STUDIA I ARTYKUŁY

„Studia Wyborcze", tom 33, 2022

DOI: https://doi.org/10.26485/SW/2022/33/1

***Michał Czakowski** **

https://orcid.org/0000-0001-7463-3490

ZAKŁÓCENIA PRZEPŁYWU INFORMACJI I INCYDENTY W PROCESIE WYBORCZYM

WPROWADZENIE

W toku procesu wyborczego może dochodzić do pozyskiwania i wykorzystywania informacji o obywatelach, które dotyczą sfery ich prywatności, co w konsekwencji może prowadzić do różnego rodzaju nadużyć zarówno ze strony organów państwa (w tym do ograniczenia wolności i praw ponad wymagany poziom) [Bień-Kacała, Jirásek, Cibulka 2016: 368], jak i innych podmiotów wewnętrznych, jeśli państwo nie zapobiegnie pozyskiwaniu takich informacji.

Do zagrożeń bezpieczeństwa przebiegu procesu wyborczego o charakterze wewnętrznym zalicza się m.in. korupcję [Letkiewicz 2013: 413–417; Hypś 2014: 59–88], naciski i ograniczenia demokracji, występujące w szczególności w krajach o słabych podwalinach demokracji, np. w Afganistanie [Marszałek 2013: 5–29]. Podczas wyborów prezydenckich w 2009 r. w tym właśnie kraju obserwatorzy zagraniczni zakwestionowali wybór Hamida Karzaja, postulując zarządzenie i przeprowadzenie ponownego głosowania [Cziomer 2010: 76]. Ostatecznie ponowne głosowanie nie odbyło się, gdyż konkurent H. Karzaja podjął decyzję o rezygnacji z kandydowania [Cziomer 2010: 76]. Ograniczenia o podobnym charakterze miały miejsce także podczas wyborów przeprowadzanych w Kirgistanie za prezydentury Kurmanbeka Bakijewa – nadużycia i ograniczenia demokracji odnotowywano wówczas w takim samym wymiarze, jaki miał miejsce w Afganistanie [Shukuralieva 2011: 121–142].

* Doktor, Wydział Nauk Prawnych, Społecznych i Humanistycznych, Kujawsko-Pomorska Szkoła Wyższa w Bydgoszczy, m.czakowski@kpsw.edu.pl

CZYNNIKI WEWNĘTRZNE

Zakłócenia wewnętrzne to w szczególności przestępstwa przeciwko wyborom, spenalizowane w Ustawie z dnia 6 czerwca 1997 r. Kodeks karny[1], ale również te dotyczące zakłócania tajności głosowania oraz ciszy wyborczej, uregulowane przez ustawodawcę w Kodeksie wyborczym[2], a ponadto przestępstwa przeciwko bezpieczeństwu informacji. Obecnie szczególnie istotne wydają się zakłócenia wpływające na działanie systemów informatycznych.

Możliwość zastosowania systemu informatycznego do realizacji zadań przypisanych poszczególnym podmiotom uczestniczącym w procesie wyborczym, w szerszym niż dotychczas zakresie, zaistniała w związku z wyborami samorządowymi w 2014 r. [Rychard 2015: 7][3]. Na jego nieprawidłowe ostatecznie funkcjonowanie, o czym była już mowa, wpływ miało wiele czynników zewnętrznych, jak brak profesjonalizmu i doświadczenia w tego typu działalności podmiotu, który przyjął zlecenie stworzenia tegoż systemu, oraz wewnętrznych, do których należy zaliczyć relatywnie niewspółmiernie niskie wobec rangi i skali przedsięwzięcia nakłady państwa poczynione na ten cel, a także brak specjalistycznej wiedzy w tym zakresie pracowników pionu informatycznego Krajowego Biura Wyborczego. Skupiając się na kwestii technicznej, można wnioskować, że system informatyczny nie był przygotowany oraz przetestowany w takim stopniu, by mógł sprostać zadaniu polegającemu na transferze danych w *de facto* najtrudniejszych z punktu widzenia organizacyjnego wyborach, jakimi są wybory samorządowe.

