УДК 004.771

ТЕХНОЛОГІЯ АВТЕНТИФІКАЦІЇ ВИБОРЦІВ У ВІДКРИТІЙ СИСТЕМІ ІНТЕРНЕТ ГОЛОСУВАННЯ

МАЧАЛІН І.О., ВИШНЯКОВ В.М., КОМАРНИЦЬКИЙ О.О.

Пропонується технологія дистанційної автентифікації виборців у відкритій системі Інтернет голосування з використанням біологічних або інших додаткових ознак, що усуває можливість передачі права голосу іншій особі і дозволяє позбутися обов'язкової очної перевірки осіб виборців перед кожним актом волевиявлення, що особливо важливо у разі тривалих відряджень виборців. При цьому зберігаються усі позитивні якості відкритої системи, включаючи повну контрольованість процесів на сервері Інтернет голосування в режимі реального часу.

Ключові слова: Інтернет голосування, дистанційна автентифікація, збереження таємниці голосів, відкрита система голосування, забезпечення довіри виборців.

1. Вступ

Дистанційне голосування через Інтернет (надалі ІГ) надає суттєві переваги виборцям щодо зручності, мобільності та економії часу. Крім того, скорочуються витрати на друк бюлетенів. Але суттєвим стримуючим фактором на шляху розвитку систем ІГ є недовіра виборців через неможливість впевнитись у тому, що в електронних засобах для голосування не закладено можливостей для розкриття таємниці голосів та/або викривлення результатів волевиявлення [1, 2]. Відомо, що для подолання недовіри треба надавати широкі можливості для контролю всіх тих об'єктів і процесів, які викликають сумніви. При цьому від повноти можливостей контролю залежить рівень довіри. Зрозуміло, що для беззаперечної довіри необхідно надати усім бажаючим можливість контролювати усі складові системи протягом усього часу її функціонування. Саме такий підхід запропоновано в роботі [3], де описані принципи побудови відкритої системи таємного голосування, у якій надається можливість масового дистанційного контролю з боку необмеженої кількості будь-яких осіб щодо усіх програмних засобів та процесів в режимі реального часу функціонування системи ІГ. У роботі [4] розвинуто цей підхід і доведено, що після проведення такого контролю не залишається підстав для недовіри, бо всі елементи системи і дії обслуговуючого персоналу, які можуть бути потенційно небезпечними, є відкритими для масового спостереження. Іншими словами, будь-яка спроба вчинення зловмисної дії у такій системі може бути виявлена та зафіксована контролюючими особами. При цьому забезпечується збереження таємниці голосів і неможливість викривлення результатів волевиявлення. Фактично тільки такі системи можуть претендувати на беззаперечну довіру виборців, бо наявність хоч однієї закритої частини завжди буде породжувати підозри щодо фальсифікації. В роботі [5] показана можливість протидії незаконному впливу на виборців (підкупом, залякуванням або силовим тиском) в умовах повністю контрольованої системи. Але, крім описаних переваг відкритих систем ІГ, слід відмітити, що залишається без відповіді питання дистанційної автентифікації особи виборця. Оскільки однією з відомих вимог до систем голосування є заборона передачі свого права голосу іншій особі, то можна вважати актуальною задачу дистанційного підтвердження особи виборця (або автентифікацію) в умовах повної відкритості (прозорості) системи ІГ з метою усунення очної перевірки особи в період уточнення списків голосуючих перед кожним актом волевиявлення. Це має особливе значення у випадках тривалих відряджень виборців.

2. Аналіз відомих рішень і постановка завдання

Для дистанційного підтвердження особи може використовуватись низка відомих ознак. Наприклад, в Естонії, де було вперше впроваджено ІГ на виборах державного масштабу [6], для підтвердження особи виборця використовують персональну електронну картку, яка є заміною паспорту. Одним з недоліків такого методу підтвердження є потреба у спеціальному пристрої для зчитування інформації з електронної картки. Крім того, як показано в роботі [5], такий метод автентифікації не захищає виборця від незаконного впливу. В Україні з 1 січня 2016 року також розпочато впровадження пластикових ID-карток замість паспортів. Але слід зауважити, що неможливо за допомогою будь-якої картки досягти беззаперечної гарантії того, що проголосувала саме та, а не якась інша особа. Це багаторазово продемонстровано голосуючими у ВР України. Тільки у тих випадках, коли ознаку неможливо відокремити від особи виборця, може бути досягнута беззаперечна гарантія того, що проголосувала саме та, а не якась інша особа. Такими властивостями у тій чи іншій мірі наділені біологічні ознаки людини. Серед цих ознак, крім широко відомих відбитків пальців, в останні десятиріччя використовують сітківку ока, райдужну оболонку ока, геометрію обличчя, термограму обличчя, геометрію руки, голос та динаміку почерку [7-10]. Найбільш придатною з перелічених ознак для дистанційної автентифікації можна вважати голос, бо майже все обладнання для доступу до мережі Інтернет має вбудований мікрофон, а у разі його відсутності можна скористатись окре-

