DOI: 10.18372/2410-7840.19.11439
УДК 681.527.7:324

ТЕХНОЛОГІЇ ОБМІНУ ДАНИМИ ДИСТАНЦІЙНИХ ЕЛЕКТРОННИХ ВИБОРІВ

Віталій Назарук, Олександр Хоменчук

У статті досліджено системи електронних виборів, які можуть використовуватись у виборчих кампаніях різного рівня. Визначено їх основні переваги та розглянуто проблеми, які виникають під час впровадження систем електронних дистанційних виборів. Встановлено, що такі системи одночасно повинні забезпечувати таємницю голосування та однозначну дистанційну ідентифікацію особистості уповноважених виборців, що виконати за допомогою існуючих протоколів обміну інформації є складною задачею. У статті запропоновано технологію обміну даними, яка передбачає: надсилання до центральної виборчої комісії бюлетенів із позначками вибору без прив'язки їх до ідентифікаторів виборців; запобігання перехопленню та модифікації даних завдяки застосуванню протоколів асиметричного шифрування; використання генераторів випадкових послідовностей для знеособлення бюлетенів при підрахунку голосів; можливість оскарження результатів свого голосування конкретним виборцем.

Ключові слова: *бюлетень, електронний цифровий підпис, автентифікація, відкритий ключ, закритий ключ.*

Актуальність теми. Існуючі системи виборів поступово втрачають довіру суспільства, що, в результаті призводить до зменшення кількості голосуючих і, як наслідок, до зміщення результатів виборів до підсумків голосування незначної частини уповноважених виборців. Крім того, наявність людського фактору при підрахунку результатів виборів надає можливість застосуванню різноманітних способів шахрайства та фальсифікацій. Тому впровадження у виборчий процес технологій, які б мінімізували зовнішнє втручання, є нагальним запитом суспільства.

Апробація існуючих виборчих інформаційних технологій, яка проводиться окремими державами, демонструє недосконаліть впроваджених засобів захисту. В результаті злому таких систем можлива реалізація наступних загроз: підміна надісланих для підрахунку бюлетенів іншими; модифікація отриманих для підрахунку бюлетенів; генерація великої кількості віртуальних виборців і вкидання їх бюлетенів на користь необхідного кандидата; розсекречення таємниці вибору конкретної особи. Слід враховувати також можливість продажу своїх голосів окремими індивідами та групами населення. Для запобігання реалізації зазначених загроз необхідні технології обміну даними, які б унеможливлювали зовнішнє та внутрішнє втручання в електронну систему виборів.

Мета статті. Огляд існуючих систем електронних дистанційних виборів та розробка безпечних технологій обміну даними між терміналами виборців та серверами виборчих комісій, які повинні забезпечувати таємницю голосування, дотримуючись при цьому принципу однозначної автентифікації уповноважених виборців.

Вступ. Використання сучасних інформаційних технологій у сфері державотворення, в тому числі систем дистанційних електронних виборів є пріоритетом у провідних країнах світу. Завдяки таким системам можливо знизити тиск на виборця і підвищити достовірність виборів, уникнути модифікації бюлетенів з позначками вибору та результатів підрахунку голосів.

Водночас впровадити повноцінні електронні вибори жодній державі поки що не вдалось. Це обумовлено вразливістю наявних систем до кібератак. Можливість застосування методів злому та модифікації в таких системах надають наступні взаємовиключні фактори. Перш за все виборчий процес повинен гарантувати таємницю голосування, дотримуючись при цьому принципу однозначної автентифікації уповноважених виборців. По-друге, програмне забезпечення має створюватись якомога простішими і доступнішими засобами для проведення відкритої експертизи та отримання довіри суспільства, що знижує його захищеність від зовнішнього втручання. По-третє, серверне обладнання повинно мати відкритий доступ для зовнішніх користувачів і, разом з тим, бути максимально захищеним від мережевих атак.

Матеріали даної статті присвячено дослідженням можливих шляхів вирішення проблеми першого фактору.