W opinii specjalistów program do obsługi wyborów nie mógł zadziałać poprawnie. Według ustaleń profesjonalnych informatyków, którzy analizowali sprawę feralnego systemu komputerowego Państwowej Komisji Wyborczej (PKW), w odpowiedzi na ogłoszony przetarg na wykonanie programu do obsługi wyborów zgłosiła się tylko jedna, nieduża firma. Jednocześnie było zbyt mało czasu na dokładne przetestowanie i sprawdzenie programu do obsługi wyborów. Zawodowi informatycy wskazali również, że PKW w wyborach powinna wykorzystywać

[1] T.j. Dz. U. 2021 poz. 2345 ze zm., dalej k.k.

[2] Ustawa z dnia 5.01.2011 r. – Kodeks wyborczy (t.j. Dz. U. 2020 poz. 1319 ze zm.).

[3] Istotę problemów, które ujawniły się w procesie głosowania, w pełni oddaje komentarz Andrzeja Rycharda, który stwierdził, że „wybory samorządowe 16 listopada 2014 roku stały się ważnym sygnałem wskazującym na stan polskiej demokracji i praktyki jej działania. Awaria systemu informatycznego, opóźnienie podania wyników, wysoki odsetek głosów nieważnych, wreszcie rozminięcie się wyników sondaży *exit poll* i oficjalnych rezultatów – to wszystko nakazywało podjąć próbę wyjaśnienia przyczyn tego stanu rzeczy" [Rychard 2015: 7].

system informatyczny opracowany przez duże i uznane na rynku podmioty, mające doświadczenie w wykonywaniu podobnych zadań[4].

Efektem ubocznym nieprawidłowości w działaniu systemu informatycznego była negatywna ocena pracy PKW przez różne środowiska, natomiast konsekwencją tych wydarzeń i ostrej krytyki skierowanej pod adresem PKW – dymisja jej członków. W tej kwestii wypowiedział się ówczesny przewodniczący PKW, sędzia Stefan Jaworski, który podkreślił: ,,krytyka wobec kierowanej przez niego instytucji była niezasłużona i czasem godziła w fundamenty systemu demokratycznego i wyborczego"[5]. Przyznał, że wadliwie działał system informatyczny, ale zapewniał, że nie miało to wpływu na rzetelność wyborów i respektowanie gwarancji głosowania zawartych w kodeksie wyborczym"[6].

Konsekwencją zakończonego niepowodzeniem wdrożenia systemu informatycznego była kontrola dokonana przez Najwyższą Izbę Kontroli (NIK). Do najważniejszych zaleceń i wniosków przedstawionych w wystąpieniu pokontrolnym[7] należy zaliczyć opracowanie i wdrożenie wieloletniej strategii informatycznej obsługi wyborów, obejmującej m.in. wykorzystanie infrastruktury informatycznej do przeprowadzania wyborów. Zalecenie wskazuje, że zapewnienie bezpieczeństwa przepływu, przechowywania informacji, w szczególności w takiej sferze działalności państwa, jaką jest organizacja i przeprowadzenie demokratycznych wyborów, winno być ujęte w planie wieloletnim, obejmującym zadania nie tylko związane z bieżącym kalendarzem wyborczym, ale też długofalowe. Kolejnym zaleceniem NIK w przedmiotowej sprawie jest prowadzenie projektów informatycznych z wykorzystaniem sprawdzonych metodyk zarządzania projektem oraz metodyk wytwarzania oprogramowania. W dobie wysoko rozwiniętych technologii informacyjnych i cyfryzacji wręcz konieczne jest powierzenie realizacji zadań o charakterze *stricte* technicznym, a mających wymierne przełożenie w rezultacie na funkcjonowanie i zapewnienie bezpieczeństwa przepływu i przechowywania informacji przez stosowne organy państwa, profesjonalistom pracującym według określonego schematu i harmonogramu działania. Wyłonienie zwycięskiego zespołu specjalistów musi się odbyć zgodnie z obowiązującymi procedurami w tym zakresie. Kontrolerzy NIK podnieśli ponadto, że konieczne jest przygotowanie planów awaryjnych

[4] *PKW kupiła system za 429 tysięcy złotych, który nie działa. Firma miała zbyt mało czasu?*, http://www.gazetaprawna.pl/artykuly/835823,pkw-kupila-system-za-429-tysiecy-zlotych-ktory-nie-dziala-firma-miala-zbyt-malo-czasu.html (dostęp 4.01.2022).

[5] *PKW ogłosiła oficjalne wyniki II tury wyborów i podała się do dymisji, 1.12.2014 r.*, https://wiadomosci.dziennik.pl/wybory-samorzadowe/artykuly/476708,wybory-2014-wyniki-ii-tury-dymisja-pkw.html (dostęp 4.01.2022).