мим телефоном. В роботі [10] щодо розпізнавання по голосу вказано на високу імовірність помилок другого роду. Такі помилки у разі зміни голосу через хворобу або з інших причин можуть унеможливити здійснення виборцем акту волевиявлення, що неприпустимо для системи голосування. Слід зауважити, що вплив помилок першого роду щодо розпізнавання голосу можна компенсувати шляхом використання комбінації голосу з паролем. При цьому для того, щоб проголосувати за когось іншого, треба крім знання паролю ще й мати такий самий або у достатній мірі схожий голос. Результати експериментальних досліджень, що наведені в роботі [9] і представлені у таблиці, свідчать про існування суттєвої залежності кількості помилок розпізнавання особи від варіанту прочитаного тексту.

Варіант тексту	Процент помилок
«шиншилла шила шубу»	18,7
«Клара украла коралі»	1,2
«витівка олігарха»	3,8

Бачимо з наведених у таблиці значень, що шиплячі звуки негативно впливають на якість розпізнавання особи, а обираючи тексти з переважною більшістю дзвінких звуків, можна значно підвищити цю якість. Дослідження в напрямку поліпшення розпізнавання по голосу тривають, а існуючі результати свідчать про можливість за допомогою біологічних ознак отримувати дані для уточнення особи виборця. В роботі [11] для автентифікації особи виборців обрано електронний цифровий підпис (ЕЦП), який може використовуватись в інших цілях, що не пов'язані з виборами, і тому не може бути переданий іншій особі. Але для того, щоб використовувати будь-яке уточнення особи у відкритих системах дистанційного голосування, слід розробити технологію, яка б дозволяла підключати додаткові засоби розпізнавання, не втрачаючи жодної з описаних вище переваг та включаючи прозорість і контрольованість. Розробка саме такої технології і є завданням даного дослідження.

3. Основна частина дослідження

В роботі [4] представлено логічну модель відкритої системи дистанційного голосування , яку зображено на рис. 1, де все, що знаходиться в середині зовнішнього кола, відповідає множині об'єктів сервера ІГ.

