.net

Анотація. *Розглянуто систему Інтернет голосування з повністю відкритим для ознайомлення і випробування програмним забезпеченням, у якій для голосування можна користуватись яким завгодно пристроєм доступу до Інтернету. Це може бути комп'ютер довільного типу, планшет, смартфон або телевізор з функцією SmartTV без будь-яких додаткових програмних або апаратних засобів. Для забезпечення довіри з боку виборців надається можливість контролю за роботою системи в реальному часі для будь-якої зацікавленої особи. Під підозрою щодо можливості утворення загроз процесу голосування є всі без винятку учасники виборчого процесу, включаючи персонал, який несе відповідальність за ті чи інші функції або ділянки системи голосування. При цьому гарантується безпека голосів виборців від розкриття, а результатів підрахунку голосів – від спотворень. Для даної системи пропонується метод голосування, який забезпечує виборцям можливість вільного волевиявлення за умов наявності таких факторів незаконного впливу, як підкуп, залякування або силовий тиск. Впровадження цього методу унеможливлює отримання точної інформації про ре-*

зультати голосування кожного окремого виборця, що приводить до недоцільності впливу на виборців вказаними незаконними методами.

Ключові слова: *інтернет голосування, безпека інформації, метод голосування, нейтралізації незаконного впливу на виборців.*

Вступ

Не викликає сумніву, що голосування через Інтернет надає суттєві переваги виборцям щодо зручності, мобільності та економії часу на голосування. Кількість виборців в Естонії, які голосують з використанням Інтернету неухильно збільшується від 1,85% у 2005 році до 30,5% у 2015 році. Крім перелічених переваг, за допомогою Інтернет голосування, як показано у даній статті, є можливість протидіяти такому незаконному явищу, як підкуп або примушування виборців віддавати свій голос під тиском зловмисників, що було зафіксовано на політичних виборах в Україні. З інформацією про подібні випадки можна ознайомитись на сайті Комітету виборців України http://cvu.org.ua. Значність незаконного впливу на виборців підтверджується підписаним Президентом України 19 жовтня 2014 р. за №1703-VII спеціальним законом. У Росії загроза впливу на виборців підкупом є в переліку загроз на сайті https://www.kartanarusheniy.org. У діючій в Естонії системі Інтернет голосування [1] також передбачено засоби боротьби проти незаконного впливу на виборців, які описані на сайті http://www.uvk.ee. Все це свідчить про важливість створення методів, які б гарантували виборцям можливість вільного волевиявлення не зважаючи на незаконний вплив.

Слід зауважити, що в системах Інтернет голосування важливо забезпечити довіру виборців до самої системи, що було визначено на шостій міжнародній конференції з питань електронного голосування [2]. Існує активна протидія Інтернет голосуванню з боку осіб, які вважають, що неможливо створити електронну систему, якій можна було б довіряти на 100%, про що свідчить інформація на http://www.electronic-vote.org/INTRO/index.php.

Тому бажано, щоб система голосування була побудована таким чином, щоб у виборців не залишалось жодного сумніву щодо будь-якої можливості викривлення результатів їх волевиявлення або розкриття таємниці їх голосу. Тільки повна прозорість із можливістю проконтролювати точність дій на всіх етапах роботи системи голосування в реальному часі будь-якою зацікавленою особою здатна подолати недовіру виборців. Саме такі властивості повинна мати система Інтернет голосування, яка б заслуговувала на довіру виборців, бо наявність хоч однієї непрозорої процедури є підставою для недовіри і дискредитації системи. Це означає, що кожен елемент системи, включаючи підсистему забезпечення інформаційної безпеки, повинен відповідати вимогам прозорості з точки зору можливості контролю за його роботою. Слід зауважити, що, як підкреслено у роботі Брюса Шнайера [3], відкритість системи не є перешкодою для захисту від загроз зловмисників, а навпаки, відкриті системи мають більше шансів бути краще захищеними через можливість залучення до участі у їх перевірці і вдосконаленні необмеженої кількості фахівців. Багаторічна історія створення систем електронного голосування зі слів самих розробників, з якою можна ознайомитись на ресурсі https://www.frisc.no/wpcontent/uploads/2014/05/finse2014-kem m erer-1.pdf, свідчить про те, що на кожну чергову ідею розробників щодо захисту системи, через деякий час знаходяться зловмисники, які здатні подолати захист. Тому можна вважати актуальною задачу створення та вдосконалення методів гарантування безпеки голосів виборців та пошуку шляхів побудови систем Інтернет голосування таким чином, щоб завдяки можливості контролю з боку будь-якої зацікавленої особи за роботою системи в реальному часі, не залишалось місця для непоміченого нештатного втручання з боку будь-кого, включаючи штатний персонал.

Метод, якому присвячена дана стаття, надає можливість виборцям голосувати за власним розсудом, не зважаючи на наявність таких факторів впливу, як підкуп, залякуванням або силовий тиск. Цей метод придатний для впровадження у будь-яку систему Інтернет голосування за умов використання паролів для автентифікації виборців.