[6] *PKW podała się do dymisji*, http://www.gazetaprawna.pl/artykuly/838927,pkw-podala-sie-do-dymisji.html (dostęp 4.01.2022).

[7] NIK, Wystąpienie pokontrolne, druk KBF – 4114-004-01/2014, I/14/006, Warszawa 2014.

na wypadek niesprawności oprogramowania i infrastruktury obsługującej wybory. Wniosek ten jest niezwykle istotny i odnosi się do każdej sfery funkcjonowania demokratycznego państwa prawa. Niedopuszczalne jest, by organy państwa, organy administracji publicznej, dysponujące danymi dotyczącymi każdego z obywateli, nie miały instrumentów do sprawnego, rzetelnego, a nade wszystko działającego na podstawie najwyższych standardów bezpieczeństwa systemu zarządzania tymi danymi.

Jednym z najważniejszych wniosków zawartych w raporcie pokontrolnym NIK z 2015 r., a dotyczącym prawidłowego, sprawnego i rzetelnie przeprowadzonego procesu wyborczego, jest przygotowywanie, z odpowiednim wyprzedzeniem, projektów wzorów dokumentów związanych z wyborami, co umożliwi ich odwzorowanie i sprawdzenie działania w systemie informatycznym. Dwutorowość działań, polegająca na prowadzeniu dokumentacji związanej z przebiegiem wyborów zarówno w formie tradycyjnej, jak i elektronicznej, jest jak najbardziej pożądana. Daje bowiem gwarancję, że w razie zaistnienia jakichkolwiek czynników zewnętrznych, np. inwigilacji nieuprawnionych podmiotów, zdarzeń losowych etc., co najmniej jedna z form dokumentacji przebiegu wyborów przetrwa. Wiele kolejnych wniosków NIK odnosi się do szeroko pojętej procedury zamówień publicznych, w związku z realizacją jednego z podstawowych zadań państwa, jakim jest organizacja i sprawne przeprowadzenie procesu wyborczego.

Nie ulega wątpliwości, że bezdyskusyjne są takie zalecenia i wnioski, jak: wzmocnienie nadzoru nad pracownikami wykonującymi czynności w postępowaniach o udzielenie zamówień publicznych, umożliwienie pracownikom wykonującym czynności w postępowaniach o udzielanie zamówień publicznych uczestniczenia w szkoleniach w zakresie stosowania ustawy Prawo zamówień publicznych, rozważenie sporządzenia odpowiednich procedur w aspekcie dokumentowania pracy biegłych w zakresie oceny ofert w postępowaniach o udzielanie zamówień publicznych oraz składania oświadczeń, o których mowa w art. 17 ust. 2 Ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych[8], czy też podjęcie stosownych czynności, które umożliwią publikowanie ogłoszeń w siedzibie Krajowego Biura Wyborczego, zgodnie z wymogami zawartymi w ustawie Prawo zamówień publicznych. Wdrożenie tych zaleceń

[8] Art. 17 ust. 2 Ustawy z dnia 11.09.2019 r. – Prawo zamówień publicznych (Dz. U. poz. 1129 ze zm.) w brzmieniu: „Osoby wykonujące czynności w postępowaniu o udzielenie zamówienia składają, pod rygorem odpowiedzialności karnej za złożenie fałszywego oświadczenia, w formie pisemnej oświadczenie o braku lub istnieniu okoliczności, o których mowa w ust. 1. Przed odebraniem oświadczenia, kierownik zamawiającego lub osoba, której powierzył czynności w postępowaniu, uprzedza osoby składające oświadczenie o odpowiedzialności karnej za złożenie fałszywego oświadczenia".

z pewnością przyczyni się nie tylko do sprawniejszej realizacji procesu wyborczego, ale także wpłynie na pogłębienie konstytucyjnej zasady zaufania obywateli do państwa poprzez stosowanie transparentnych reguł w działalności głównych organów państwa.