Аналіз останніх досліджень і публікацій. У статті Д. Джефферсона (Ліверморська національна лабораторія) [1] надано детальний аналіз потеційних загроз інформаційним ресурсам в ході проведення онлайн-виборів. Порівняння проводиться з онлайн-банкінгом, і визначається принципова різниця концепцій двох систем. У виборчому процесі кожен конкретний виборець знає, як він проголосував, але він не має повноважень на зберігання доказів свого вибору і не має права це

довести. В онлайн-банкінгу та онлайн-шопінгу кожна транзакція повинна бути відкритою для двох сторін і підтверджуватись відповідним документом, який може бути доказом при виникненні спірних питань чи шахрайства.

Масштаби наслідків недотримання вимог захисту інформації в інформаційно-телекомунікаційних системах також різні. Якщо збитки від реалізованих загроз в інтернет-банкінгу можуть вимірюватись десятками тисяч доларів, то в інтернет-виборах ці суми можуть сягнути мільярдів доларів і призвести до зміни геополітичного устрою.

П. Биргер в [2] подає інформацію про результати практичного застосування систем електронних виборів в Естонії, Великобританії, США, Швейцарії, Канаді та застерігає про недосконалість існуючих систем. Для прикладу приведено виборчу систему «Digital Vote by Mail», що проходила випробовування в окрузі Колумбія, і вразливість якої довела група аналітиків Мічиганського університету.

Ряд езотеричних протоколів запропоновано Брюсом Шнайєром в [3]. До таких належать: спрощений протокол голосування з асиметричним шифруванням; спрощений протокол голосування з асиметричним шифруванням та електронним цифровим підписом; голосування із сліпими підписами; голосування з двома виборчими комісіями; голосування з однією центральною комісією; покращене голосування з центральною виборчою комісією, голосування без виборчої комісії. Зазначені протоколи потребують розробки інформаційних технологій для їх практичної реалізації.

У [4] пропонується для захисту обміну даними в інформаційно-телекомунікаційних системах на ділянці «термінал виборця – сервер виборчої комісії» застосування симетричного шифру Вернама. Такий криптоалгоритм працює за принципом одноразового блокнота і при виконанні встановлених вимог не підлягає розшифруванню.

Важливою складовою процесу шифрування є забезпечення криптоалгоритму випадковими послідовностями. В статті [5] роозроблено механізм отримання випадкових чисел, що базується на використанні обох кварцових резонаторів, що є складовими елементами будь-якого комп'ютеризованого пристрою, у поєднанні з фізичним процесом обробки зовнішніх запитів засобами операційної системи, що надходять із мережі Інтернет.

Виклад основного матеріалу. Застосування надійних та об'єктивних засобів голосування і захисту їх результатів були предметом неодноразового обговорення на міжнародному та європейському рівнях, що викладене зокрема у ряді доповідей Європейської комісії за Демократію через Право (Венеціанська Комісія) (European Commission for Democracy through Law – Venice Commission), присвячених проблемам відповідності віддаленого голосування (голосування поштою або електронне голосування) стандартам Ради Європи.

У доповіді від 13 березня 2004 року Венеціанська Комісія попередила про необхідність вжиття додаткових заходів для мінімізації ризиків фальсифікацій та визначила 5 принципів, що відображають засади європейської демократії та однаково придатні як для виборчих кампаній, так і для референдумів:

– Універсальне право голосу: всі люди мають право голосу.

– Рівні права голосу: кожен виборець має рівну кількість голосів.

– Свобода права голосу.

– Таємність права голосу.

– Пряме право голосу.

Зважаючи на це, Венеціанська Комісія рекомендувала наступне: електронне голосування може використовуватися лише за умови, що:

– система є безпечною/захищеною і надійною;

– система електронного голосування повинна бути прозорою, тобто надавати можливість перевірки щодо її функціонування;

– виборці повинні мати нагоду одержати підтвердження свого вибору і виправити його у разі допущення помилки;

– для полегшення перерахунку голосів у разі конфліктної ситуації може передбачатися процедура роздрукування голосів [6, 7].

Комп'ютерне голосування може бути застосовано у виборах лише в тому випадку, коли появляться комунікаційні протоколи, які одночасно задовольнятимуть виконання вищеназваних вимог. Такі протоколи повинні захищати таємницю особистості і запобігати шахрайству [3].

Розглянемо ті з них, які мають практичне застосування.

