NAUKA 4/2021 • 105–115 DOI: 10.24425/nauka.2021.137645

Adam Wójtowicz*

Zarządzanie bezpieczeństwem zbiorowego podejmowania decyzji w jednostkach naukowych w okresie postpandemicznym

Pandemia Covid-19 przyspiesza procesy cyfryzacji i migrację do zdalnego trybu świadczenia usług – w wielu dziedzinach, w wielu krajach. Dzieje się tak również w polskim szkolnictwie wyższym w zakresie prowadzenia badań naukowych, dydaktyki i procesów organizacyjnych. Pod presją obostrzeń sanitarnych uwolniony zostaje potencjał technologii informatycznych dostępnych od kilkunastu lat w środowisku naukowym i szerzej w gospodarce, ale z różnych względów niewykorzystywanych. Przykładem mogą być tu przyspieszone wdrożenia systemów elektronicznego obiegu dokumentów na uczelniach. Generalnie zjawisko to ma charakter modernizacyjny i jednoznacznie pozytywny. Jednak w niektórych obszarach migracja do zdalnego trybu świadczenia usług – na przykład w dziedzinie zdalnie prowadzonej dydaktyki – budzi istotne i często uzasadnione kontrowersje (choćby związane z niedoborem interakcji społecznych w procesie dydaktycznym), ale także przyciąga sporo uwagi – w środowisku akademickim, a nawet w debacie publicznej. Z kolei w zakresie organizacji instytucji naukowych zmiany technologiczne stymulowane przez pandemię również nieuchronnie następują, ale już nie przyciągają takiej uwagi środowiska, choć niektóre z nich są nie mniej istotne.

Jednymi z takich istotnych zagadnień są procesy zbiorowego podejmowania decyzji w jednostkach naukowych, na przykład wybory władz uczelni (rektorów, prorektorów, członków senatów, rad czy kolegiów). W okresie postpandemicznym na uczelniach może nasilać się migracja, na wzór innych procesów, w stronę realizacji takich głosowań w trybie zdalnym drogą elektroniczną. Oznacza to wykorzystanie urządzeń użytkowników, łączy internetowych i dedykowanych systemów zbierających i zliczających głosy zamiast tradycyjnych procedur i infrastruktury: fizycznej obecności, papierowych kart do głosowania, kabin i urn. Zjawisko to wymaga pogłębionej analizy, której celem jest ułatwienie zarządzającym jednostkami naukowymi dokonania wyboru optymalnych rozwiązań w kolejnych latach, gdy takie decyzje będą mogły się odbywać bez presji czasu i inwazyjnych obostrzeń sanitarnych.

* Dr hab. inż. Adam Wójtowicz, prof. UEP, (awojtow@kti.ue.poznan.pl), Katedra Technologii Informacyjnych, Uniwersytet Ekonomiczny w Poznaniu

W procesie elektronicznego głosowania zdalnego kluczowym wymaganiem jest jego bezpieczeństwo. Fakt, że analizowany jest przypadek środowiska akademickiego, które nie leży w głównym obszarze zainteresowań cyberprzestępczości i w którym panują na ogół wysokie standardy etyczne oraz ponadprzeciętny poziom społecznego zaufania, nie powinien prowadzić do luzowania wymagań związanych z cyberbezpieczeństwem, choćby ze względu na skalę zjawiska – liczbę pracowników uczelni w Polsce i wynikające z niej prawdopodobieństwo, że w niektórych z nich może w mniej lub bardziej odległej przyszłości dochodzić do zewnętrznych lub wewnętrznych ataków na procesy wyborcze realizowane drogą elektroniczną.

Bezpieczeństwo elektronicznego głosowania zdalnego ma szereg różnych, niekiedy wzajemnie przeciwstawnych, atrybutów: autentyczność, poprawność, anonimowość, weryfikowalność, brak potwierdzeń (ang. *receipt-freeness*), dostępność. Wybór i szczegółowa definicja poszczególnych atrybutów wynikają ze sposobu działania systemów elektronicznego głosowania, ale także zależą od konkretnych uwarunkowań prawnych danego rodzaju głosowania. Poniżej przedstawiono krótką charakterystykę atrybutów bezpieczeństwa systemów zdalnych głosowań elektronicznych.

