

Забезпечення прозорості та відкритості виборчого процесу та процесу голосування в контексті запровадження новітніх технологій



Юрій КЛЮЧКОВСЬКИЙ,
президент Всеукраїнської
громадської організації
«Інститут виборчого права»

Починаючи розмову про високі технології, про їх застосування у виборчому процесі, цікаво принагідно згадати, коли вперше виникла сама ідея використання комп'ютера у виборах? Я переконаний, що абсолютна більшість аудиторії цього не знає. Бо ідея належить відомому американському фантасту Айзеку Азімову, який написав серію новел про суперкомп'ютер під назвою «Мультивак», одна з яких називається «Елекшен дей». За сюжетом для того, щоб провести вибори президента, комп'ютер обирає одного середнього американця. І цей один американець, голосуючи, обирає президента. Прекрасний спосіб застосування комп'ютерної технології, чи не так? Адже комп'ютер об'єктивний, на перший погляд. Питання тільки в тому, які критерії «середньості»

американця закладені в його програмі, за якими ознаками він обирає того середнього американця. Бо якщо ви зміните ці ознаки, то зміняться й результати виборів. А це означає, що так чи інакше, коли ми застосуємо комп'ютерні технології, то виникає дуже багато запитань, насамперед до того, хто писав програму, що в ній закладено і чи немає там різноманітних пасток? А хто це може перевірити, не відомо.

Виникає дуже багато запитань і щодо безпеки. На мою думку, у разі будь-якої катастрофи, досить імовірної в наших умовах, нам все одно потрібні паперові протоколи. То навіщо від них відмовлятися, якщо вони все одно мають бути? І плюс новітні технології. Тому тут є дуже багато речей, на які треба звернути увагу. Однак мені здається, що все одно треба виходити з певних загальних засад. Якими, безперечно, є міжнародні принципи і стандарти виборчого права, серед них – надзвичайно важливий стандарт чесних виборів, а в Кодексі належної практики у виборчих справах Венеціанської комісії він має вигляд процедурних гарантій дотримання всіх принципів виборчого права. І серед цих гарантій є дві, які я вважаю ключовими. Перша – це ефективна система спостереження і таким чином забезпечення максимальної прозорості всіх без винятку етапів виборчого процесу, в тому числі підрахунку голосів і передачі результатів. Друга – ефективна сис-

тема оскарження будь-яких правопорушень на будь-якій стадії.

Отже, по-перше, система має бути такою, щоб було видно всі правопорушення, і щоб була можливість їх оскаржити.

З огляду на це перше, що викликало занепокоєння, це питання складання е-протоколу на виборчій дільниці після підрахунку бюлетенів. Справа в тому, що закон передбачає дещо інший підхід. Протокол про підрахунок голосів складається поступово у процесі такого підрахунку і основна ідея полягає в тому, що коли встановлено один показник, його зафіксують і вже більше не можуть змінити. А потім переходять до встановлення іншого показника, наступного по черзі. Таким чином, щоб повернутися і підправити цифри вже ніхто не зміг. Відтак протокол складається у процесі підрахунку голосів, а не після його завершення. Кажуть, це можна зробити, вносячи дані у комп'ютер. Наприклад, ноутбук або інший маленький пристрій з маленьким екраном. А у мене виникає запитання – хто бачитиме, що вноситься в комп'ютер, крім тієї особи, яка це робитиме? Як можна спостерігати за цим процесом, яка його прозорість? Скажіть, ви пробували дивитися на екран ноутбука збоку? Хіба там щось видно, якщо він рідкокристалічний? Нічого! Тому, природно, виникає ще одне запитання – де гарантії, що вноситься в комп'ютер будуть ті цифри, які були встановлені? Чим об-

грунтовані мої підозри? Колеги з ЦВК знають принаймні випадки на виборах 2012 року, як деяких системних адміністраторів з ОВК ловили за руку, коли вони вносили в систему недостовірні дані з протоколів. Завідомо сфальсифіковані і не ті, які були в протоколах ДВК. Тобто така загроза є.