Аналіз принципів побудови безпечних систем голосування

Метою цього аналізу є виявлення та розкриття принципів побудови систем Інтернет голосування, використання яких надає можливість реалізації вимог, що в тій чи іншій мірі відповідають бажаним властивостям безпечної системи.

Безпечною будемо вважати таку систему Інтернет голосування, у якій голоси виборців досконало захищені від розкриття, а всі без винятку небезпечні дії можуть бути своєчасно виявлені завдяки безперервному контролю з боку зацікавлених осіб. Досконалим будемо називати такий захист, витрати часу на подолання якого перевищують межі реальності. Зауважимо, що, як доведено в роботі [4], абсолютний захист від розкриття забезпечує алгоритм Вернама, але для реалізації цього алгоритму у чистому вигляді необхідно мати додатковий абсолютно захищений канал для обміну ключовою інформацією. Всі інші відомі нам алгоритми не гарантують абсолютного захисту, але можливо підібрати до них такі параметри, щоб час на розкриття інформації в сучасних умовах обчислювався сотнями, або навіть мільярдами років. Такий захист будемо називати досконалим, хоч він в практичному розумінні може не поступатись абсолютному.

Досконало захищене ядро безпеки на сервері може бути створено на рівні операційної системи. Наприклад, обираючи серверну операційну систему *OpenBSD*, яка зарекомендувала себе досконало захищеною, отримуємо для кожної діючої програми окрему, захищену від дії всіх інших програм, ділянку пам'яті, що і буде являти собою потрібне ядро безпеки. Головне, щоб у обраній операційній системі не

існувало можливості для доступу до ділянки оперативної пам'яті діючої програми з боку будь-якої іншої програми.

Для досконалого захисту сервера від шкідливого впливу дій зловмисників достатньо обмежити доступ для всіх користувачів, крім адміністратора, таким чином, щоб не існувало можливості заподіяти шкоду. Дії адміністратора можна обмежити на рівні прав доступу і забезпечити над ними повноцінний контроль, як запропоновано в роботі [5]. Ті дії адміністратора, які потребують права повного доступу, виконуються на етапі підготовки сервера до встановлення і запуску прикладного програмного забезпечення (ПЗ). Після виконання підготовчих дій, які включають створення користувачів з правами контролерів, потреби управління сервером з правами повного доступу немає, тому можна заблокувати користувача з правами повного доступу, що сприятиме захисту від несанкціонованого доступу (НСД) з боку будь-кого, включаючи і самого адміністратора. Надалі сервер може працювати в автоматичному режимі під управлінням прикладної програми до моменту фізичного відключення. Таким чином, будь-які спроби зловмисників на отримання НСД протягом усього циклу роботи сервера приречені на неуспіх через відсутність можливості отримання повного доступу. При цьому, усі зацікавлені особи, кількість яких необмежена, можуть, отримавши права контролера, передивлятись усі файли на сервері, але не можуть нічого змінювати або доповнювати. Контролери можуть виконувати команди, які дозволяють впевнитись у тому, що сервер працює в штатному режимі і на ньому відсутні будь-які доробки або зміни ПЗ. Кожен може інсталювати на своєму комп'ютері таке ж ПЗ, що й на сервері, і шляхом порівняння файлів між сервером і своїм комп'ютером, впевнитись у відсутності будь-яких підробок у ПЗ. Зауважимо, що сучасна нормативна база [6] щодо захисту інформації WEB-сторінок розрахована на випадки, коли є довіра до адміністратора, бо там не передбачено користувачів з правами контролерів, а системи голосування без контролю з боку усіх без винятку зацікавлених осіб не мають шансів на беззаперечну довіру виборців.

Навіть на прикладі системи опитування «Викладач очима студентів», з якою можна ознайомитись на сайті http://fit.univ.kiev.ua/archives/3246), де випробувалось описане ПЗ, бачимо, що у разі розкриття викладачами інформації про те, хто як їх оцінює, можуть виникнути негативні наслідки для студентів на іспитах. Для об'єктивності подібного опитування студенти повинні бути впевнені, що адміністратор сервера не в змозі розкрити їх голоси.

Вибір для демонстрації методу конкретної системи не означає, що запропонований метод не може використовуватись за своїм призначенням в інших системах.

Дерево функцій сервера виборчої дільниці зображено на рис. 1, а часова діаграма роботи цього сервера показана на рис. 2.

Зміст та призначення файлів, які повинен занести адміністратор в свою директорію, описано у таблиці 1.

Технологія функціонування серверної програми схематично представлена на рис. 3, а алгоритм обміну даними між виборцем і сервером під час голосування представлено на рис. 4.