Atrybuty bezpieczeństwa

(A1) Autentyczność oddawanych głosów

System zapewnia, że głosować mogą tylko zarejestrowani głosujący – każdy maksymalnie raz. Niektóre systemy pozwalają na wielokrotne głosowanie i w wynikach uwzględniają jedynie ostatni głos danego głosującego – tylko ostatni głos jest autentyczny. Ma to utrudnić wymuszanie określonego głosowania przez fizyczną obecność atakującego w pobliżu głosującego. Głosujący może bez wiedzy i nadzoru atakującego zagłosować powtórnie i unieważnić tym samym poprzedni, wymuszony głos.

(A2) Poprawność zbioru oddanych głosów

Poprawność oddanych głosów musi być zachowana, zatem system musi uniemożliwiać modyfikowanie, zastępowanie, usuwanie oraz dodawanie („dosypywanie") głosów przed, w trakcie i po głosowaniu. Niemożliwe powinno być przeprowadzanie ataków tego typu z zewnątrz, ale także proceder ten powinien być niemożliwy do przeprowadzenia dla operatora głosowania czy administratora systemu, nawet mającego pełen dostęp do wszystkich modułów systemu i przechowywanych w nich danych.

(A3) Anonimowość głosujących

Oddane głosy muszą być anonimowe, to znaczy, że tożsamość ani inne dane identyfikujące głosującego nie mogą być na żadnym etapie głosowania możliwe do powiązania z wyborem dokonanym w oddanym głosie. Tego powiązania nie może dokonać nie

tylko zewnętrzny atakujący, ale też operator głosowania mający pełen dostęp do wszystkich modułów systemu. Anonimowość głosujących musi być zachowana zarówno w samym systemie, jak i w kanałach komunikacyjnych.

(A4) Weryfikowalność wyników głosowania

System musi umożliwiać kryptograficzne zweryfikowanie przez zewnętrzną stronę, np. głosującego (nie tylko przez operatora głosowania), czy głos danego głosującego został nie tylko zarejestrowany w systemie, ale też poprawnie zliczony, tj. uwzględniony w opublikowanych wynikach. Możliwa powinna być też globalna weryfikacja (audyt) poprawności działania systemu i poprawności wyników: zachowania wymagań (A1) i (A2).

(A5) Brak potwierdzeń oddanych głosów

System nie może udostępniać głosującym kryptograficznych potwierdzeń oddanego głosu wraz z zapisanym wyborem, np. w celu zapewnienia atrybutu (A4). W przeciwnym przypadku umożliwiałby prowadzenie procederu handlu głosami lub wymuszania określonego głosowania. Brak dokumentu kryptograficznie potwierdzającego określony głos nie daje kupującemu głosy pewności, że głosujący rzeczywiście oddał głos zgodny z intencją kupującego.

(A6) Dostępność i identyfikowalność systemu głosowania

System musi być dostępny dla głosujących w okresie głosowania, tzn. musi być odporny na awarie różnego rodzaju oraz ataki odmowy dostępu. Ponadto autentyczność systemu musi być możliwa do weryfikacji przez głosujących, aby zminimalizować ryzyko ataku, polegającego na podstawieniu głosującym fałszywego systemu, np. przez *phishing*.

Wymienione wymagania odróżniają zdalne głosowania elektroniczne od innych zastosowań, w których bezpieczeństwo również jest krytyczne, takich jak często przywoływana elektroniczna bankowość („skoro robimy przelewy *online*, dlaczego nie możemy głosować?"). W elektronicznej bankowości nie mamy do czynienia z wymaganiami (A3), (A4) czy (A5), co czyni bezpieczeństwo procesu głosowań znacznie trudniejszym do osiągnięcia niż bezpieczeństwo przelewów *online*, zwłaszcza że w tym drugim zastosowaniu ewentualne błędy są odwracalne. Dorobek bezpieczeństwa elektronicznej bankowości jedynie w ograniczonym zakresie stosuje się do dziedziny głosowań.