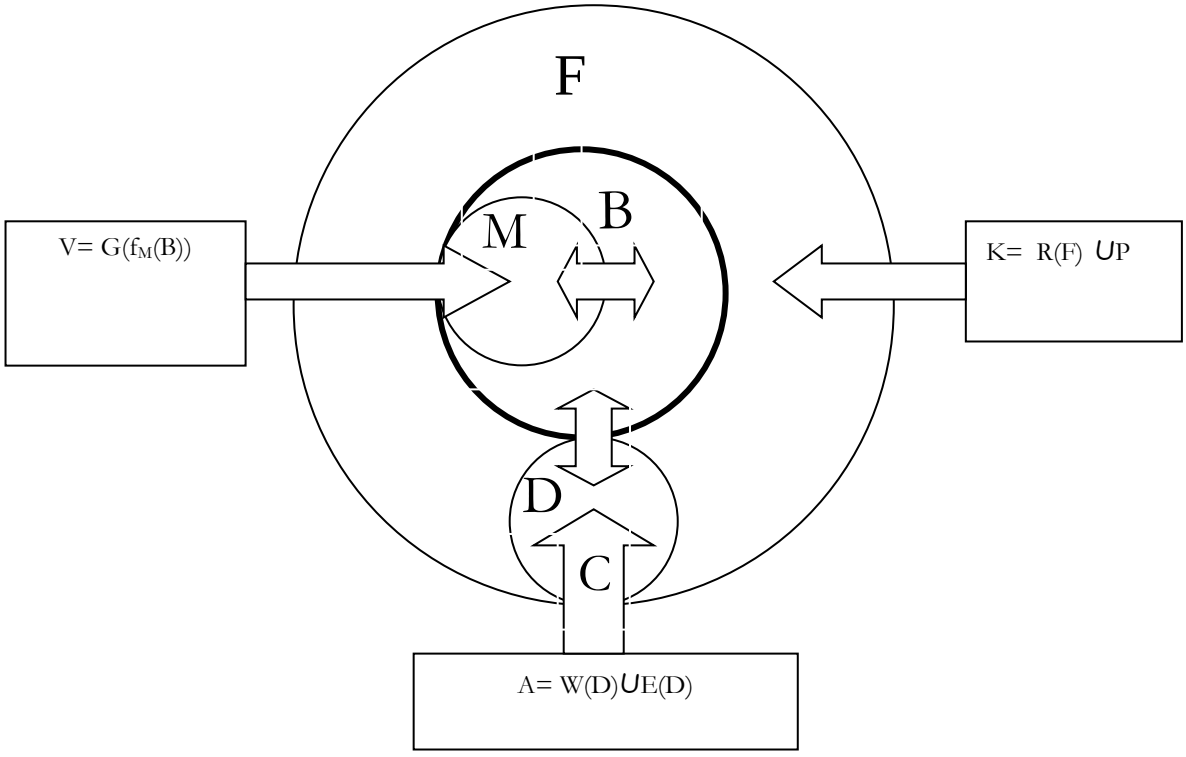

Рис. 1. Логічна модель відкритої системи дистанційного голосування

У цій моделі передбачено, що операційна система сервера ІГ (після певних процедур налаштування) дозволяє виконувати користувачам ті і тільки ті дії, що є елементами множини Q, де Q - об'єднання множин дій голосуючих виборців, адміністратора сервера ІГ та контролерів, які в сукупності складають повну групу можливих дій користувачів:

$$Q=V\cup A\cup K$$

де V – множина дій голосуючих виборців (ця множина у разі потреби може доповнюватись діями осіб для виконання спеціалізованих наперед відомих дій, що повинні бути відображені у заздалегідь відкритій прикладній програмі); A – множина можливих (штатних і нештатних) дій адміністратора сервера; K – множина дій контролюючих осіб.

Слід зауважити, що всі некоректні і помилкові дії тут не розглядаються, бо вони не сприймаються сервером.

Повна множина об'єктів, над якими можуть виконуватись дії користувачів, складається з таких множин: F – множина даних, що розміщені у файловій системі сервера, включаючи файли з програмами, готовими до виконання, а також з історією команд адміністратора; C – множина відображень команд адміністратора сервера, 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, причому $B \not\subset F$; M – множина даних для моніторингу звернень виборців (ці дані використовує прикладна програма для авторизації голосуючих виборців), причому $M \subset B$ (множина M у разі необхідності може доповнюватись діями осіб для виконання спеціалізованих наперед відомих процедур, що повинні бути відображені у заздалегідь відкритій прикладній програмі).

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

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

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;

$$A = W(D) \cup E(D),$$

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

$$K = R(F) \cup P,$$

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 (команд) контролера щодо перевірки статусу процесів на сервері та отримання інших відомостей, які можуть свідчити про порушення політики безпеки.

Єдиний користувач, який має можливість виконання небезпечних дій на сервері, це – адміністратор сервера, бо будь-які дії виборців і контролерів не здатні утворити загрозу штатній роботі сервера. Тому, для запобігання можливим несанкціонованим діям, адміністратору дозволено виконувати тільки дві дії, а саме: заносити файли в свою директорію і запускати на виконання (тільки один раз) програму з цієї директорії. При цьому будь-яка нештатна дія адміністратора може бути зафіксована контролерами. Не існує таких дій, які можна було б приховати від контролерів. Представлена модель (див. рис. 1) за умов повної відкритості програмного забезпечення, включаючи операційну систему, дозволяє забезпечити досконалий захист критичних даних при обміні через середовище Інтернет, а також гарантує збереження таємниці голосів та неможливість фальсифікації результатів волевиявлення за умови повної недовіри до усіх без винятку користувачів системи. Крім того, як показано в роботі [5], така модель дозволяє застосовування методу протидії незаконному впливу на виборців. Головним досягненням відкритих систем дистанційного голосування є можливість їх повноцінного контролю з боку необмеженої кількості будь-яких осіб, а саме такого контролю, після проведення якого не повинно залишитись жодних підстав для недовіри щодо дійсності результатів волевиявлення і збереження таємниці голосів. З метою збереження досягнень відкритої системи не можна розміщувати на сервері для дистанційного голосування файли, які не є відкритими для ознайомлення, бо це позбавляє систему прозорості. А встановлення на цьому сервері додаткового програмного забезпечення для автентифікації осіб виборців буде ускладнювати процедуру спостереження за роботою сервера та перешкоджатиме проведенню повноцінного контролю. Тому розміщення на сервері дистанційного голосування додаткових засобів для розпізнавання осіб виборців є неприпустимим. Навпаки, слід максимально обмежувати функціональність цього сервера, видаляючи з нього усі зайві файли, з метою забезпечення прозорості для повноцінного контролю з боку спостерігачів. Таким чином, розміщення додаткових засобів для розпізнавання осіб виборців потребує додаткового сервера, який повинен сприймати ознаки виборців і обмінюватись даними з сервером для голосування.