1. Голосування із сліпими підписами. Необхідно відділити бюлетень від голосуючого, зберігши процедуру ідентифікації особистості. Саме це можна здійснити за допомогою протоколу сліпого підпису.

1.1. Кожен виборець створює 10 наборів повідомлень, кожен набір містить правильний бюлетень для кожного можливого результату голосування (наприклад, якщо бюлетенем є одна з відповідей «так»-«ні», то кожен набір складається з двох

бюлетенів, одного для «так», а іншого для «ні»). Кожне повідомлення включає також випадковим чином створений ідентифікаційний номер, достатньо великий, щоб виключити плутанини з іншими виборцями.

1.2. Кожен виборець особисто маскує всі повідомлення і надсилає в Центральну виборчу комісію (ЦВК) разом з маскуючими множниками.

1.3. ЦВК по своїй базі перевіряє, що користувач не надсилав раніше для підпису свої замасковані бюлетені. Потім вона індивідуально підписує кожне повідомлення набору і надсилає їх назад виборцю, зберігши ім'я виборця в своїй базі даних.

1.4. Виборець знімає маскування з повідомлень і отримує набір бюлетенів, підписаних ЦВК. Ці бюлетені підписані, але не зашифровані, тому виборець легко побачить, який бюлетень – «так», а який – «ні».

1.5. Кожен виборець вибирає один з бюлетенів і шифрує його відкритим ключем ЦВК.

1.6. Виборець відправляє свій бюлетень.

1.7. ЦВК розшифровує бюлетені, перевіряє підписи, перевіряє по базі даних унікальність ідентифікаційного номера, зберігає останній номер і підводить підсумки. Вона публікує результати голосування разом з кожним наступним номером і відповідним бюлетенем.

Зловмисник не може обманути цю систему. Протокол сліпого підпису забезпечує автентичність його бюлетенів. Якщо він спробує відправити той самий бюлетень двічі, ЦВК виявить дублювання номерів на етапі 1.7 і не буде враховувати другий бюлетень. Якщо він спробує отримати декілька бюлетенів на етапі 1.2, ЦВК виявить це на етапі 1.3. Виборець не може створювати свої власні бюлетені, тому що він не знає закритого ключа комісії. З тієї ж причини він не може перехватити та змінити чужі бюлетені.

Протокол «Розрізати і вибирати» на етапі 1.3 повинен забезпечувати унікальність бюлетенів. Без цього зловмисник міг би створити такий же (за виключенням ідентифікаційного номера) набір бюлетенів і завірити їх всі в ЦВК.

ЦВК не може дізнатися, як голосував конкретний виборець. Враховуючи те, що протокол сліпих підписів маскує номери бюлетенів до моменту підведення підсумків, ЦВК не може встановити зв'язок між підписаним нею замаскованим бюлетенем і підсумковим бюлетенем. Опублікування переліків номерів і зв'язаних з ними бюлетенів дозволяє виборцям переконатись в тому, що їх бюлетені враховані правильно.

Проте проблеми все-таки залишаються. Якщо етап 1.6 є не анонімним, ЦВК може записати, хто який бюлетень надіслав, і взнати, хто за кого голосував. Це неможливо, коли комісія отримує бюлетені в опечатаній урні та рахує їх пізніше. Хоча ЦВК і не зможе встановити зв'язок між виборцями та їх бюлетенями, вона зможе створити велику кількість підписаних і правильних бюлетенів та зшахраювати, надіславши їх сама собі [3].

2. Голосування з двома ЦВК.

Одним з рішень є варіант поділу ЦВК наполовину. У жодної з них не буде достатньої влади, щоб зшахраювати на свій розсуд. В такому протоколі використовується центральне управління реєстрації (ЦУР), яке займається перевіркою користувачів, та окрема ЦВК для підрахунку голосів.

2.1. Кожен виборець відправляє лист в ЦУР із запитом на реєстраційний номер.

2.2. ЦУР повертає виборцю випадковий реєстраційний номер на випадок, якщо хтось спробує проголосувати двічі.

2.3. ЦУР відправляє список реєстраційних номерів в ЦВК.