Наступна ідея полягає в тому, щоб вилучити ОВК з процесу встановлення результатів голосів. Пропозиція, мабуть, була б слушною, якщо б не виникало просте запитання: чи зможе ЦВК без попередньої перевірки на рівні округу впоратися з тридцятьма п'ятьма тисячами протоколів ДВК? Сьогодні ці протоколи перевіряються ОВК і вважається, що саме ОВК робить попередню перевірку, узагальнюючи дані в межах округу. І при цьому залишаються відомості з окремих дільниць, а це, на мою думку, підвищує надійність. Фахівці теорії добре знають, що таке завадостійкість системи. Так от, вона визначається кількістю збереженої на носіях інформації: чим більший її надлишковий обсяг, тим більша завадостійкість всієї системи і тим складніше зіпсувати відомості. Саме тому сьогодні передбачається передача в протоколі ОВК не тільки підсумкових відомостей в межах області, а й з кожної дільниці окремо.

Однак, а ми знаємо також, що сьогодні ОВК вже складає е-протокол згідно з чиним законом і з постановами ЦВК, проте в Комісії не узагальнюють відомості з виборчих дільниць, це робить програма ІАС «Вибори», якою керує не член виборчої комісії, а системний адміністратор, оператор терміналу в ОВК. І члени ОВК підпису-

ють складений таким способом е-протокол, не перевіряючи цих даних. Тут знову виникає запитання, а чи не впорядкувати хоча би постановою ЦВК процедуру діяльності окружних комісій? Бо процедура дійсно ніким не встановлена і різні ОВК діють на свій розсуд. Як на мене, це значно дешевше, ніж купувати складне обладнання.

Можна запроваджувати багато змін, можна і треба позбуватися процедури уточнення протоколів, їх повернення назад. Це дійсно джерело багатьох зловживань, але їх можна завбачити.

І третє, на що я хочу звернути увагу, як ЦВК перевірить достовірність е-протоколів, які до неї надійдуть за цією новою е-системою передачі даних? Адже інших джерел, крім цих е-протоколів у Комісії не буде. Таким чином, вона автоматично покладатиметься тільки на електронні протоколи.

Тоді виникає запитання: а якими каналами зв'язку передаються ці дані? Ми знаємо, хто володіє всеукраїнською дротовою мережею передачі даних – Укртелеком. Це приватна компанія. І ми приватній компанії доручаємо передачу даних щодо встановлення результатів виборів всеукраїнської влади?! А про мобільний зв'язок взагалі не йдеться! Останні події в Україні не раз засвідчили, що не можна користуватися мобільним зв'язком при передачі закритих даних.

Виникає ще одне запитання: а що можна оскаржити, що можна побачити спостерігачеві, якщо він підозрює, що були правопорушення, чи були фальсифікації, і результати виборів не відповідають результатам волевияв-

лення громадян. Чи можна буде що-небудь побачити? Звісно, ні. І знов-таки в теорії інформації така система називається «чорний ящик». Коли є щось на вході і щось на виході, а що відбувається всередині, не відомо. Кажуть, все підлягає перевірці, мовляв можна порахувати систему кодів, можна подивитися на програмне забезпечення. А хто дивитиметься, хто буде цей хтось, хто рахуватиме? І з яких підстав, і в яких випадках? Чи це зробить спостерігач, чи довірена особа партії? Вони матимуть можливість це зробити, адже доступ до програмного забезпечення теж має бути достатньо захищений і авжеж будь-хто не повинен цього робити. Відтак оскаржувати нічого і нікому, бо нам доведеться вірити в ці встановлені «чорним ящиком» результати.