Розглянемо технологічний цикл функціонування системи дистанційного голосування, зображений на рис. 2, з метою визначення часових інтервалів, у яких доцільно розпізнавання осіб виборців з використанням біологічних або інших додаткових ознак.

Рис. 2. Технологічний цикл функціонування системи голосування

На рис. 2 сірим тоном виділені процеси, які відбуваються на сервері ІГ, і прийнято такі скорочення назв періодів технологічного циклу: ППД – період підготовки даних про претендентів на дистанційне голосування; ППС – період підготовки сервера ІГ (встановлення ОС та програм загального користування); ППЗ – прикладне програмне забезпечення для дистанційного голосування; ПВЕБ – період введення електронних бюлетенів (в цей період запити виборців сервером не обслуговуються, а в дільничних списках виборців помічають тих, хто голосуватиме дистанційно, щоб не видавати їм паперові бюлетені). Проаналізуємо кожний з періодів технологічного циклу з метою визначення тих періодів, де є потреба у додаткових засобах розпізнавання осіб виборців.

В період підготовки даних про претендентів на дистанційне голосування необхідна особиста присутність виборців з паспортами. В цей період відбувається очна перевірка осіб виборців і занесення в базу даних відомостей про них та ознак, що необхідні для ідентифікації та автентифікації. Для зберігання цих даних використовується окремий сервер, який працює незалежно від сервера ІГ і може зберігати дані протягом багатьох голосувань.

В період підготовки сервера ІГ, крім встановлення ОС *OpenBSD* і пакетів *Node.js*, які забезпечують виконання програми на мові *Java Script*, створюють користувача *kontrol* з правами спостерігача (без права на внесення будь-яких змін на сервері), а також користувача *admin* з правами роботи виключно у директорії *home/admin* і блокують користувача *root* з повними правами. Після цього сервер буде працювати автоматично в режимі обмеженої функціональності, що дозволяє уникнути будь-яких спроб щодо зловмисного втручання в роботу сервера.

В період встановлення ППЗ адміністратор повинен занести в директорію *home/admin* такі три файли:

– файл з серверною програмою на мові *Java Script*;

– файл з клієнтською програмою на мовах *HTML* та *Java Script*;

– файл з даними, який формується по запиту адміністратора на окремому сервері для кожного голосування. Конфіденційні дані у цьому файлі знаходяться у зашифрованому вигляді.

З початку цього періоду кожен користувач мережі може отримати права на спостереження за усіма файлами і параметрами процесів на сервері ІГ. Це надає можливість впевнитись у тому, що все програмне забезпечення сервера ІГ є штатним, а потрібні дії адміністратора виконуються точно за графіком. Слід зауважити, що цей графік, а також все програмне забезпечення заздалегідь відкриті для проведення будь-яких експертиз.

В період введення паролів для дистанційного голосування виборці повинні пройти процедуру автентифікації. Слід зауважити, що в цей період згідно з виборчим законодавством [12] на основі Державного реєстру виборців (ДРВ) складаються, а потім уточнюються списки виборців. Тривалість підготовчого періоду зазвичай вкладається в 15 днів до виборів, бо раніше за законом можуть бути ще не створені дільничні комісії. Період введення паролів недоцільно розпочинати до створення виборчих дільниць, а оскільки збільшення цього періоду розширює інтервал часу для обрання виборцями зручного моменту проходження автентифікації, то зменшувати цей період теж недоцільно. В роботі [3] для введення паролю запропоновано приймати виборців у відділах ДРВ, де й проводити очну перевірку. Але завдяки дистанційній автентифікації не

обов'язковою стає очна перевірка, що особливо доцільно у разі тривалих відряджень виборців. Таким чином, саме в період введення паролів для дистанційного голосування існує потреба у додаткових засобах розпізнавання осіб виборців, щоб уникнути можливої підміни особи голосуючого.

В період введення електронних бюлетенів запити не обслуговуються, тому залишається проаналізувати тільки період голосування. В цей час виконуються найбільш відповідальні дії, але за допомогою нейтралізації незаконного впливу на виборців, як запропоновано в роботі [5], шансів примусити виборця голосувати всупереч власному розсуду не існує. Це може статись тільки тоді, коли сам виборець передасть свій вірний пароль для голосування іншій особі, при цьому виборець захищений тим, що має можливість передати зловмиснику помилковий пароль, бо система однаково реагує як на вірний, так і на помилковий пароль. Оскільки цей пароль вводять у відкритому вигляді, то сам виборець завжди побачить і виправить помилку. Через відкрите введення паролю не виникає небезпеки, бо пароль діє лише один раз і ним не можна скористатись вдруге. У разі виникнення сумнівів у виборця щодо точності пароля можна багато разів голосувати з різними паролями, але зараховано буде тільки один голос з вірним паролем.