Godzenie sprzeczności

Już z wyżej przedstawionego krótkiego wypunktowania wymagań bezpieczeństwa widać, że naiwne podejście do konstrukcji systemu zdalnych głosowań, polegające na przeprowadzaniu tajnego głosowania w zwykłym izolowanym systemie informatycznym

(baza danych głosów, nawet zaszyfrowanych w czasie składowania na serwerze w tzw. chmurze), nie spełniałoby co najmniej wymagania (A2) – operator głosowania lub administrator systemu mógłby dowolnie modyfikować wyniki głosowania. Co gorsza odbywałoby się to bez żadnego wiarygodnego śladu, brak byłoby możliwości „ponownego przeliczenia głosów". Nawet jeżeli ogłoszony wynik głosowania byłby poprawny, przegrywający nie ma podstaw, by mu wierzyć. Niestety takie systemy oferowane na rynku są reklamowane jako bezpieczne.

Przeciwną skrajnością są systemy głosowań publicznych, gdzie jawne głosy są rejestrowane w rejestrach publicznych. Podczas gdy znacząco utrudniają one naruszenia wymagania (A2), nie zapewniają one wymagania (A3). W wielu przypadkach – w tym w wielu głosowaniach na uczelniach – wymaganie (A3) jest wymuszone przez prawo lub wewnętrzne uregulowania, gdyż brak obligatoryjnej anonimowości może prowadzić do poddania głosujących presji przełożonych, środowiska czy władz państwowych oraz znacząco ułatwia proceder handlu głosami.

W odpowiedzi na wyżej wymienione ograniczenia świat nauki od lat rozwija protokoły i systemy łączące do pewnego stopnia sprzeczne wymagania, jak (A2) i (A3), czy (A4) i (A5), które są oparte na formalizmach kryptograficznych. W omawianych zastosowaniach popularne są na przykład szyfrowanie homomorficzne (ang. *Homomorphic Encryption*, HE) [1], dowody o wiedzy zerowej (ang. *Zero-Knowledge Proofs*, ZKP) [2] czy *mix networks* [3]. Na ich podstawie powstają systemy jak Helios [4], zgodne z podejściem *End-to-end verifiability* [5].

Systemy takie jak Helios zapewniają, że głos jest oddawany zgodnie z intencją anonimowego głosującego, zbierany przez system zgodnie z tym, jak został oddany, i zliczany zgodnie z tym, jak został zebrany. W systemach tych nie ma stron zaufanych, są zaprojektowane z założeniem, że każda ze stron procesu (głosujący, operator głosowania, administrator serwera, dostawca/poddostawca oprogramowania, dostawca sprzętu) może być źródłem ataku. W przypadku serwerów własność tę osiąga się przez ich rozproszenie między niezależne, nieufające sobie podmioty. Systemy te umożliwiają również kryptograficzną weryfikację publikowanych wyników: głosujący może zweryfikować, czy jego głos został uwzględniony w wynikach bez ujawniania go, a każdy może zweryfikować sumę zliczonych głosów bez wiedzy, kto jak głosował. Kod źródłowy realizujący operacje kryptograficzne jest otwarty (ang. *open source*), jest możliwa zewnętrzna ocena jego jakości i bezpieczeństwa. Istotna część kodu – na przykład szyfrująca głos – jest wykonywana po stronie klienta, czyli na urządzeniu głosującego, pod jego kontrolą. Zatem głosujący wie, jaki kod w rzeczywistości jest w użyciu w procesie głosowania i teoretycznie może zweryfikować jego poprawność czy wybrać alternatywną implementację. Jest to zgodne z jedną z fundamentalnych zasad tworzenia bezpiecznych rozwiązań programowych opartych na kryptografii – zasadą otwartego projektu. Mówi

ona, że bezpieczeństwo rozwiązania nie może zależeć od tajności jego projektu czy implementacji. Tajność projektu czy implementacji (*security by obscurity*) wprowadza złudne poczucie bezpieczeństwa (jest łatwa do naruszenia), usypia czujność i utrudnia wnikliwą „recenzję tysiąca oczu" ze strony kryptografów i programistów.