W związku z rozwojem technicznym pojawiła się również potrzeba wykorzystania w procesie wyborczym możliwości, jakie daje dostępność do systemów informatycznych. Wybory samorządowe z 2018 r. miały być jeszcze bardziej transparentne – zakładano bowiem transmisję na żywo z lokali wyborczych lub, w braku takiej możliwości, zapis do późniejszego odtworzenia[9]. Jednocześnie na podstawie nowelizacji Kodeksu wyborczego z 2015 r. przyznano mężom zaufania uprawnienia do rejestracji prac komisji [Wrzalik 2015: 225]. Obecnie, z mniej lub bardziej zadowalającym rezultatem, testowano wiele systemów, np. podczas wyborów samorządowych w 2014 r. planowane było uruchomienie tzw. platformy wyborczej 2.0. Ostatecznie zdołano wdrożyć system obsługujący wybory samorządowe, który jednak, o czym już wspomniano, nie spełnił oczekiwanych wymagań [Małecki-Tepicht 2014][10]. Często komisje wyborcze dla wspomagania liczenia głosów wykorzystują tzw. kalkulator wyborczy. W 2018 r. uruchomiono WOW – system wspomagania organów wyborczych. Szeroko pojęta informatyzacja administracji skutkowała tym, że w celu wprowadzenia usprawnień dla obywateli-wyborców planowano wprowadzenie centralnego elektronicznego rejestru wyborców. Ponieważ jednak systemy informatyczne są często narażone na działanie negatywnych czynników zewnętrznych i wewnętrznych, informacja przez nie przechodząca może zostać zniekształcona.

Kolejne wybory samorządowe przeprowadzone w 2018 r. obrazują zupełnie inne podejście administracji wyborczej. Jako rodzaj bufora chroniącego przed nieprzewidzianymi informacjami stworzono portal bezpiecznewybory.pl, na którym publikowane były informacje dla wyborców, komitetów i komisji, w szczególności dotyczące niebezpieczeństw związanych z wyjaśnieniem, czym jest i jak może wyglądać tzw. phishing. Jak zabezpieczyć się przed phishingiem, co zrobić, jeśli już jest się ofiarą? Na stronie wskazano także przykładowe ataki w innych państwach oraz zagrożenia w czasie wyborów.

---

[9] *Wybory samorządowe: W lokalach wyborczych nie będzie kamer*, https://www.rp.pl/Wybory-samorzadowe/180529360-Wybory-samorzadowe-W-lokalach-wyborczych-nie-bedzie-kamer.html (dostęp 14.01.2022).

[10] *Po wyborach samorządowych 2014 roku – o efektywności i przejrzystości procesu wyborczego*, http://niezniknelo.pl/OK2/artykul/po-wyborach-samorzadowych-2014-roku-o-efektywnosci-i-przejrzystosci-procesu-wyborczego/index.html (dostęp 6.01.2022).

Rysunek 1. Bezpiecznewybory.pl

Źródło: opracowanie własne na podstawie bezpiecznewybory.pl

CZYNNIKI ZEWNĘTRZNE

Wybory, jako ważna część demokratycznego porządku prawnego, muszą być odpowiednio zabezpieczone przed szkodliwym oddziaływaniem czynników zewnętrznych. W trakcie procesu wyborczego informacja wyborcza i jej przepływ muszą być właściwie chronione, w szczególności przed ingerencją obcych państw silnych ekonomicznie lub militarnie. W literaturze przedmiotu jako główne zagrożenia mające wymierny wpływ na przepływ informacji w procesie wyborczym wskazano brak centralnych ośrodków władzy odpowiedzialnych za tę sferę bezpieczeństwa w państwie [Kuźniar 2012: 43–55], prowadzenie działań o charakterze asymetrycznym przez biedniejsze kraje [Urbanek 2013: 181–191; Liedel, Piasecka, Aleksandrowicz 2007: 210–243], występowanie nowych zagrożeń w formie cyberataków [Zakrzewska 2014: 156], a także ze strony organizacji międzynarodowych, w tym korporacji [Białoskórski 2010], nadto ze strony oponentów politycznych i różnych grup interesu, a także w postaci praktyk lobbystycznych[11]. Nieustannie zmieniające się uwarunkowania społeczno-polityczne na świecie determinują zatem konieczność rozważenia wprowadzenia strategicznego planowania opartego na stworzonej taktyce dostosowanej do aktualnych uwarunkowań bezpieczeństwa międzynarodowego [Banasik 2016: 364]. Zmiany polityczno-ustrojowe

[11] *EU vs DiSiNFO*, https://euvsdisinfo.eu/ – na portalu zawarto wiele ciekawych danych o działaniach dezinformacyjnych (dostęp 14.02.2022).

w Polsce i Europie Środkowo-Wschodniej z początku lat dziewięćdziesiątych XX w. spowodowały rozpad dwubiegunowego układu sił na świecie [Chrobak, Kubiński 2013: 250], co przez jakiś czas owocowało kooperacją – współpracą państw [Kośmider 2014: 28]. Obecnie odnotowuje się znaczący wzrost roli Chin w polaryzacji sił na świecie, obok tradycyjnie dominujących Stanów Zjednoczonych, przy znacznie mniejszym znaczeniu Europy oraz Rosji [Olszewski 2006: 123].