Технологію отримання пароля для голосування у спеціалізованому пункті представлено на рис. 3.

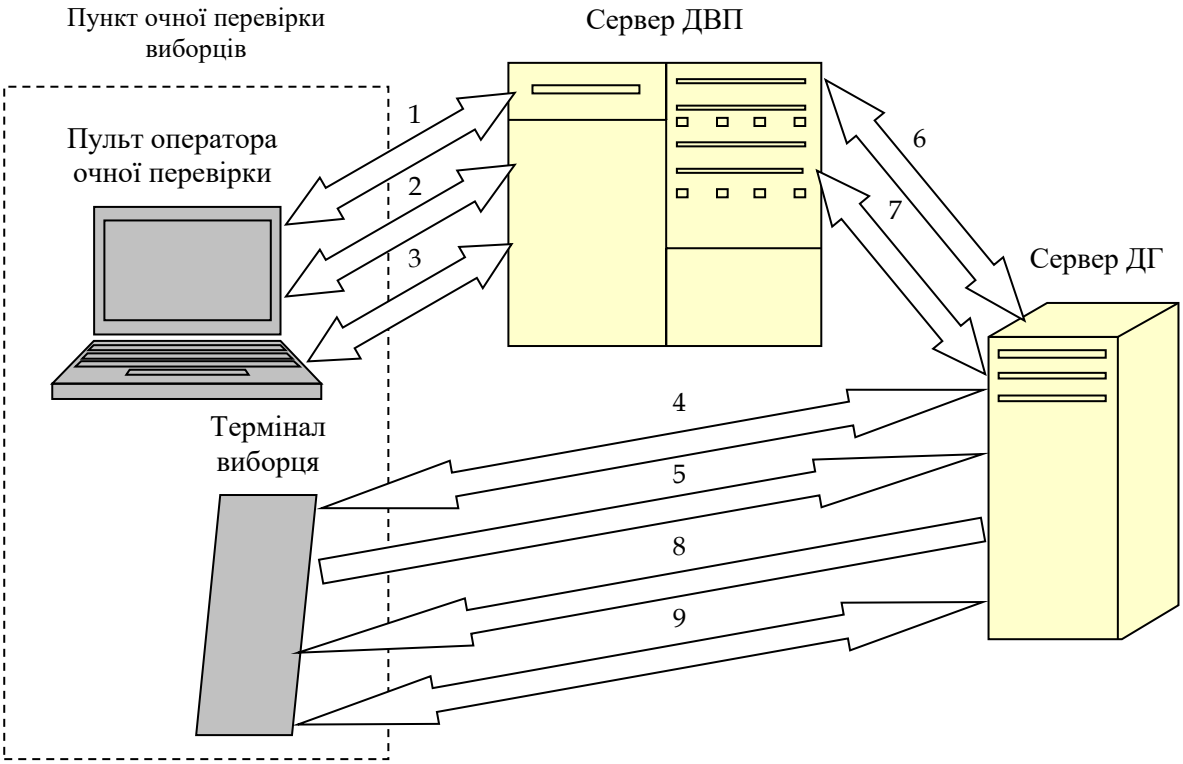

Рис. 3. Технологія отримання пароля для голосування у спеціалізованому пункті, де Сервер ДВП – сервер дозволу введення паролю

Ця технологія передбачає прибуття виборця з паспортом і, можливо, зі своїм мобільним терміналом до спеціалізованого пункту. Замість свого терміналу виборець може скористатись будь-яким іншим, наприклад, тим, що призначений для загального користування, але своєму він більше довірятиме. Після очної перевірки особи виконується така послідовність дій:

1. Оператор відправляє на сервер ДВП запит для утворення захищеного з'єднання (через обмін ключами за алгоритмом Діффі-Геллмана).
2. Оператор авторизується через захищене з'єднання та отримує дозвіл на відправку ідентифікатора виборця.
3. Оператор відправляє на сервер ДВП ідентифікатор виборця (після очної перевірки) і отримує повідомлення про надання 10 хвилин для введення паролю.
4. Виборець відправляє на сервер ДГ запит на утворення захищеного з'єднання (через обмін ключами за алгоритмом Діффі-Геллмана).
5. Виборець авторизується через захищене з'єднання на сервері ДГ і очікує дозвіл на відправку пароля.

6. Сервер ДГ утворює захищене з'єднання з сервером ДВП (через обмін ключами за алгоритмом Діффі-Геллмана).
7. Сервер ДГ відправляє на сервер ДВП запит з ідентифікатором виборця і, якщо момент запиту вкладається у виділені 10 хвилин, отримує відповідь з цим самим ідентифікатором.
8. Сервер ДГ відправляє на термінал виборця дозвіл для введення паролю.
9. Виборець відправляє на сервер пароль для голосування і отримує відповідь про успішне завершення процедури.