Otwarte problemy

Jednak wdrażanie w praktyce nawet zaawansowanych rozwiązań opartych na sprawdzonej kryptografii nie jest wolne od problemów wpływających na bezpieczeństwo lub wiarygodność procesu głosowania. Pierwszym problemem jest poziom kompetencji przeciętnego głosującego, który na ogół nie jest w stanie dokonać świadomie wspomnianej wyżej weryfikacji poprawności użytego przez siebie narzędzia, weryfikacji autentyczności systemu, weryfikacji zliczenia swojego głosu przez system (P1), ani być pewnym swojej anonimowości. Jest to niezależne od tego, czy narzędzia kryptograficzne, którymi się posługuje, są „obudowane" prostymi interfejsami użytkownika czy nie. Sama idea szyfrowania homomorficznego, gdzie jest możliwe przeprowadzanie operacji na zaszyfrowanych danych (np. sumowanie zaszyfrowanych głosów) bez znajomości tych danych (bez wiedzy – kto jak głosował) wydaje się trudna do przyjęcia dla głosujących bez technicznego wykształcenia. Podobnie jest z dowodami o wiedzy zerowej, gdzie jedna ze stron potrafi udowodnić drugiej, że dysponuje pewną informacją, bez jej ujawniania. Trudności ze zrozumieniem działania systemu i weryfikacją jego poprawności są więc już na poziomie koncepcyjnym, nie wspominając o poziomie implementacyjnym. Nawet w środowisku akademickim.

Wiąże się to z kolejnym problemem – braku zaufania przegranych i neutralnych obserwatorów do opublikowanych wyników (P2). To właśnie akceptacja woli wyborców przez wszystkie strony niezależnie od jej werdyktu leży u podstaw demokratycznego głosowania. Proces wyborczy, którego wyniki nie budzą zaufania, zamiast umożliwić bezkonfliktowe podjęcie decyzji w społeczności akademickiej, będzie te konflikty dodatkowo podsycał.

Serwery udostępniające funkcjonalności zdalnego głosowania muszą być siłą rzeczy wystawione na ruch sieciowy z Internetu, więc tym samym mogą być celem anonimowych ataków przeprowadzanych w sposób zautomatyzowany z różnych lokalizacji geograficznych (P3). Na przykład przez wykorzystanie tzw. *zero day*, czyli świeżo wykrytej i niezałatanej podatności w systemie obsługującym głosowanie lub w oprogramowaniu serwera, na serwer może zostać załadowane złośliwe oprogramowanie lub wstrzyknięty fragment kodu. Bardzo trudno jest tworzyć oprogramowanie gwarantujące, że jest w pełni wolne od błędów na poziomie projektu, implementacji i wdrożenia. W przypadku zdalnych głosowań elektronicznych dodatkowo dochodzi wymaganie tzw. niezależności od oprogramowania, tzn. „niewykryty błąd oprogramowania nie może powodować

niewykrywalnych zmian w wyniku głosowania" [6]. Serwery mogą stać się również obiektem ataków sieciowych czy prób podszycia się, na przykład w schemacie *Man in the Middle*, lub ataków odmowy dostępu usługi (DDoS). Te ostatnie mogą być przeprowadzane nie tylko przeciwko całemu systemowi, ale również w odniesieniu do wybranych głosujących lub grup głosujących. Generalnie omawiany problem (P3) dotyczy nie jednego, a aż trzech atrybutów bezpieczeństwa: (A1), (A2) i (A6).

Kolejnym problemem jest bezpieczeństwo tzw. „końcówek klienckich", czyli urządzeń i systemów, z których korzystają głosujący (P4). Nawet jeżeli sam system głosowania jest bezpieczny zarówno na poziomie projektu, kryptografii, jak i implementacji, to urządzenie, z którego użytkownik głosuje, nie może być postrzegane jako bezwarunkowo bezpieczne, np. może pozostawać pod kontrolą strony trzeciej lub być zainfekowane złośliwym oprogramowaniem, w szczególności oprogramowaniem dedykowanym atakom na głosowania. Zdalna kontrola bezpieczeństwa urządzeń będących w dyspozycji użytkowników końcowych jest bardzo trudna, jeśli nie niemożliwa do wdrożenia w praktyce. Zatem złośliwe oprogramowanie (np. w schemacie *Man in the Browser* albo za pomocą zmodyfikowanej wtyczki do przeglądarki lub aplikacji mobilnej) może modyfikować oddawany głos bez wiedzy użytkownika – już na urządzeniu użytkownika, zanim zostanie on przesłany do bezpiecznego systemu kryptograficznego. Analogicznie informacja zwrotna dostarczana użytkownikowi przez system może być modyfikowana przez złośliwe oprogramowanie dopiero na urządzeniu klienckim tuż przed jej wyświetleniem, utrzymując użytkownika w błędnym przekonaniu – na przykład, że oddał ważny głos.