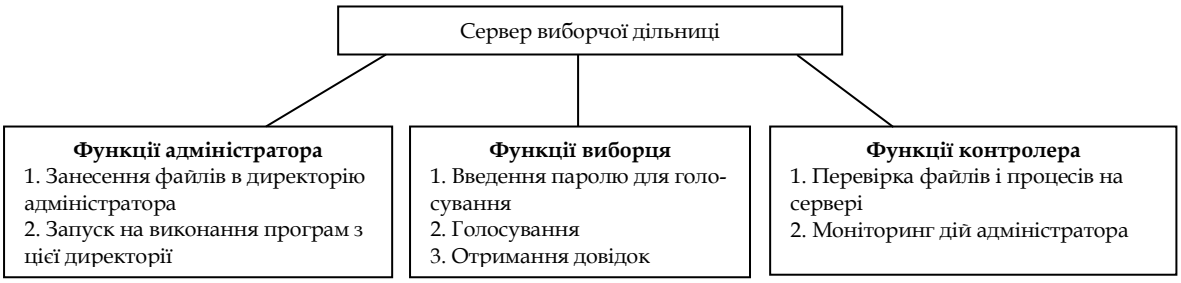


Рис. 1. Дерево функцій сервера виборчої дільниці

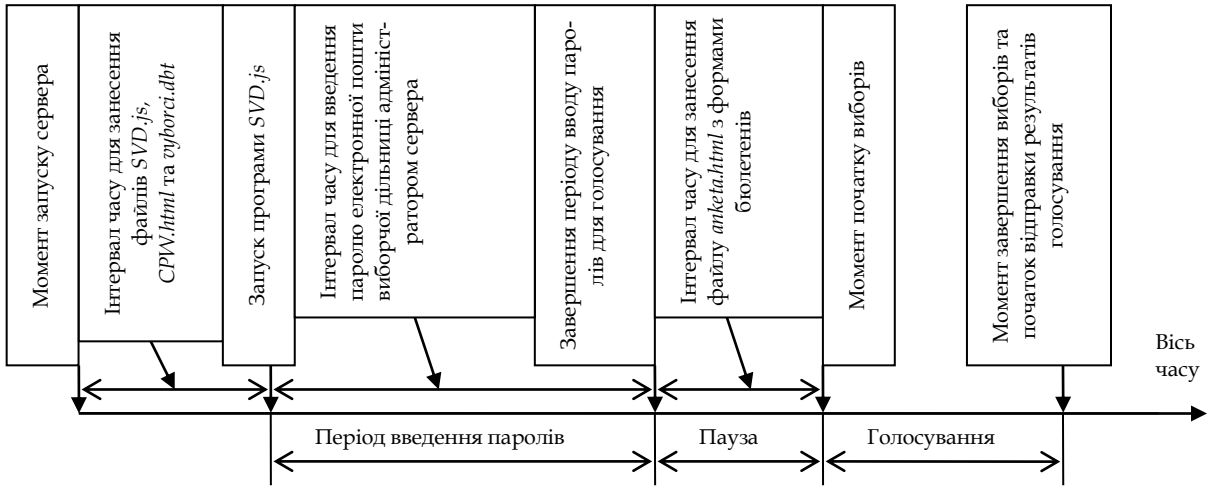


Рис. 2. Часова діаграма роботи сервера виборчої дільниці

Файли прикладного програмного забезпечення Таблиця 1

Ім'я файлу	*Зміст файлу*	*Призначення*
SVD.js	Текст серверної програми на мові *JavaScript* для серверів	Управління роботою сервера виборчої дільниці протягом усього періоду виборчого процесу
CPW.html	Текст клієнтського модулю на мові HTML з програмою обміну даними з сервером на мові *JavaScript* для періоду введення паролів	Реалізація досконало захищеного діалогу між виборцем і серверною програмою в період введення паролів для голосування
vyborci.dbt	База даних про виборців, де критичні дані зберігаються у зашифрованому вигляді	Занесення значень у масиви даних серверної програми для процедур ідентифікації та автентифікації виборців, а також для заповнення довідок про хід та результати голосування
anketa.html	Текст клієнтського модулю на мові HTML з виборчими бюлетенями і програмою обміну даними з сервером на мові *JavaScript* в період голосування, а також для отримання довідок про хід та результати голосування	Реалізація досконало захищеного діалогу між виборцем і серверною програмою в період голосування, а також надання можливості клієнтам отримувати відкриті довідки про хід та результати голосування