І останнє, що я хотів сказати. Тут була названа сума в півмільярда гривень, скільки коштує ця система. Знаєте, мені не віриться, і з дуже простої причини. Кілька років тому ми встановлювали на всі виборчі дільниці відеокамери. Відеокамера це значно дешевше, ніж принтер, модем, сканер і комп'ютер. Ця система камер на всі дільниці коштувала мільярд гривень. Щоправда, туди входило і обслуговування, і програмне забезпечення. А хіба тут цього не буде? І тому сума в півмільярда занижена, я думаю, разів у 5. І тоді виникає запитання, а хто буде бенефіціантом цих грошей? Як тільки ми отримаємо на це відповідь, то зрозуміємо, хто лобюватиме цю систему і для чого вона потрібна – для чесних виборів чи для нових корупційних схем.

А повертаючись до питання довіри, колеги, хочу нагадати – довіра не включається. Її можна

тільки виключити. Втрата довіри стається миттєво. А здобуття довіри відбувається лише поступово і тривалий час. Тому давайте ми спочатку забезпечимо прозорість і чесність наших виборів у межах теперішніх паперових техноло-

гій. Так, щоб ніхто не сумнівався, що переміг дійсно достойний, щоб у нас закінчилися «206-і» округи, які здобули в наших умовах після Революції Гідності сумну славу. І от коли ми досягнемо довіри до організаторів виборів,

якщо ми зрозуміємо, що у нас влада така, яка не зацікавлена в якихось конкретних результатах виборів і не втручається в них, тоді й будемо спрощувати собі життя за допомогою дорогих ІТ-технологій. Дякую.



Ольга АЙВАЗОВСЬКА,
голова правління Всеукраїнської
організації «Громадянська
мережа «ОПОРА»

На мою думку, ця дискусія є вкрай корисною, але ми не пройшли батьох дуже важливих етапів, без яких не можемо дати сто відсоткової відповіді.

Перше – це питання оцінки ризиків, які не є загальними, а особливими суто в українських реаліях і можуть бути оцінені тільки спеціалістами, наприклад, під час хакатонів або іншого зразка зустрічей, мозкових штурмів, спорів між генераторами та критиками окремих ідей, і, безумовно, з обов'язковим вивченням правового поля.

Відомо, що на старті запровадження будь-якої ідеї робляться краш-тести – для того, щоб іще до початку втілення глобальної програми змін мати відповідь на

більшість технічних запитань, оскільки людині доведеться довіряти, з одного боку, програмі і машині, а з іншого – припускати, що може знайтися набагато досвідченіша і розумніша особа, в якій зовсім інші завдання щодо застосування таких програм і систем. Припускати, що Україна є другою Силіконовою долиною і зможе подолати будь-які ризики чи виклики, погодьтеся, наївно.

На основі таких краш-тестів формуються протоколи збоїв, виявляються прогалини і проблеми, розробляються спеціальні інструкції, як треба працювати з системами в таких умовах. Зарубіжна практика застосування подібних систем свідчить, що вибори – це тільки олдскул, тобто стара перевірена система роботи з паперовими носіями, бо машинами можуть керувати розумніші за розробників люди.

Друге це те, що може статися напередодні дня голосування з будь-якою системою збору і обробки даних, свідками чого ми з вами не раз були. Це всілякі вірусні атаки, втручання в систему зовні. Наприклад, вибори 2004 року та історія з так званим паралельним сервером. Або недавні вибори 2014 року, коли ми спостерігали атаку на сайт ЦВК та спроби виведення з ладу ІАС «Вибори». Минули роки і навіть десятиліття, а ми й досі не по-

чули відповіді на запитання, що тоді дійсно сталося? Але суспільство має отримати ці відповіді, бо питання довіри тут ключове і це не питання покарання всіх підряд чи їх ув'язнення, це питання адекватної відповіді на те, що тоді трапилося.