2.4. Кожен виборець вибирає випадковий ідентифікаційний номер. Він створює повідомлення з цим номером, реєстраційним номером, отриманим в ЦУР, та своїм бюлетенем. Він посилає своє повідомлення в ЦВК.

2.5. ЦВК перевіряє реєстраційні номери по списку, отриманому від ЦУР на етапі 1.3. Якщо реєстраційний номер є в списку, ЦВК викреслює його, щоб запобігти повторному голосуванню. ЦВК додає ідентифікаційний номер до списку тих, хто проголосував за певного кандидата, і додає одиничку до відповідного підсумкового числа.

2.6. Після того, коли всі бюлетені будуть отримані, ЦВК публікує результати разом із списками, які містять ідентифікаційні номери і відповідні бюлетені.

Як і в попередньому протоколі кожен виборець може побачити список ідентифікаційних номерів і знайти в ньому свій власний. Так він може переконатись, що його бюлетень враховано. Звичайно, всі повідомлення, якими обмінюються учасники протоколу, повинні бути зашифровані і підписані, щоб завадити зловмиснику видати себе за іншого, або перехопити повідомлення.

ЦВК не може змінити бюлетені, тому що кожен виборець буде шукати свій реєстраційний номер. Якщо виборець не знаходить свій реєстраційний номер або знаходить його в підсумковому списку з іншими результатами голосування, він негайно взнає, що відбувся обман. ЦВК не може добавити бюлетені, оскільки «урна» знаходиться під контролем ЦУР. ЦУР знає, скільки виборців зареєструвалось, їх реєстраційні номери, і виявить будь-які зміни.

Зловмисник може спробувати зшахраювати, вгадавши правильний реєстраційний номер. Ця загроза може бути мінімізована, якщо множина можливих реєстраційних номерів набагато більша, ніж множина реальних реєстраційних номерів: 100-бітове число для мільйона виборців. Звичайно, реєстраційні номери повинні генеруватись випадковим чином.

Незважаючи на це, ЦУР повинна бути органом влади, який заслуговує довіри, адже вона може зареєструвати неправомочних виборців. Вона може також зареєструвати правомочних виборців декілька разів. Цей ризик може бути зведеним до мінімуму, якщо ЦУР опублікує список зареєстрованих виборців (але без їх реєстраційних номерів). Якщо число виборців у цьому списку менше, ніж число підрахованих бюлетенів, значить щось не так. Проте якщо зареєструвалось більше виборців, ніж було надіслано бюлетенів, то це, можливо, означає, що ряд зареєстрованих виборців не проголосував.

Цей протокол беззахисний перед змовою ЦВК і ЦУР. Якщо вони діють разом, то можуть об'єднати свої бази даних і взнати, хто за кого голосував [3].

Наявні на даний час технології обробки та захисту інформації дозволяють здійснювати розробку та верифікацію перспективних протоколів з використанням алгоритмів асиметричного шифрування та електронного цифрового підпису [8].

3. Для мінімізації впливу дестабілізуючих факторів на виборчий процес доцільно організувати за 2-рівневою структурою електронного голосування, яка зображена на рисунку 1.

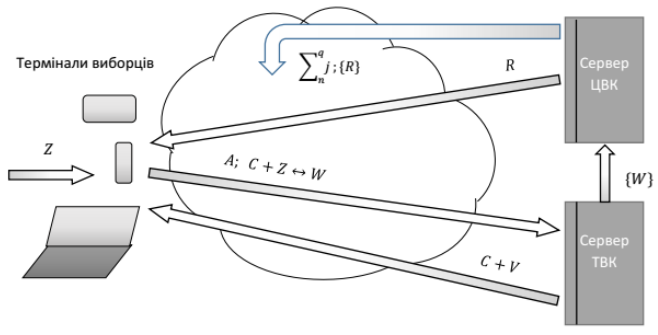

Рис. 1. Технологія побудови комунікаційних протоколів

1 рівень – Територіальної виборчої комісії (ТВК);

2 рівень – Центральної виборчої комісії (ЦВК).

Побудову протоколів обробки та обміну інформації пропонується здійснюватися за наступною технологією.

3.1. Публікація ЦВК програмного забезпечення «Вибори» та відкритого ключа k.

3.2. Реєстрація виборця в ТВК для Е-голосування з відмовою від паперового варіанта.