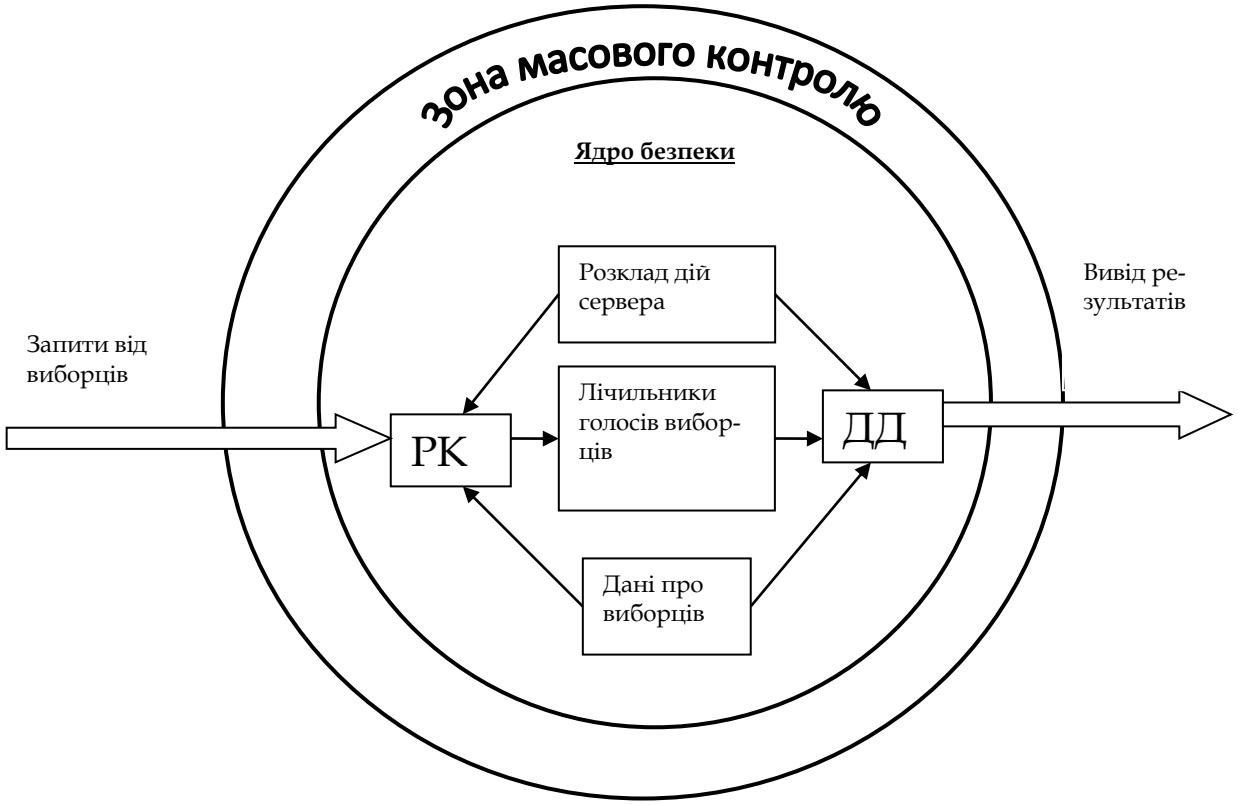


Рис. 3. Технологічна схема безпечного функціонування серверної програми, де прийнято такі скорочення: РК – блок розшифровки та контролю запитів виборців; ДД – блок дозволу доступу до результатів волевиявлення та формування довідок

Через те, що зміст бюлетенів можуть корегувати напередодні виборів, файл *anketa.html* з текстами бюлетенів заносять на сервер в період паузи саме перед початком голосування.

Досконало захищений канал за принципом End-to-End для обміну даними між виборцем і ядром безпеки створюється на початку кожного сеансу зв'язку (див. дії 1-4 на рис. 4). Для цього на кожній стороні обміну даними генерується чисто випадкова послідовність бітів за методом, який описано в роботі [7], після чого, в результаті перетворень за алгоритмом Диффі-Хеллмана, як описано в роботі [5], утворюються однакові випадкові послідовності бітів на обох кінцях обміну даними, що є передумовою для подальшого використання шифру Вернама (*one-time pad*), який забезпечує абсолютну криптографічну стійкість. Розкриття інформації в цьому випадку можливо тільки шляхом подолання стійкості алгоритму Диффі-Хеллмана, що потребує дискретного логарифмування, а це для великих значень довжини бітових послідовностей являє собою надскладну задачу. Таку задачу періодично для деяких окремих випадків вдається розв'язати, витрачаючи на це чимало часу і потужності суперкомп'ютерів [8, 9]. З останніми досягненнями цієї діяльності можна ознайомитись за посиланням: https://en.wikipedia.org/wiki/Discrete_logarithm_records.

В роботі [5] обрано для реалізації алгоритму Диффі-Хеллмана поле Галуа $GF(2^n)$, де n =503, тобто довжина випадкових послідовностей дорівнює 503 біти. Процедура дискретного логарифмування є найбільш ускладненою коли n являє собою безпеч-

не просте число, що належить ряду 359, 383, 467, 479, 503, 563, 587, 719, 839, 863, 887, 983, 1019, …, який обчислюється за формулою:

$$n = 2p + 1, \quad (1)$$

де p – просте число.