У разі, коли момент запиту (див. дію 7) не вкладається у виділені 10 хвилин, відповідь сервера ДВП замість ідентифікатора заповнюється нулями. При цьому виборцю замість дозволу для введення паролю відправляється відмова.

Введення сервера ДВП дозволяє при повному збереженні прозорості сервера ІГ доповнювати систему додатковими засобами дистанційного розпізнавання осіб виборців по голосу, по ЕЦП. Ці засоби встановлюються на сервері ДВП, який не потребує повної контрольованості (прозорості) в режимі реального часу, бо в період голосування, а тільки в цей період на сервері ІГ з'являється інформація, яка потребує абсолютного захисту, ніякої взаємодії між серверами ІГ і ДВП не відбувається. Тому на сервері ДВП можуть використовуватись традиційні засоби захисту інформації. Оскільки між обома серверами для кожного сеансу обміну даними утворюється спеціальний захищений канал зв'язку, то це дозволяє розміщувати їх незалежно один від одного в довільному місці мережі Інтернет. Запропонований в даній роботі розподіл дій між серверами ІГ і ДВП дозволяє виборцям отримувати пароль для голосування без обов'язкової очної перевірки. Кількість обраних виборцями додаткових ознак для автентифікації залежить тільки від можливостей придбання ними тих чи інших засобів для введення цих ознак. Запропонована технологія представлена на рис. 4.

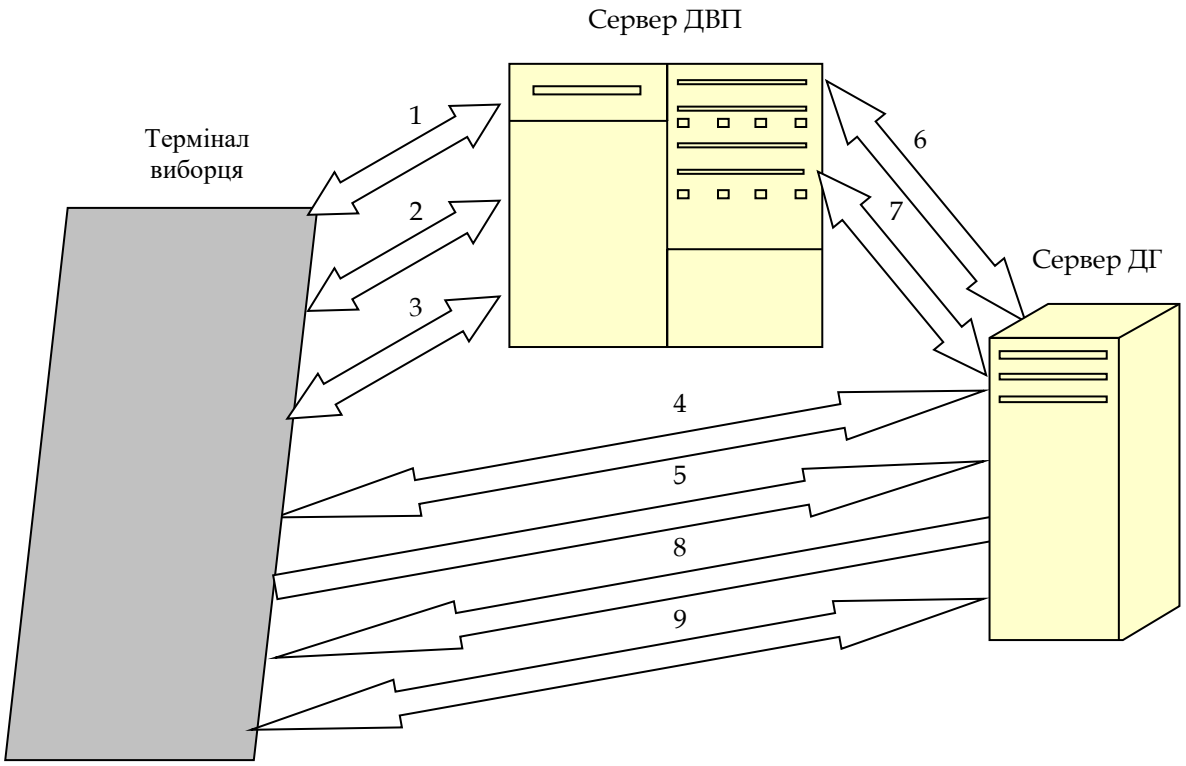

Рис. 4. Технологія отримання пароля для голосування без очної перевірки

Ця технологія передбачає наявність на сервері ДВП біологічних та/або інших ознак виборців, які заздалегідь повинні бути занесені в базу даних. Крім того, на сервері ДВП повинно бути встановлено програмне забезпечення для розпізнавання осіб виборців за цими ознаками в дистанційному режимі. При цьому для отримання пароля виконується така послідовність дій:

1. Виборець відправляє на сервер ДВП запит для утворення захищеного з'єднання (через обмін ключами за алгоритмом Діффі-Геллмана).
2. Виборець авторизується через захищене з'єднання та отримує запит на введення біологічних або інших додаткових ознак своєї особи.
3. Виборець виконує запит сервера ДВП щодо введення додаткових ознак та отримує повідомлення про вдалу автентифікацію і надання 10 хвилин для введення пароля. У разі невдалої

автентифікації виборець отримає запрошення на повторну спробу введення додаткових ознак. Слід зауважити, що кількість додаткових ознак може бути якою завгодно.

Дії 4 – 9 в точності збігаються з відповідними діями технології, розглянутої вище.

Таким чином, запропонована технологія автентифікації виборців у відкритій системі ІГ, за рахунок доповнення системи сервером ДВП, у якому розміщені засоби розпізнавання осіб виборців за додатковими біологічними або іншими ознаками, дозволяє створити більш зручні умови для виборців, не вимагаючи від них проходження обов'язкової очної перевірки перед кожним голосуванням, що особливо доцільно у разі тривалих відряджень виборців.

4. Висновки

1. Запропоновано технологію дистанційної автентифікації виборців для відкритої системи таємного голосування в мережі Інтернет, яка надає можливість позбутися обов'язкової очної перевірки осіб виборців перед кожним актом волевиявлення, що особливо доцільно у разі тривалих відряджень виборців. При цьому збережено усі позитивні якості відкритої системи, включаючи повну контрольованість процесів на сервері Інтернет голосування в режимі реального часу, що усуває будь-які підстави для недовіри з боку виборців щодо збереження таємниці голосів або точності підрахунку.

2. Визначено найбільш доцільний період технологічного циклу виборчого процесу щодо дистанційної автентифікації осіб виборців з використанням біологічних (або інших) особистих ознак, а саме під час введення паролів для дистанційного голосування, що позбавляє можливості забороненої передачі свого права голосу іншій особі.

3. З метою захисту від будь-якого негативного впливу процесів, що пов'язані з автентифікацією, на роботу сервера Інтернет голосування, запропоновано для виконання цих процесів ввести окремий сервер дозволу введення пароля. При цьому між обома цими серверами для кожного сеансу обміну даними утворюється спеціальний захищений канал зв'язку, що дозволяє розміщувати їх незалежно один від одного в довільному місці мережі Інтернет.

4. Запропонована технологія надає можливість виборцям гнучкого вибору методів автентифікації, не позбавляючи їх можливості користуватись також і очною перевіркою. Обрання виборцями додаткових ознак для автентифікації залежить тільки від можливостей придбання ними тих чи інших засобів для введення обраних ознак.

Література: 1. 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. http://www.electronic-vote.org 3. Вишняков В.М., Пригара М.П., Воронін О.В. Відкрита система таємного голосування // Управління розвитком складних систем. 2014. Вип. 20. С. 110-115. 4. 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. 5. Чуприн В.М. Метод протидії незаконному впливу на виборців у системі Інтернет голосування / В.М. Чуприн, В.М. Вишняков, М.П. Пригара // Безпека інформації. – 2017. Т. 19, №1. С. 7-14. 6. https://github.com/vvk-ehk/evalimine 7. Брагина Е.К., Соколов С.С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития. // Вестник АГТУ. 2016. № 61. С. 40–45. 8. Daugman J.Information Theory and the Iris-Code. IEEE Trans. Info.Foren.Sec 11(2), 2015. – P. 400-409. 9. Тассов К. Л., Дятлов Р. А. Метод идентификации человека по голосу. Инженерный журнал: наука и инновации, 2013, Вып. 6. 10 с. 10. Матвеев Ю. Н . Технологии биометрической идентификации личности по голосу и другим модальностям // Вестник МГТУ им. Н. Э. Баумана. Сер. «Приборостроение». 2012. С. 46-61. 11. Назарук В.Д. Технології обміну даними дистанційних електронних виборів / В.Д. Назарук, О.А. Хоменчук // Захист інформації. 2016. Т. 18, №4. С. 10-15. 12. Постанова Центральної виборчої комісії від 25 вересня 2015 року № 370 «Про Роз'яснення щодо складання та уточнення списків виборців для підготовки і проведення голосування з місцевих виборів».