3.3. Отримання виборцем електронного цифрового підпису (ЕЦП) Z.

3.4. Автентифікація A виборця в ТВК та отримання ним бюлетеня V для голосування та супровідного листа C.

3.5. Прикріплення до бюлетеня n-значного коду R, вибраного за допомогою генератора випадкових чисел та збереження цього коду до закінчення процесу виборів. Для побудови генератора випадкових чисел доцільно використовувати технологію, представлену в статті [5].

3.6. Фіксація позначки в бюлетені відповідно до здійсненого вибору -Vr.

3.7. Шифрування S бюлетеня з позначкою вибору Vr відкритим ключем k: $W = S\ Vr(k)$. Вибір криптоалгоритму асиметричного шифрування, на відміну від запропонованого в [4] симетричного, обумовлений тим, що для останнього практично неможливе дотримання вимог зберігання та розповсюдження секретних ключів в інформаційно-телекомунікаційних системах, які використовуються для проведення електронних виборів із застосуванням інтернет-технологій.

3.8. Накладення ЕЦП Z на супровідний лист C: $C+Z$. Електронний цифровий підпис отримується виборцем в акредитованих центрах сертифікації ключів і може використовуватись також в інших цілях, не пов'язаних з виборами.

3.9. Прикріплення шифрованого бюлетеня W до супровідного листа C з ЕЦП Z: $C+Z \leftrightarrow W$. Цей етап забезпечує нерозривний зв'язок файла підписаного супровідного листа з файлом зашифрованого бюлетеня з позначкою вибору. Супровідний лист необхідний для того, щоб по накладеному на нього ЕЦП однозначно ідентифікувати особу виборця. Якщо ж особу виборця ідентифікувати по бюлетеню W, то таємниця голосування розкривається.

3.10. Відправка підписаного супровідного листа $C+Z$ із зашифрованим бюлетенем W в ТВК.

3.11. Накопичення в буфері ТВК супровідних листів з бюлетенями $C+Z \leftrightarrow W$ від m виборців на час можливого відкату T.

3.12. Повторне голосування у разі зміни виборцем рішення стосовно свого вибору за процедурою 4-11 впродовж часу T з видаленням попередніх результатів $C+Z \leftrightarrow W$.

3.13. Заборона ТВК повторного голосування виборцям, які проголосували за час T.

3.14. Копіювання сервером ТВК зашифрованих бюлетенів *W*, прикріплених до супровідних листів *C+Z* та збереження їх окремими файлами.

3.15. Передача послідовності зашифрованих бюлетенів {*W*} за час *T* до ЦВК. Файли із супровідними листами та зашифрованими бюлетенями із сервера ТВК видаляються (знищуються) в період від закінчення процесу голосування до оголошення результатів виборів. Процедури 13 – 14 потребують окремого детального опису технології копіювання та передачі послідовності зашифрованих бюлетенів, яка повинна передбачати запобіганню підміни бюлетенів, надісланих виборцями. Моніторинг журналу подій має здійснюватися незалежними адміністраторами безпеки та експертами.

3.16. Накладення на зашифровані бюлетені *W* секретного ключа ЦВК *d*.

3.17. Підрахунок результатів голосування $\sum_n^q j$, де *n* – кількість кандидатів, *q* – номер кандидата, *j* – кількість виборців, які за нього проголосували за час *T*. Підрахунок голосів потребує тих же заходів безпеки та моніторингу, що і процедури 13 – 14.

3.18. Публікація підсумків голосування за час *T*.

3.19. Публікація послідовності кодів бюлетенів {*R*}, які брали участь у голосуванні.

3.20. Звірка виборцем збереженого коду *R* бюлетеня *Vr* з опублікованими кодами бюлетенів, які взяли участь у голосуванні. При встановленні виборцем відсутності серед опублікованих кодів збереженого ним, він матиме право оскаржити особистий результат волевиявлення.

Висновки.