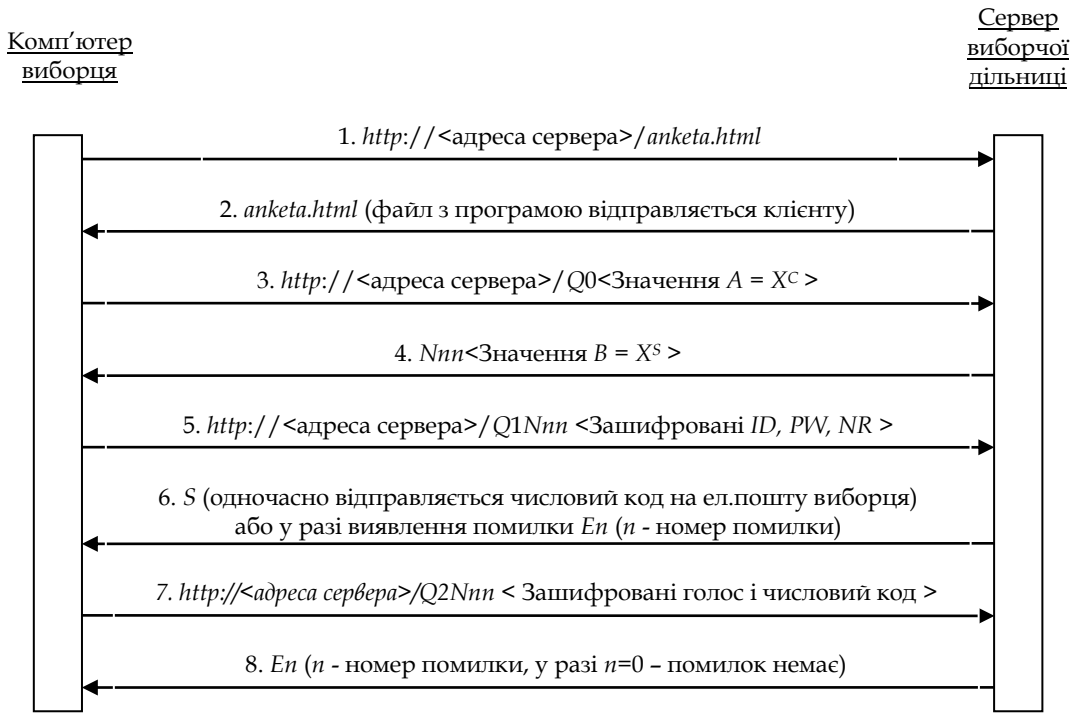


Рис. 4. Алгоритм обміну даними між виборцем і сервером виборчої дільниці, де прийнято такі скорочення: *X* – примітивний елемент поля Галуа; *C* і *S* – випадкові числа; *nn* – умовний номер з'єднання (від 00 до 99) ; *ID* – ідентифікаційні дані виборця; *PW* – пароль виборця; *NR* – номер режиму (0-голосування, 1, 2, 3 – довідки)

Операції перетворення випадкових чисел над полем Галуа $GF(2^{503})$ мають такий вигляд:

$$A = X^C; B = X^S, \quad (2)$$

де X – примітивний елемент поля Галуа $GF(2^{503})$, C – випадкова послідовність з 503 бітів, що отримана на клієнтському пристрої, S – випадкова послідовність з 503 бітів, що отримана на сервері.

Після обміну значеннями A і B між клієнтом і сервером отримаємо остаточний результат у вигляді однакових ключів K на обох кінцях обміну даними:

$$K = B^C = A^S = X^{SC}. \quad (3)$$

Враховуючи те, що кількість інформації, яка потребує захисту під час акту голосування, ніколи не перевищує 500 біт, то найкращим рішенням в цьому випадку є використання шифру Вернама.

У разі збільшення потужності комп'ютерів, збільшуються також можливості дискретного логарифмування, але ніщо не заважає при цьому для досконалого захисту обрати більшу довжину випадкової послідовності бітів. В сучасних умовах витрати часу на шифрування у разі n =503 не перевищують двох секунд, а універсального методу дешифрування поки що не знайдено.

Недоцільність використання стандартних засобів симетричного шифрування, наприклад, ДСТУ 7624:2014, у даному разі пояснюється тим, що кількість бітів для шифрування тут не перевищує довжину ключа. В цих випадках шифр Вернама дозволяє спрощувати реалізацію і одночасно покращувати захист.

Можливо, що в інших системах будуть використані не такі засоби захисту від розкриття голосів під час передавання і підрахунку, як у цій системі, що обрана для демонстрації методу. Це не обмежує впровадження методу в інших системах.

В різні періоди сервер по-різному реагує на запити виборців, що описано у таблиці 2.

Метою даної роботи є надання рекомендацій щодо створення такої технології Інтернет голосування, яка б крім гарантування безпеки голосів виборців від розкриття, а результатів підрахунку голосів – від спотворень, надавала б можливість виборцям голосувати за власним розсудом за умов наявності таких факторів впливу як підкуп, залякування або силовий тиск.

Протидія факторам незаконного впливу на виборців

Для забезпечення виборцям можливості вільного вираження своєї точки зору під час голосування необхідно створити такі умови, щоб будь-який незаконний вплив не завадив проголосувати за власним розсудом.