Ustalenia te wskazują, że w trakcie wyborów może dochodzić do pozyskiwania i wykorzystywania informacji przez zewnętrzne podmioty i organizacje (także terrorystyczne; walka z cyberterroryzmem jest nierozerwalnie związana z cywilizacją XXI w. [Jagusiak 2011: 266]) zainteresowane uzyskaniem wpływu na wynik wyborczy i rozstrzygnięcia polityczne w danym kraju, co stoi w sprzeczności z podstawowymi zasadami państwa prawa i jest zaprzeczeniem demokracji [Buczkowski 2012: 15–16].

Działalność Edwarda Snowdena pozwoliła na ujawnienie opinii publicznej skali istniejących zagrożeń związanych z przechowywaniem, zabezpieczaniem i przepływem informacji, które mogą być interesujące z punktu widzenia organów państwa, a zarazem zasygnalizowała rodzaje i intensywność ryzyka, jakie rodzi brak ochrony informacji. Oczywista stała się więc okoliczność, że jeżeli do tajnych danych ma dostęp osoba, która nie daje rękojmi przestrzegania ich poufności i wykonuje swoją pracę tymczasowo, to wzrasta ryzyko ujawnienia informacji osobom i instytucjom trzecim.

Wydarzenia w USA związane z działalnością E. Snowdena potwierdzają istnienie potrzeby podjęcia szczegółowych badań nad zasadami dostępu do informacji oraz bezpieczeństwem jej przepływu i przetwarzania, co wydaje się tym pilniejsze i bardziej istotne, jeśli zważyć na szczególny charakter informacji przekazywanych w toku wyborów i na fakt, że bezpośrednio oddziałują one na decyzje polityczne związane z kształtowaniem i składem organów władzy publicznej w państwie. Należy podkreślić zarówno publiczno-, jak i prywatnoprawny charakter wykorzystywanych w toku wyborów informacji. Wydaje się, że szczególne ryzyko dla bezpieczeństwa w czasie wyborów rodzi dostęp przedsiębiorstw prywatnych i ich pracowników do dokumentów niejawnych.

Zasadnicze dla prowadzonej analizy stają się nie tylko te wątki, które dotyczą treści informacji, ale także te dotyczące kręgu podmiotów, które uzyskują do nich dostęp. Nie mniej zatem ważne od zapewnienia bezpieczeństwa integralności informacji jest prawidłowe wyodrębnienie kręgu podmiotów, które stają się ich depozytariuszami.

Zapewnienie odpowiedniego, tj. neutralizującego ryzyko, ujawnienia informacji, jej zniekształcenia lub nieuprawnionego wykorzystania – poziomu bezpieczeństwa informacji wymaga przezorności i roztropności ze strony

autorów, wytwórców i dysponentów tychże informacji, których owe informacje bezpośrednio dotyczą. Krąg podmiotów zainteresowanych uzyskaniem dostępu do informacji oraz metody ich wykorzystania sygnalizują, że pozyskane informacje mogą być narzędziem używanym do walki politycznej w toku kampanii wyborczych, a także do uzyskiwania wpływu na kształtowanie sceny politycznej przez te podmioty, które znajdą się w ich posiadaniu. Należy bowiem zwrócić uwagę, że firmy o ogromnym potencjale, jak: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube i Apple, udostępniają swoje serwery i zasoby informacyjne zarówno podmiotom publicznym, np. National Security Agency, jak i prywatnym. Dzięki dostępowi do tych zasobów NSA i inne podmioty mogą uzyskać faktyczny dostęp do danych klientów i osób korzystających z programów czy aplikacji należących do tych przedsiębiorstw i korporacji finansowych.