А що, коли йтиметься про офіційні результати виборів і встановлення офіційних результатів волевиявлення громадян? Це питання я порушую не з метою когось звинуватити, а тому, що це частина великого ризику, це вивчення власного досвіду і власних проблем у ході технологічного забезпечення життєздатності системи адміністрування виборчого процесу. Якщо ми щось упустимо, то для нас буде закрито шлях до будь-яких масштабних нововведень.

Але я не ретроград і не хочу сказати, що в Україні не потрібно працювати над удосконаленням збору і оприлюднення даних, які стосуються підрахунку голосів і встановлення результатів виборів. Проте ми повинні більш адекватно підходити до того, що жодний текст презентації, законопроекту чи ідеї нам не дасть відповіді на технічні запитання, так само як присутні тут люди, в тому числі і я, які мають гуманітарну освіту, не можуть адекватно зараз ні опонувати, ні захищати позицію, яка стосується безпосередньо

е-протоколів, збору та передачі інформації, захищеності каналів зв'язку тощо. А головне, щоб люди, які це критикуватимуть, були абсолютно незалежними і представляли як мінімум різні групи інтересів. Лише тоді формат пілотного проекту з бекап-системою, а бекап має бути передбачений при запровадженні будь-яких новацій у встановленні результатів голосування та підрахунку голосів, матиме сенс. Без можливості по-

вернення до початкового рівня, у разі знищення бази даних, більше нічого не залишається, тоді вибори не відбулися, і плюс-мінус мільярд гривень викинуто на вітер! Цього не можна допустити, тому що в нашій країні питання виборів це частина глобальної безпеки і якщо вибори будуть зірвані, то наступні вже можуть відбутися або не в цих кордонах або за іншої адміністрації.

І останнє. Дійсно, людський

фактор є визначальним у будь-якій системі, в тому числі у виборчому процесі. Якщо чесно, мені не зрозуміло, чим довіра до членів ОВК є нижчою, ніж довіра до членів ДВК? Тому що їх просто більше чи, може, це дешевше коштує? Чи просто адміністративно складніше. Тому не думаю, що варто дискредитувати прошарок виборчих комісій середньої ланки тільки для того, щоб виправдати новітню технологію.



Олексій КОШЕЛЬ,
*голова правління
Всеукраїнської громадської
організації «Комітет
виборців України»*

Щодо концепції використання інформаційних технологій, запропонованих Центральною виборчою комісією, то ми детально вивчали цю концепцію, більше того, навіть обговорили її в обласних організаціях КВУ і, на відміну від багатьох моїх колег, у нас немає серйозних зауважень. Тобто зараз досить рано критикувати, оскільки ми бачимо лише концепцію, а не бачимо самого тексту законопроекту. На етапі вивчення,

обговорення, внесення змін до законопроекту, можна буде вирішити досить багато суперечливих питань, про які сьогодні згадували. Тому не хотілося б розглядати цю концепцію виключно в чорно-білому форматі.

Знов-таки, якщо розглядати досвід низки європейських держав, то єдине суттєве зауваження до концепції і до майбутнього законопроекту полягає в тому, що протоколи обов'язково повинні дублюватися в паперовому форматі, оскільки це питання довіри до результатів виборів і ми вже не раз бачили приклади досить серйозних кібер-атак.

Питання інформаційної безпеки на виборах – це не лише питання законодавчого регулювання, тому що на законодавчому рівні можна лише збільшити рівень відповідальності за ті чи інші порушення. Насамперед це питання безпосередньої роботи з політичними партіями, це навчання партій азам інформаційної безпеки.

Я наведу лише один з прикладів. Наша організація звернулася до трьох парламентських фракцій з тим, щоб вони не використовували

у своїй роботі чужі соцмережі. В період реальної війни три парламентські фракції з шести офіційно використовують такі соцмережі. Чи створює це ризики у виборчому процесі? Звичайно так, і досить серйозні. Тут можна пригадати офіційну заяву СБУ 2014 року, коли вона радила і виборцям, і суб'єктам виборчого процесу відмовитися від використання чужих соцмереж.