Досвід вивчення загроз незаконного впливу на виборців свідчить про те, що зловмисник обов'язково хоче дізнатись справжній результат голосування виборця. Для цього виборців примушували вкидати вже заповнені бюлетені, отримані від зловмисників, а свої законні віддавати за винагоро-

ду. В інших випадках виборців примушували фотографувати бюлетені після заповнення. У разі електронного голосування зловмиснику також потрібна інформація про результат, але замість фотографування або заміни бюлетеня він може вимагати, щоб виборець голосував під чиїмось наглядом або щоб виборець дозволив комусь проголосувати замість себе. В усіх випадках зловмиснику важливо отримати інформацію про те як насправді зараховано голос виборця. Без такої інформації втрачається доцільність спроб впливу на виборця, бо зловмисник не буде мати гарантій щодо отримання бажаного результату від своїх дій. В системі Інтернет голосування в Естонії, як вважають розробники, незаконний вплив на виборців нейтралізується тим, що виборець може скільки завгодно разів змінювати свій голос протягом 7 днів.

Але при цьому не враховано те, що зловмисник може запропонувати виборцю за винагороду проголосувати під наглядом в останній день, після чого картку, без якої там голосувати неможливо, заклеїти у поміченому конверті. Бажану винагороду виборець зможе отримати після виборів тільки у тому разі, якщо конверт з карткою не буде пошкоджено. Крім того, можливість змінювати голос протягом 7 днів вимагає збереження голосів виборців в сервері разом з їхніми особистими даними. Цей факт сприяє можливості розкриття голосів виборців.

Реакції сервера на запити клієнтів (виборців) в різні періоди часу Таблиця 2

Назва періоду	*Реакція сервера*
Введення паролів	Відправляє клієнту файл *CPW.html* для підтримки досконало захищеного діалогу щодо введення паролю для голосування
Пауза	Повідомляє клієнта, що час для введення паролів вичерпано
Голосування	Відправляє клієнту файл *anketa.html* з бюлетенями і підтримує досконало захищений діалог щодо голосування або відправляє довідку у разі отримання відповідного запиту від клієнта
Завершення голосування	Повідомляє клієнта, що час для голосування вичерпано і відправляє довідку про результати голосування

У системі, що була розглянута вище, голоси виборців одразу знищуються після залічування. Іншою перевагою цієї системи у порівнянні з Естонською є те, що виборці для голосування можуть скористатись звичним методом доступу до мережі Інтернет з будь-якого термінального пристрою (комп'ютер, планшет, смартфон, телевізор з функцією Smart-TV тощо) без застосування додаткових спеціалізованих програмних або апаратних засобів. Інакше втрачається основна привабливість дистанційного волевиявлення для широкого загалу виборців.

В роботі [10] для боротьби з незаконним впливом на виборців запропоновано ввести два варіанти авторизації, один для справжнього голосування, а другий – для фіктивного. При цьому з'являються додаткові вимоги до виборця, бо замість одного пароля, йому треба пам'ятати і не переплутати два паролі. Головне, що за умов повністю відкритого програмного забезпечення, від зловмисника на сервері нічого неможливо приховати. Знаючи про таку властивість системи, зловмисник буде вимагати від виборця проголосувати два рази з різними варіантами авторизації.

Метод, який пропонується у цій статті, не має жодного з перелічених недоліків.

Зазвичай системи Інтернет голосування інформують виборців про можливі помилки, як під час процедури авторизації, так і після завершення голосування. Приклад такого інформування наведено у таблиці 3.

У разі інформування подібно тому, як показано у таблиці 3, відкриваються можливості для незаконного впливу зловмисників на виборців, бо всю потрібну інформацію про те як проголосував виборець можна отримати шляхом спостереження за процесом голосування.

Метод протидії незаконному впливу на виборців, який пропонується в даній роботі, у деякій мірі обмежує інформативність повідомлень від сервера про хід голосування, але при цьому він не залишає для зловмисників жодного шансу для того, щоб дізнатись про те, як дійсно проголосував виборець.

Крім того, у порівнянні з методом, який запропоновано у роботі [10], виборцю не треба запам'ятовувати ніяких зайвих паролів, крім одного вірного пароля, який потрібно знати в усіх подібних системах авторизації.

Головною перевагою нашого методу є те, що зловмисники, ознайомившись з серверною програмою, можуть впевнитись у відсутності будь-якої можливості для отримання бажаної інформації і прийти до висновку про недоцільність своїх незаконних дій.

Варіант повідомлень, які пропонується відправляти виборцю від сервера з метою протидії незаконному впливу на процес голосування, представлено у таблиці 4.

Аналізуючи повідомлення сервера, що представлені у таблиці 4, неможливо дізнатись про дійсний результат голосування, бо у всіх випадках голосування з будь-яким паролем, що має таку ж довжину, як правильний пароль, повідомлення від сервера будуть однаковими. Зрозуміло, що сервер зараховує від кожного виборця тільки один голос, який буде подано з правильним паролем.

Єдине питання, яке може виникнути у супротивників такої пропозиції, буде стосуватись того, яким чином сам виборець дізнається про результат свого голосування.