Запропонована технологія обміну даними дозволяє забезпечити наступні вимоги, які ставляться до виборчих систем:

– однозначна автентифікація виборця за рахунок пред'явлення сертифікованого автентифікатора;

– виключення можливості надсилання до ТВК, і, як наслідок, до ЦВК більш ніж одного бюлетеня від одного автентифікованого виборця, а також більшої кількості бюлетенів, ніж кількість виборців, які зареєструвались для електронного голосування;

– неможливість перехопити та модифікувати відправлений виборцем бюлетень завдяки застосуванню протоколів асиметричного шифрування;

– забезпечення таємниці голосування шляхом відділення бюлетеня з позначкою вибору від супровідного листа з електронним цифровим підписом автентифікованого виборця;

– можливість оскарження результатів виборів по кожному конкретному виборцю у разі відсутності в кодах, опублікованих ЦВК, коду, отриманого виборцем.

Для практичної реалізації розглянутої технології необхідна розробка протоколів обміну інформацією з детальним описом та ґрунтовним аналізом кожного етапу процесу. Програмне забезпечення повинно бути представлене на експертизу щодо відповідності вимогам з технічного захисту інформації.

Подальших досліджень потребують також додаткові методи захисту серверів ТВК та ЦВК від мережевих атак.

ЛІТЕРАТУРА

[1]. Jefferson D. If I Can Shop and Bank Online, Why Can't I Vote Online? [Electronic resource] Access mode: World Wide Web. – URL: https://www. verifiedvoting. org/resources/ internet-voting/vote-online/.

[2]. Биргер П. Электронные выборы: как интернет помогает волеизъявлению [Електронний ресурс] Режим доступу: World Wide Web. – URL: https:// republic.ru/future/elektronnye_vybory_kak_tekhnologii_pomogayut_chestnomu_voeizyavleniyu-722030. xhtml? page=4#pager.

[3]. Шнайер Б. Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке Си. – Москва: Триумф, 2002. – С. 94-100.
Вишняков В. М., Пригара М. П., Воронін О. В. Відкрита система таємного голосування // Управління розвитком складних систем. Збірник наукових праць. – 2014. – Вип. 20. – С. 110-115. [Електронний ресурс] Режим доступу: World Wide Web. – URL: http://urss. knuba.edu.ua/ files/zbirnyk-20/ 22.pdf.

[4]. Чуприн В. М., Вишняков В. М., Пригара М. П. Генерування випадкових чисел штатними засобами хостів мережі інтернет//Захист інфомації. Науковий фаховий журнал. – 2016. – Том 18. – № 4. – С. 323-335. [Електронний ресурс] Режим доступу: World Wide Web. – URL: http: // jrnl. nau. edu. ua / index.php / ZI / article / view/ 11085 / 14800.

[5]. Савчук О. Системи електронних виборів процедури голосування та матеріально- технічні засоби. Міжнародний досвід. [Електронний ресурс] Режим доступу: World Wide Web. – URL: http://euinfocenter. rada.gov.ua/uploads/documents/ 28966.pdf.

[6]. Панцир С., Когут А. Е-демократія в Україні: рекомендації щодо впровадження політики та забезпечення її результативності. [Електронний ресурс] Режим доступу: World Wide Web. – URL: http://euinfocenter. rada.gov.ua/uploads/documents/28784.pdf.

[7]. Назарук В. Д., Хоменчук О..А., Круліковський Б. Б. Інформаційна технологія побудови комунікаційних протоколів дистанційних електронних виборів //

Матеріали конференції "Інформаційно-обчислювальні технології, автоматика та електротехніка". – Рівне, 2016. – С. 309-312.

REFERENCES

[1]. Jefferson D. If I Can Shop and Bank Online, Why Can't I Vote Online? [Electronic resource] Access mode: World Wide Web. – URL: https://www. verifiedvoting. org/resources/ internet-voting/vote-online/.

[2]. Byrger P. Electronic elections: how the Internet helps consent [Electronic resource] Access mode: World Wide Web. – URL: https:// republic. ru / future / elektronnye_vybory_kak_tekhnologii_pomogayut_chestnomu_voeizyavleniyu-722030.xhtml?page=4# pager.

[3]. Schneier B. Applied Cryptography. 2 edition. Protocols, algorithms and source code in the language of Си. – Moscow: Triumph, 2002. – P. 94-100.