Знов-таки існує серйозна загроза інформаційних диверсій, починаючи від використання е-пошти, сервер якої знаходиться на території сусідньої держави, закінчуючи нехтуванням елементарних правил інформаційної безпеки. Тому ризик інформаційних диверсій залишається досить високий, крім того, ще й ризики оприлюднення приватного листування е-пошти та іншої інформації суб'єктами виборчого процесу. І на цьому етапі, мені здається, насамперед варто приділити увагу навчанню партійних керівників, партійних штабів основам комп'ютерної безпеки, оскільки це дійсно може покращити рівень інформаційної безпеки під час виборів. Дякую.



Євген РАДЧЕНКО,
експерт Реанімаційного
Пакету Реформ

Будь-які ініціативи, будь-які пропозиції і реформи мають бути не тільки обгрунтованими, а й проаналізованими, при чому не раз і не двічі, а кілька разів, щоб виключити всі загрози.

Перший аналіз, як на мене, має включати найнеймовірніші загрози, які тільки можна собі уявити. Я вже не раз казав, що від сокири в моніторі ніхто не застрахований! І під час передачі результатів голосування з дільниці до Центральної виборчої комісії. І це, повірте, не перебільшення. Адже є такі члени комісій, які дійсно можуть і по голові дати, і стрільбу на дільниці відкрити. Якщо вони не зуміють сфальсифікувати результати мирним шляхом, то вдаватимуться і до радикальних заходів. Тому система має бути проаналізована

і на ці загрози в тому числі. Будь-яка пропонована система повинна мати запас міцності, інакше вона завжди може бути порушена чи поламана.

Ще одна дуже важлива річ. Що робити, коли виникає надзвичайна ситуація: блокування чи поламка? Система тоді повинна передбачати можливість перерахунку вручну. Без використання спеціальних пристроїв. Якщо це можливо зробити, тоді вона справді заслуговує на увагу. А якщо будь-яка техногенна катастрофа або чийсь умисел можуть зірвати роботу системи при підрахунку голосів або передачі даних, чи, скажімо, заблокувати їх оприлюднення, то така система, звісно, не має права на існування.

Ще один дуже важливий критерій. Ми всі повинні бути впевнені в тому, що тут не переслідуються будь-які інші інтереси, про які не сказано, а про які ми можемо тільки здогадуватися. Наприклад, чи немає нічийого інтересу при закупівлі устаткування, яким пропонується обладнати 30 з лишком тисяч виборчих дільниць? Сума закупівлі просто величезна! І це дійсно загроза.

І останнє. Ми повинні дуже чітко проаналізувати і подумати, а чи мають взагалі сенс такі реформи. Моє глибоке переконання в тому, що без реформи виборчої системи – запрова-

дження відкритих списків, суто пропорційної виборчої системи – нововведення в обробці даних і передачі інформації на комп'ютерах сенсу не матимуть. Чому? Та дуже просто. Наші мажоритарні кандидати зіпсують будь-яку систему, вчинять диверсії і все що завгодно, аби тільки відкоригувати свій результат на виборах! І саме мажоритарна складова, на мою думку, є найбільшою загрозою для існування нормальних, адекватних систем передавання даних.

Так само, я вважаю, і з другою ініціативою. Сенс реформування виборчого бюлетеня теж не є однозначним. При існуючій виборчій системі голосування шляхом вписування кандидатів, можливо, й зекономить кошти, але, як на мене, несе багато загроз. Однак при системі з відкритими списками такий бюлетень і форма голосування шляхом вписування дійсно потрібні, навіть більше – це є сувоюрою необхідністю.

Тому, якщо ми не проаналізуємо всіх цих факторів ризику, буде досить складно переконати і громадянське суспільство, і експертне середовище, і журналістів у тому, що автори пропонованих нововведень не мають інших інтересів, відмінних від тих, які задекларовані. А над довірою працювати треба передусім авторам подібних нововведень. Дякую.