Transliterated bibliography:

1. 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. http://www.electronic-vote.org

3. *Vy`shnyakov V.M., Pry`gara M.P., Voronin O.V.* Vidkry`ta sy`stema tayemnogo golosuvannya // Upravlinnya rozvy`tkom skladny`x sy`stem. 2014. Vy`p. 20. S. 110-115.

4. *Chupry`n V.M.* Zaxy`st operacijnogo seredovy`shha sy`stem Internet golosuvannya / V.M. Chupry`n, V.M. Vy`shnyakov, M.P. Pry`gara // Zaxy`st informaciyi. 2017. T. 19, #1. S. 56-66.

5. *Chupry`n V.M.* Metod proty`diyi nezakonnomu vply`vu na vy`borciv u sy`stemi Internet golosuvannya / V.M. Chupry`n, V.M. Vy`shnyakov, M.P. Pry`gara // Bezpeka informaciyi. 2017. T. 19, #1. S. 7-14. 6. https://github.com/vvk-ehk/evalimine

7. *Bragina E.K., Sokolov S.S.* Sovremennye metody biometricheskoj autentifikacii: obzor, analiz i opredelenie perspektiv razvitija // Vestnik AGTU. 2016. № 61. S. 40–45.

8. *Daugman J.* Information Theory and the Iris-Code. IEEE Trans. Info.Foren.Sec 11(2), 2015. P. 400-409.

9. *Tassov K.L., Djatlov R.A.* Metod identifikacii cheloveka po golosu // Inzhenernyj zhurnal: nauka i innovacii. 2013, Vyp. 6. 10 c. DOI: 10.18698/2308-6033-2013-6-1103

10. *Matveev Ju.N.* Tehnologii biometricheskoj identifikacii lichnosti po golosu i drugim modal'nostjam // Vestnik MGTU im. N. Je. Baumana. Ser. «Priborostroenie». 2012. S. 46-61.

11. *Nazaruk V.D.* Texnologiyi obminu dany`my` dy`stancijny`x elektronny`x vy`boriv / V.D. Nazaruk, O.A. Xomenchuk // Zaxy`st informaciyi. 2016. T. 18, #4. S. 10-15.
12. *Postanova* Central`noyi vy`borchoyi komisiyi vid 25 veresnya 2015 roku # 370 «Pro Roz'yasnennya shhodo skladannya ta utochnennya spy`skiv vy`borciv dlya pidgotovky` i provedennya golosuvannya z miscevy`x vy`boriv».

Надійшла до редколегії 12.05.2018
Рецензент: д-р техн. наук, проф. Бараннік В.В.

Мачалін Ігор Олексійович, д-р техн. наук, проф., директор Навчально-наукового інституту Аеронавігації, електроніки та телекомунікацій Національного авіаційного університету, Наукові інтереси: експлуатація та проектування інформаційно-телекомунікаційних систем. Хобі: музика. Адреса: Україна, 03054, Київ, пр. Космонавта Комарова, 1,
e-mail: igor.machalin@ukr.net
Вишняков Володимир Михайлович, канд. техн. наук, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури. Наукові інтереси: захист інформації в комп'ютерних мережах, криптографія. Хобі: Інтернет. Адреса: Україна, 03037, Київ, пр. Повітрофлотський, 31,
e-mail: volodymyr.vyshniakov@gmail.com
Комарницький Олег Олександрович, головний спеціаліст, Департамент інформаційно-комунікаційних технологій Київської міської державної адміністрації. Наукові інтереси: Інтернет технології. Хобі: спорт. Адреса: Україна, 01044, Київ, Хрещатик, 36, e-mail: komarnitskiy2012@gmail.com
Machalin Igor Alekseevich, Dr. Sc. (Ing), Prof., Director of the Educational and Scientific Institute of Aeronavigation, Electronics and Telecommunications of the National Aviation University, Research interests: operation and design of information and telecommunication systems. Khobi: music. Address: Ukraine, 03054, Kyiv, Cosmonaut Komarov Ave., 1,
e-mail: igor.machalin@ukr.net
Vyshniakov Volodymyr Mykhailovych, PhD in engineering, associate professor, Department of Cyber Security and Computer Engineering, Kyiv National University of Construction and Architecture. Research interests: data protection. Khobi: Internet. Address: Ukraine, 03037, Kyiv, Povitroflotski Ave., 1,
e-mail: volodymyr.vyshniakov@gmail.com
Komarnitskiy Oleg Oleksandrovich, Chief Specialist, Department of Information and Communication Technologies of Kyiv City State Administration. Research interests: Internet technologes. Khobi: sport. Address: Ukraine, 01044, Kyiv, Xreshhaty`k., 36,
e-mail: komarnitskiy2012@gmail.com