Warto zauważyć, że ataki przeprowadzane w ten sposób nie muszą wymagać od zlecającego atak wiedzy technicznej z zakresu hakingu. Atakujący może uzyskać płatny dostęp do gotowych narzędzi ataku w modelu *as a service* w tzw. darknecie. W takim scenariuszu rośnie efektywność ekonomiczna ataku.

We wcześniejszych sekcjach został już poruszony wątek handlu głosami oddawanymi elektronicznie, a także wymuszenia określonego głosowania, stanowiące kolejny problem związany z bezpieczeństwem i wiarygodnością całego procesu (P5). Proceder handlu głosami staje się możliwy do prowadzenia na większą skalę dzięki systemom zdalnych głosowań wydającym kryptograficzne potwierdzenia oddanych głosów, jeśli potwierdzenia te zawierają informacje o dokonanym wyborze. Mogą być one żądane przez kupującego w zamian za opłatę, przez co proceder jest mniej ryzykowny dla kupującego głosy: głosujący nie może sekretnie zagłosować wbrew woli kupującego mimo wcześniejszej sprzedaży głosu. Potwierdzenia mogą być wykorzystywane nie tylko w procederze kupowania, lecz także wymuszania, przez wymuszających stojących wyżej w hierarchii społecznej czy zawodowej. Ryzyka te mogą być do pewnego stopnia zredukowane dzięki systemom pozbawionym potwierdzeń (A5), co jednak utrudnia zabez-

pieczenie systemu przed problemami (P1) i (P2). Innym podejściem redukującym ryzyko jest gwarantowanie kryptograficznej wiarygodnej zaprzeczalności (ang. *plausible deniability*), polegającej na udostępnieniu głosującemu alternatywnych potwierdzeń, które może przedstawić stronie kupującej głosy, a ta je zweryfikować.

Strona kupująca głosy może również prowadzić swój proceder, płacąc za dostęp do pełnego oprogramowania klienckiego na cały czas głosowania (włącznie z udostępnieniem i zmianą haseł), *de facto* kupując możliwość zdalnego podszycia się pod tożsamość głosującego. Ten schemat kupowania głosów eliminuje – z punktu widzenia atakującego – konieczność dostarczenia potwierdzenia oddanego głosu. Ryzyko tego typu mogłoby (do pewnego stopnia) zostać zredukowane przez zastosowanie systemów biometrycznej identyfikacji głosujących, ale one z kolei niekorzystnie wpływają na utrzymanie poziomu anonimowości głosujących i tworzą inne problemy techniczne i organizacyjne.

Wymuszenie określonego głosowania, przeprowadzanego w trybie zdalnym, może się również odbywać po prostu przez fizyczną obecność wymuszającego w pobliżu głosującego w trakcie głosowania – choć już na mniejszą skalę. To ryzyko może być redukowane przez umożliwienie wielokrotnego głosowania i zliczanie jedynie ostatniego oddanego głosu, jak wspomniano w punkcie (A1). Głosujący może w późniejszym terminie, już bez nadzoru wymuszającego, zagłosować powtórnie i unieważnić tym samym poprzedni głos – chyba że do wymuszenia doszło tuż przed upływem okresu głosowania.

Bezpieczeństwo tradycyjnych procedur

W procesie głosowania realizowanym na miejscu z użyciem tradycyjnych procedur poziom wyżej wymienionych ryzyk jest znacznie niższy. Głosowanie i zliczanie głosów odbywają się w przestrzeni kontrolowanej przez przedstawicieli różnych kandydatów lub zwolenników różnych stanowisk oraz neutralnych obserwatorów. Nie ufają oni sobie i kontrolują proces wyborczy oraz siebie wzajemnie. Jednocześnie w tej przestrzeni publicznej możliwe jest wydzielenie prywatnych obszarów (kabin), w których odbywa się zaznaczenie przez głosującego sekretnego wyboru na karcie do głosowania. Anonimowość głosowania jest też zapewniana przez odseparowanie procesu wydawania kart poprzedzonego weryfikacją tożsamości od procesu dokonywania wyboru na karcie i wrzucania karty do urny. Nie są wydawane żadne oficjalne potwierdzenia dokonanego wyboru, zatem proceder handlu głosami jest utrudniony. Cały proces jest zrozumiały dla wszystkich członków komisji, a także dla poszczególnych głosujących. Co ważne, w przypadku podejrzeń nieprawidłowości czy protestów możliwe jest ponowne przeliczenie składowanych bezpiecznie głosów oddanych na papierze – również w procedurze zrozumiałej dla wszystkich stron.