W istocie zatem ryzyko dotyczące zapewnienia bezpieczeństwa informacji w toku wyborów związane jest z ustaleniem poziomu zaufania do organizacji finansowej jako dysponenta danych o osobach. Do zagadnień wymagających na pewno rozstrzygnięcia, które jednak nie stanowi zasadniczego celu niniejszej pracy, należy ustalenie zakresu i rodzaju informacji o obywatelach, które znajdują się w posiadaniu korporacji finansowych. Zagrożeniem dla bezpieczeństwa przepływu informacji nie jest więc działanie ze strony organów państwa, lecz brak takiego działania wówczas, gdy dysponentem informacji o obywatelach stają się podmioty prywatne realizujące cele inne niż te związane z zapewnieniem bezpieczeństwa państwa. Warto podkreślić, że w Polsce zadania informacyjne służące ochronie oraz propagowaniu krajowych interesów, ale także informacyjnemu osłabianiu przeciwnika, są realizowane w szczególności przez niemilitarne struktury obronne państwa [Kuliczkowski 2013: 196].

Rewolucja naukowo-informacyjna zmieniła najważniejsze cele konfliktów [Kuliczkowski 2016: 10], dlatego wśród zagrożeń zewnętrznych, w tym międzynarodowych [Czaputowicz 2010: 13–15], warto wskazać zwłaszcza poczynania hakerów [Doroziński 2001: 28–33; Biernacik, Kalman 2016: 122–146] oraz służb informatycznych [Herman 2002: 35–43; Natorska 2014: 84–92] różnych państw (w szczególności Rosji, która ma potencjał destabilizujący najbliższe kraje) [Czajkowski 2010: 106–108]. Zapewnienie bezpieczeństwa w cyberprzestrzeni jest też bardzo ważnym zadaniem dla NATO [Grenda 2016: 177–190], w tym na tzw. wschodniej flance[12].

W związku z wyborami do Parlamentu Europejskiego w 2019 r. Szymon Palczewski wskazał, że „rosyjscy cyberprzestępcy rozpoczęli nową kampanię

[12] *Wyzwania cyberbezpieczeństwa na wschodniej flance NATO*, https://www.cyberdefence24.pl/wyzwania-cyberbezpieczenstwa-na-wschodniej-flance-nato-analiza (dostęp 24.01.2022).

hakerską, której celem są europejskie instytucje rządowe. Jak informuje firma FireEye, główną metodą działania hakerów jest spear phishing" [Palczewski 2019b][13]. Celem grup hakerskich jest próba uzyskiwania dostępu do sieci w celu zebrania informacji i przygotowania wycieku danych [Palczewski 2019b][14]. W 2018 r. w niemieckich mediach pojawiła się informacja o ujawnieniu wewnętrznych dokumentów partii oraz danych osobowych polityków za pośrednictwem Twittera. Incydent objął wszystkie ugrupowania Bundestagu poza skrajnie prawicową Alternatywą dla Niemiec (AfD) [Palczewski 2019a][15]. Natomiast wcześniejsze incydenty wyborcze podczas elekcji prezydenckiej w Stanach Zjednoczonych w 2016 r. zostały przez Prokuratora Generalnego USA na podstawie raportu Roberta S. Muellera[16] uznane za nieprzedstawiające dowodów na zmowę między sztabem kandydata w wyborach Donalda Trumpa a Rosją[17].

ZAKOŃCZENIE

Współczesne zakłócenia procesu wyborczego, zarówno wewnętrzne, jak i zewnętrzne stanowią poważne zagrożenie funkcjonowania demokratycznych państw, w tym także ich suwerenności. W dużej mierze zagrożeniem są działania lub ich brak, mające charakter informatyczny.

Ciekawym rozwiązaniem, które ma zapewnić cyberbezpieczeństwo wyborów, jest np. opracowanie i wdrożenie przez Defense Advanced Research Projects Agency[18] systemu, który po pierwsze, byłby odporny na wielowątkową działalność hakerów, po drugie, umożliwiałby sprawdzenie przez wyborców,

[13] *Rosyjscy hakerzy w gotowości. Eurowybory zagrożone?*, https://www.cyberdefence24.pl/rosyjscy-hakerzy-w-gotowosci-eurowybory-zagrozone (dostęp 22.01.2022); przez pojęcie *spear phishing* należy rozumieć spersonalizowany atak na użytkownika Internetu, poprzedzony z reguły pogłębionym wywiadem środowiskowym prowadzonym w sieci.