[4]. Vyshniakov V. M., Prygara M. P., Voronin O. V. Opensecret ballot system, Managing the development ofcomplexsystems, vol. 20, P. 110-115. [Electronic resource] Access mode: World Wide Web. – URL: http:// urss. knuba. edu. ua / files / zbirnyk-20 / 22. pdf.

[5]. Chupryn V. M., Vyshniakov V. M., Prygara M. P. Method of generation casual numbers on the basis of the use of apparatus of the computer plugged in the internet. Ukrainian Information Security Research Journal, vol 18, № 4 (2016), P. 323-335. [Electronic resource] Access mode: World Wide Web. – URL: http://jrnl. nau.edu.ua/index.php/ZI/article/view/11085/14800.

[6]. Savtchuk O. Systems electronic voting: procedures, material and technical means. International experience. [Electronic resource] Access mode: World Wide Web. – URL: http: // euinfocenter. rada. gov. ua / uploads / documents / 28966. pdf.

[7]. Panzyr S., Kogut A. E-Democracy in Ukraine: Recommendations for implementing policy and its effectiveness. [Electronic resource] Access mode: World Wide Web. – URL: http: // euinfocenter. rada. gov. ua / uploads / documents / 28784. pdf.

[8]. Nazaruk V.D., Khomenchuk O.A., Krulikovskiy B.B. Information technology of remote electronic communication protocols elections // Conference materials "Information and computer-oriented technologies, automation and electrical engineering." – Rivne, 2016. – P. 309-312.

ТЕХНОЛОГИИ ОБМЕНА ДАННЫМИ ДИСТАНЦИОННЫХ ЭЛЕКТРОННЫХ ВЫБОРОВ

В статье исследованы системы электронных выборов, которые могут использоваться в избирательных кампаниях различного уровня. Определены их основные преимущества и рассмотрены проблемы, возникающие при внедрении систем электронных дистанционных выборов. Установлено, что такие системы одновременно должны обеспечивать тайну голосования и однозначную дистанционную идентификацию личности уполномоченных избирателей, выполнить которые с помощью существующих протоколов обмена информации является сложной задачей. В статье предложена технология обмена данными, которая предусматривает: отправку в Центральную избирательную комиссию бюллетеней с отметками выбора без привязки их к идентификаторам избирателей; предотвращение перехвата и модификации данных благодаря применению протоколов асимметричного шифрования; использование генераторов случайных последовательностей для обезличивания бюллетеней при подсчете голосов; возможность обжалования результатов своего голосования конкретным избирателем.

Ключевые слова: бюллетень, электронная цифровая подпись, аутентификация, открытый ключ, закрытый ключ.

DISTANCE COMMUNICATION TECHNOLOGY ELECTRONIC ELECTIONS

Electronic voting systems, which can be used in election campaigns of a different level, are examined in the article. Their main benefits are determined, and problems, that appear when implementing remote electronic voting systems, are contemplated. It is found that such systems at the same time are supposed to ensure vote secrecy and unambiguous remote person identification of authorized voters; and all that is difficult to perform with the help of existing information exchange protocols. Data exchange technology, that considers: sending to a central election committee ballots with signs of an option without binding them to voters identifications, is offered in the article; prevent data interception and modification through the use asymmetric encryption protocols; use generator of random sequences for depersonalization ballots during the vote count; to appeal election your results to specific voter.

Keywords: ballot, electronic digital signature, authentication, public key, private key.

Назарук Віталій Дмитрович, кандидат технічних наук, старший викладач кафедри обчислювальної техніки (Національний університет водного господарства та природокористування).
E-mail: v.d.nazaruk@nuwm.edu.ua

Назарук Виталий Дмитриевич, кандидат технических наук, старший преподаватель кафедры вычислительной техники (Национальный университет водного хозяйства и природопользования).

Nazaruk Vitaly, candidate of technical sciences, senior lecturer in Computer Engineering (National university of water and environmental engineering).

Хоменчук Олександр Анатолійович, начальник відділу інформаційних технологій (Національний університет водного господарства та природокористування).
E-mail: khomenchuk@nuwm.edu.ua

Хоменчук Александр Анатольевич, начальник отдела информационных технологий (Национальный университет водного хозяйства и природопользования.

Khomenchuk Alexander, head of information technology (National university of water and environmental engineering).