Ryzyko: prawdopodobieństwo a wpływ

Stuprocentowe bezpieczeństwo nie istnieje i oczywiście możliwe są skuteczne ataki również na proces przeprowadzany metodami tradycyjnymi. Z punktu widzenia zarządzania bezpieczeństwem kluczowe jest oszacowanie poziomu ryzyka w obu podejściach. W najprostszym modelu współczynnik ryzyka definiowany jest jako iloczyn prawdopodobieństwa zajścia zdarzenia i współczynnika wpływu tego zdarzenia na chroniony zasób czy proces. To właśnie współczynnik wpływu stanowi o różnicy ryzyk (iloczynów) między analizowanymi dwoma podejściami: w przypadku głosowania zdalnego drogą elektroniczną udany atak na system (z zewnątrz lub z wewnątrz) najczęściej umożliwi trudny do wykrycia *post factum* i przesądzający wpływ na ostateczny wynik głosowania, podczas gdy w modelu tradycyjnym udany atak będzie skutkował sfałszowaniem (np. unieważnieniem) niewielkiego odsetka głosów – na przykład przez jednego z członków komisji nie dość skutecznie skontrolowanego przez pozostałych. Oszacowanie prawdopodobieństwa zajścia incydentu jest trudniejsze – na niekorzyść modelu zdalnego świadczy otwarcie infrastruktury na anonimowe zautomatyzowane ataki z całego świata, trudność w zagwarantowaniu braku luk w oprogramowaniu i ułatwienie procederu handlu głosami w porównaniu z modelem tradycyjnym. Wszystkie te czynniki mogą zwiększać prawdopodobieństwo zajścia udanego ataku w modelu zdalnym. Z kolei na niekorzyść modelu tradycyjnego świadczy brak konieczności posiadania wiedzy eksperckiej z dziedziny IT potrzebnej do przeprowadzenia ataku.

Dostępne są również podejścia hybrydowe – zakładające głosowanie lokalne z użyciem urządzeń elektronicznych, utrzymywanych przez operatora głosowania, a jednocześnie papierowych kart. Jeżeli są oparte na sprawdzonych protokołach [7], zmniejszają poziom pewnych ryzyk, zapewniając lepszą weryfikowalność i audyt. Niestety nawet wtedy nie eliminują wszystkich ryzyk (ataki odmowy dostępu), dokładają nowe problemy (awaryjność, koszty), a przede wszystkim pozostawiają niski poziom wygody – w dalszym ciągu głosujący muszą fizycznie udać się do pomieszczenia, w którym odbywa się wydawanie kart i głosowanie. Natomiast, jeżeli maszyny do elektronicznego głosowania na miejscu nie są oparte na sprawdzonych protokołach, lista ryzyk jest jeszcze dłuższa (problem zaufania do urządzeń, włamania do systemu, ataki wewnętrzne).

Generalnie największe autorytety z dziedziny kryptografii czy kryptografii stosowanej, jak Ron Rivest (litera „R" w algorytmie RSA leżącym u podstaw współczesnej kryptografii asymetrycznej, zapewniającej bezpieczeństwo w Internecie) [8] czy Bruce Schneier (autor wielu klasycznych monografii z dziedziny kryptografii i cyberbezpieczeństwa) [9], są zgodne w swoim sceptycyzmie odnośnie do aplikowania zdalnych metod elektronicznych w zastosowaniach, gdzie może dochodzić do kupowania głosów lub wymuszeń – dopóki nie wypracujemy lepszych rozwiązań, na co się na razie nie zanosi. Można powiedzieć, że panuje w tej sprawie ekspercki konsensus.