Розглянемо варіанти помилок, які можуть бути допущені виборцем, і відповідні реакції сервера:

– помилка в ідентифікаційних даних супроводжується повідомленням сервера;

– помилкова довжина паролю супроводжується повідомленням сервера;

– помилковий числовий код підтвердження супроводжується повідомленням сервера;

– помилковий пароль правильної довжини виявляється сервером, але супроводжується тими ж повідомленнями, як і вірний пароль.

Як бачимо, єдина помилка, яка може пройти непомітною для виборця, це помилковий пароль правильної довжини. Для того, щоб унеможливити допущення непоміченої помилки під час введення паролю, можна без жодного побоювання надати можливість відкритого введення цього паролю. Зауважимо, що закривати пароль від спостерігачів доцільно тільки в тих випадках, коли пароль можна буде використати в якомусь іншому випадку, а цей пароль має одноразову дію, бо повторне голосування з правильним паролем не зараховується. Пароль для голосування, як описано в роботі [5], виборець обирає самостійно і власноручно заносить його в оперативну пам'ять сервера, перебуваючи у спеціальному безпечному місці. Якщо виборець хоч один раз виконав акт голосування з правильним паролем і отримав підтвердження від сервера, то не має ніяких підстав для сумнівів в тому, що його голос з абсолютною точністю зараховано, бо вивіреним комп'ютерним програмам можна довіряти на 100%. Знання і нерозголошення паролю є важливою перевагою виборця над зловмисниками, які планують позбавити його можливості голосувати за власним розсудом.

Повідомлення сервера на дії виборця без захисту від незаконного впливу Таблиця 3

Дія виборця	*Можливий варіант відповіді від сервера*
Помилкове введення ідентифікаційних даних	«Звернення відхилено через помилкові ідентифікаційні дані»
Правильне введення ідентифікаційних даних, але помилка у паролі	«Помилковий пароль. Звернення відхилено»
Правильне введення ідентифікаційних даних і пароля	«Робіть свій вибір.» або ніяких повідомлень у разі якщо виборець ще не проголосував. «Доступ відхилено через спробу повторного голосування»
Помилкове введення числового коду*	«Ваш голос відхилено через помилковий числовий код»
Правильне введення числового коду*	«Ваш голос прийнято і зараховано»

*Числовий код сервер відправляє виборцю на E-mail або через СМС.

Повідомлення сервера на дії виборця у разі захисту від незаконного впливу Таблиця 4

Дія виборця	*Можливий варіант відповіді від сервера*
Помилкове введення ідентифікаційних даних	«Звернення відхилено через помилкові ідентифікаційні дані»
Правильне введення ідентифікаційних даних, але помилка у довжині паролю	«Помилковий пароль. Звернення відхилено»
Правильне введення ідентифікаційних даних і правильна довжина паролю	«Робіть свій вибір.» або ніяких повідомлень
Помилкове введення числового коду	«Ваш голос відхилено через помилковий числовий код»
Правильне введення числового коду	«Ваш голос прийнято сервером»

Обмеження у видачі довідкової інформації про хід голосування з метою протидії загрозам впливу на виборців стосується тільки довідки про персональну активність виборців. У довідці про кількість виборців, яка формується на запити виборця по всіх квартирах його будинку, по всіх будинках його вулиці і по всіх вулицях його виборчої дільниці, не можна буде вказувати кількість виборців, які вже проголосували. При цьому головна користь від цієї довідки не втрачається, бо інформація про кількість виборців надає можливість виявляти приписки. За допомогою цієї довідки кожен виборець може виявити зайву кількість зареєстрованих виборців у якійсь квартирі або неіснуючі квартири чи будинки. Довідку про активність виборців можна надавати у вигляді проценту від загальної їх кількості, що не дозволяє розкрити інформацію про активність конкретного виборця.

Висновки

1. У системах Інтернет голосування вкрай важливо гарантувати безпеку голосів виборців від розкриття, а результати підрахунку голосів – від спотворень, крім того бажано надати можливість голосування зі звичних для користувачів засобів доступу до мережі Інтернет, будь то комп'ютер довільного типу, планшет, смартфон або телевізор з функцією SmartTV без будь-яких додаткових програмних або апаратних засобів. При цьому система голосування повинна бути повністю контрольованою з боку будь-якої зацікавленої особи, щоб не було жодного приводу для недовіри щодо точності її функціонування. Але всі ці характеристики не позбавляють можливості незаконного впливу на виборців підкупом, залякуванням або силовим тиском, що може суттєво вплинути на результат голосування, спотворюючи справжність виявлення суспільної думки і заважаючи розвитку демократичного суспільства.

2. Враховуючи той факт, що зловмисникам, які займаються протизаконною діяльністю, примушуючи виборців голосувати не за власним розсудом, а за вказівкою, потрібна інформація про результат голосування кожного з цих виборців, в даній роботі запропоновано метод протидії незаконному впливу на виборців, який не залишає шансів зловмисникам дізнатись про те, як дійсно проголосували виборці. Суть цього методу полягає в тому, що повідомлення, які виборцю відправляє сервер, нічим не відрізняються у разі введення будь-якого паролю правильної довжини.