Blockchain nie stanowi rozwiązania

W ostatnich latach modną technologią jest *blockchain*, który rzekomo ma rozwiązać wiele problemów w dziedzinie projektowania systemów, w tym te dotyczące ich bezpieczeństwa. Niestety sama technologia *blockchain* jest niewystarczająca do zabezpieczenia systemów elektronicznych zdalnych głosowań [10]. Rozproszony rejestr oparty na łańcuchach bloków samodzielnie może być wykorzystany jako jeden z elementów większego systemu – jako zaufana tablica wyników głosowania, a i w tym zakresie dotychczas stosowane technologie są bardziej odpowiednie i sprawdzone. Nie rozwiązuje też żadnego z wyżej opisanych problemów związanych z bezpieczeństwem, głosujący są ciągle zdani na niezaufane urządzenia końcowe oraz infrastrukturę sieciową podatne na ataki i awarie. W ramach sieci *blockchain* z powodzeniem realizowane są funkcjonalności, takie jak możliwość uzyskania wiarygodnego konsensusu przez rozproszone węzły sieci *blockchain* czy funkcjonalność „głosowania" na wyniki inteligentnych kontraktów (ang. *smart contracts*). Mogą one obserwatorowi technologii przypominać usługi zdalnego elektronicznego głosowania. Niestety możliwość realizacji tych funkcjonalności w sieci *blockchain* nie rozwiązuje żadnego z opisanych we wcześniejszych sekcjach problemów i wymagań bezpieczeństwa zdalnych głosowań. Co gorsza stosowanie technologii *blockchain* wprowadza nowe problemy, związane z wysoką złożonością zdecentralizowanych systemów utrzymywanych przez wiele stron i trudnościami w ich zarządzaniu. Aktualizacje protokołów czy łatanie luk bezpieczeństwa i ich wdrażanie wymaga znacznie więcej nakładów i czasu, co może się okazywać krytyczne w takich zastosowaniach jak zdalne głosowania.

Ryzyka w innych procesach

Warto nadmienić, że głosowania nie są jedynym procesem, który na wyższych uczelniach podlega cyfryzacji mogącej mieć wpływ na autentyczność informacji. W dziedzinie badań naukowych zbieranie danych w formie cyfrowej zastępuje tradycyjne formy zbierania danych. Przykładem i pewną analogią do problemu głosowań może być proces ankietyzacji. Papierowe ankiety zostawiające ślad (dowód) są zastępowane elektronicznymi usługami, które mają liczne zalety, ale jednocześnie ich cyfrowe wyniki łatwiej jest sfałszować. Oczywiście świat nauki przez lata wypracował inne skuteczne procedury weryfikacji wyników badań – na przykład *peer review* czy badania replikacyjne – zatem problem ten nie jest tak krytyczny w procedurach samych badań naukowych. Natomiast w obszarze – na przykład – oceny pracowniczej ankietyzacja studentów dotycząca oceny jakości dydaktyki i prowadzących zajęcia odgrywa kluczową rolę, choć budzi też kontrowersje [11]. Ankietowani studenci mogą dokonywać autocenzury, jeżeli nie mają przekonania, że system ankietowy jest oparty na weryfikowalnych rozwiązaniach kryptograficznych gwarantujących ankietowanym anonimowość. Z drugiej strony na podstawie wyni-

ków anonimowych ankiet studenckich zbieranych drogą elektroniczną na wielu uczelniach podejmowane są istotne decyzje odnośnie do karier zawodowych pracowników naukowo-dydaktycznych, a zwykle nie używa się systemów udostępniających kryptograficzne i weryfikowalne dowody na autentyczność wyników ankietyzacji. Gdyby doszło do jakiekolwiek naruszenia anonimowości czy fałszerstwa, byłoby to w praktyce nie do wykrycia. Niewątpliwie potrzebne jest stosowanie systemów weryfikowalnych.

Osiągnięciem cywilizacyjnym jest podejmowanie ważnych decyzji na podstawie zweryfikowanych oraz wiarygodnych danych. Nie powinniśmy – jako środowisko naukowe – od niego odchodzić. Z samego faktu, że jakieś rozwiązanie otacza aura „technologii" (a tak naprawdę jest prostym serwisem internetowymi niemającym wiele wspólnego ze współczesnymi innowacjami) nie wynika, że rozwiązanie to jest bezpieczniejsze od dotychczas używanego, czy że jest po prostu bezpieczne.

Być może nie ma przeszkód, żeby z głosowań przez Internet przy użyciu sprawdzonych rozwiązań kryptograficznych (na przykład zgodnych z podejściem *end-to-end verifiability*) korzystał w rzeczywistości postpandemicznej samorząd studencki (gdy waga decyzji nie jest szczególnie krytyczna) czy międzynarodowe stowarzyszenie kryptografów [12]. W tym ostatnim przypadku trudno jest głosującym zebrać się lokalnie, głosujący rozumieją, jak działa protokół, nie mają silnej motywacji do wymuszania określonego głosowania u innych, zachowują ponadprzeciętną świadomość zasad bezpieczeństwa i poziom zabezpieczeń urządzeń, a także niewielkie jest ryzyko ataku z zewnątrz. Ryzyko to ciągle istnieje, lecz jest stosunkowo niewielkie. Jednak odmiennym przypadkiem są głosowania nad ważnymi decyzjami na publicznych wyższych uczelniach, skupiających lokalne środowiska, mogące korzystać w głosowaniach z lokalnej tradycyjnej infrastruktury – w odpowiednim reżimie sanitarnym, jeżeli sytuacja będzie tego wymagała. Konsensus amerykańskich specjalistów od cyberbezpieczeństwa w tej sprawie [13] powinien studzić zapał do nieprzemyślanych wdrożeń, również w polskiej nauce.

Bibliografia

[1] Gentry C., *Fully Homomorphic Encryption Using Ideal Lattices*. [w:] 41st ACM Symposium on Theory of Computing (STOC), 2009

[2] Goldwasser S., Micali S., Rackoff C. (1989). *The knowledge complexity of interactive proof systems.* SIAM Journal on computing, 18(1), 186–208.

[3] Chaum D.L. (1981). *Untraceable electronic mail, return addresses, and digital pseudonyms.* Communications of the ACM, 24(2), 84–90.

[4] Adida B. (2008). *Helios: Web-based Open-Audit Voting*. [w:] USENIX security symposium (t. 17, s. 335–348).

[5] Benaloh J., Rivest R., Ryan P.Y., Stark P., Teague V., Vora P. (2015). *End-to-end verifiability*. arXiv preprint arXiv:1504.03778.

[6] Rivest R.L., Wack J.P. (2006). *On the Notion of Software Independence. Voting Systems.* White paper. https://www.nist.gov/system/files/si-in-voting.pdf
[7] Chaum D., Carback R., Clark J., Essex A., Popoveniuc S., Rivest R.L., Ryan P.Y., Shen E. and Sherman A.T., (2008). *Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes*. EVT, 8, s. 1–13.
[8] Rivest R., *Election Security*. (2019) Ding-Shum Lecture given at Harvard University.
[9] Schneier B., *American elections are too easy to hack. We must take action now*. The Guardian (2018), https://www.theguardian.com/commentisfree/2018/apr/18/american-elections-hack-bruceschneier
[10] Park S., Specter M., Narula N., Rivest R., *MIT, Going from bad to worse: from Internet voting to blockchain voting*, Journal of Cybersecurity, t. 7, nr 1, 2021, tyaa025, https://doi.org/10.1093/cybsec/tyaa025
[11] Grzegorek T. (2021). *Czy jest jakiś pożytek ze studenckiej ankiety ewaluacji zajęć?* Nauka nr 1, s. 103–118.
[12] Haber S., Benaloh J., Halevi S. (2010). *The helios e-voting demo for the iacr. International Association for Cryptologic Research*. http://www.iacr.org/elections/eVoting/heliosDemo.pdf
[13] American Association for the Advancement of Science, *Internet or Online Voting Remains Insecure*, AAAS, 2021, https://www.aaas.org/programs/epi-center/internet-online-voting

Security Management of Collective Decision Making in Academia in Post-Pandemic Period

Under the pressure of sanitary restrictions, the potential of information technologies available to the academic communities for over a dozen years, but not used for various reasons, is released. As a specific case of this trend, a migration from brick-and-mortar voting towards the remote voting by electronic means may intensify in the post-pandemic period at universities. This phenomenon requires an in-depth analysis, the aim of which is to facilitate the management of academic units to choose optimal solutions in the coming years, when such decisions can be made without time pressure and invasive sanitary restrictions. In the process of electronic remote voting, security is a key requirement, which has a number of various attributes: authenticity, correctness, anonymity, verifiability, receipt-freeness, availability. In response to these, to some extent contradictory, requirements, the world of science has been developing protocols and systems based on cryptographic formalisms for years. This article explains the main challenges related to security of remote electronic voting, from which even advanced solutions implemented in academic practice are not free.

Key words: security management, cybersecurity, electronic voting, remote voting, Internet voting, online voting, information authenticity