3. Впровадження запропонованого методу в умовах відкритої для вивчення і перевірки системи Інтернет голосування, надає можливість впевнитись

у неможливості отримання зловмисниками бажаної інформації і примушує прийти до висновку про недоцільність незаконного впливу на виборців.

4. Наведений варіант побудови системи Інтернет голосування демонструє можливість реалізації запропонованого методу і не є єдиним варіантом для впровадження цього методу. Потрібні подальші дослідження у напрямку визначення найкращих технічних рішень з урахуванням конкретних умов застосування систем Інтернет голосування.

Література

[1] E-hääletamise tarkvara [Electronic resource] – Available at: https://github.com/vvk-ehk/evalimine.

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

[3] Schneier B. What's Wrong With Electronic Voting Machines? [Electronic resource] – Available at: https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html.

[4] Shannon C.E. The Communication Theory of Secrecy Systems / C.E. Shannon // Bell System Technical Journal. – 1949 – v.28, n.4 – P.654-715.

[5] Вишняков В.М. Відкрита система таємного голосування / В.М. Вишняков, М.П. Пригара, О.В. Воронін // Управління розвитком складних систем. Збірник наукових праць. – 2014. – Вип. 20. – С. 110-115.

[6] НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу – Чинний від 15.04.2003. – К.: ДСТСЗІ СБ України, 2003.

[7] 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.

[8] Jens Zumbrägel. «Discrete Logarithms in GF(2^9234)», 31 January 2014, [Електронний ресурс] – Режим доступу: https://listserv.nodak.edu/cgi-bin/wa .exe?A2=NMBRTHRY;9aa2b043.1401.

[9] Antoine J. «Discrete logarithms in GF(2^{6168}) [=GF((2^{257})^{24})]», May 21, 2013. [Electronic resource] – Available at: https://listserv.nodak.edu/cgi-bin/waexe ?A2=ind1305&L=NMBRTHRY&F=&S=&P=3034.

[10] Essex A., Clark J., Hengartner U. Cobra: Toward Concurrent Ballot Authorization for Internet Voting. Electronic Voting Technology Workshop/ Work shop on Trustworthy Elections (EVT/WOTE'12). Bellevue (USA), 2012, pp. 1-13.

УДК 004.78 (045)

Чуприн В.М., Вышняков В.М., Пригара М.П. Метод борьбы с противозаконным влиянием на избирателей в системе Интернет голосования

Аннотация. *Рассматривается система Интернет голосования с полностью открытым для ознакомления и испытания программным обеспечением. Акт голосования в этой системе может осуществляться с помощью любого клиентского устройства, имеющего доступ в Интернет. Это может быть компьютер любого типа, планшет, смартфон или телевизор с функцией SmartTV без использования каких-либо дополнительных программных или аппаратных средств. Для обеспечения доверия со стороны избирателей предоставляется возможность контроля за работой системы в реальном времени любому заинтересованному лицу. В качестве возможных нарушителей безопасности процесса голосования рассматриваются все без исключения участники избирательного процесса, включая персонал, который несет ответственность за те или иные функции или участки системы голосования. При этом гарантируется безопасность голосов избирателей от раскрытия, а точность подсчета голосов – от нарушений. Предлагается такой метод голосования в этой системе, который обеспечивает для избирателей возможность свободного волеизъявления при условии наличия факторов противозаконного влияния, таких как подкуп, запугивание или силовое давление. Применение предлагаемого метода исключает возможность получения информации о результате голосования любого отдельно взятого избирателя, из-за чего становится бессмысленным использование противозаконного влияния на избирателей.*

Ключевые слова: *Интернет голосование, безопасность информации, метод голосования, нейтрализация противозаконного влияния на избирателей.*

Chupryn V., Vyshniakov V., Prygara M. Method of combating illegal influence on voters in the Internet voting system

Abstract. *A system of Internet voting with fully open to inspection and testing software. The act of voting in this system can be carried out using any device with Internet access. This can be any type of computer, tablet, smartphone, or TV with SmartTV function without using any additional software or hardware. In order to ensure the confidence of the voters the opportunity to monitor the performance of the system in real time to any interested party. As a potential security violators of the voting process are considered by all participants in the electoral process, including personnel, which is responsible for certain functions or areas of the voting system. This ensures the safety of the votes from the disclosure, and the accuracy of the counting of votes - against abuse. It proposed a method of voting in this system, which provides for the possibility of free will of voters subject to the availability of illegal influence factors such as bribery, intimidation or military pressure. Application of the proposed method eliminates the possibility of obtaining information about the result of the vote of any particular voter, because of what becomes meaningless use of illegal influence on voters.*

Key words: *Internet voting, information security, the voting method, the neutralization of illegal influence on voters.*

Отримано *20 жовтня 2016 року*, затверджено редколегією *15 лютого 2017 року*