[14] *Rosyjscy hakerzy w gotowości…*

[15] *Największy cyberatak w historii Niemiec. Bezpieczna tylko skrajna prawica*, https://www.cyberdefence24.pl/dane-niemieckich-politykow-w-sieci-bezpieczna-tylko-skrajna-prawica (dostęp 24.01.2022).

[16] *Report On The Investigation Into Russian Interference In The 2016 Presidential Election Volume I of II Special Counsel Robert S. Mueller, III*, Washington 2019, https://cdn.cnn.com/cnn/2019/images/04/18/mueller-report-searchable.pdf (dostęp 24.01.2022).

[17] *Prokurator generalny USA: raport Muellera nie przedstawia dowodów na zmowę między sztabem Trumpa a Rosją, 24.03.2019 r.*, https://wiadomosci.onet.pl/swiat/prokurator-generalny-usa-raport-muellera-nie-przedstawia-dowodow-na-zmowe-miedzy/v61myml (dostęp 27.01.2022).

[18] DARPA – amerykańska agencja rządowa zajmująca się rozwojem technologii wojskowej, działająca w strukturach Departamentu Obrony.

czy ich głosy są w nim poprawnie zarejestrowane [Palczewski 2019c][19]. Innym ważnym problemem jest niezawodne działanie systemów informatycznych w trakcie wyborów – np. podczas polskich wyborów samorządowych w 2018 r. awarii uległa usługa Elektronicznej Skrzynki Podawczej (e-PUAP), co wielu wyborcom uniemożliwiło sprawne głosowanie [Suchorabski 2018][20]. Jednocześnie należy podkreślić, że Państwowa Komisja Wyborcza z wyprzedzeniem informowała o zagrożeniach odnoszących się do wyborów poprzez wiele komunikatów i ostrzeżeń[21], czego przykładem jest np. stanowisko PKW w sprawie materiałów wyborczych mogących wprowadzać wyborców w błąd[22]. Stanowisko dotyczyło pojawiających się sformułowań sugerujących, że konkretny sposób głosowania jest prawidłowy, jak choćby: „Jeżeli chcecie Państwo wybrać […], proszę postawić X w «okienku» przy jego imieniu i nazwisku […], jeżeli ktoś zaznaczy X przy innym nazwisku na karcie wyborczej, karta zostanie uznana za nieważną"[23]. Ostatecznie można wnioskować, że dopiero odpowiednie w sensie organizacyjnym, technicznym (cyberbezpieczeństwo) i prawnym zorganizowanie procesu wyborczego oraz przeciwdziałanie jego zakłóceniom może przynieść pożądane efekty.

BIBLIOGRAFIA

Banasik Mirosław. 2016. *Planowanie strategiczne bezpieczeństwa narodowego. Wybrane problemy*. Toruń: Wydawnictwo Adam Marszałek.

Białoskórski Robert. 2010. *Wyzwania i zagrożenia bezpieczeństwa XXI wieku*. Warszawa: Wyższa Szkoła Cła i Logistyki w Warszawie.

[19] *Wybory staną się w pełni bezpieczne. Specjaliści tworzą innowacyjny system*, https://www.cyberdefence24.pl/wybory-stana-sie-w-pelni-bezpieczne-specjalisci-tworza-innowacyjny-system (dostęp 24.01.2022).

[20] *Problemy z głosowaniem: Obywatele korzystający z ePUAP nie zostali dopisani do rejestru*, https://serwisy.gazetaprawna.pl/samorzad/artykuly/1312309,wybory-samorzadowe-2018-brak-nazwiska-w-rejestrze-epuap.html (dostęp 25.01.2022).

[21] Por. np. komunikat *PKW nie patronuje stronom www zbierającym dane osobowe kandydatów na członków komisji wyborczych*, https://pkw.gov.pl/337_Informacje/1/33870_PKW_nie_patronuje_stronom_www_zbierajacym_dane_osobowe_kandydatow_na_czlonkow_komisji_wyborczych (dostęp 24.01.2022).

[22] *Stanowisko Państwowej Komisji Wyborczej z dnia 8 października 2018 r. w sprawie materiałów wyborczych mogących wprowadzać wyborców w błąd*, https://pkw.gov.pl/345_Wyjasnienia_stanowiska_komunikaty/1/29858_Stanowisko_Panstwowej_Komisji_Wyborczej_z_dnia_8_pazdziernika_2018_r_w_sprawie_materialow_wyborczych_mogacych_wprowadzac_wyborcow_w_blad (dostęp 24.01.2022).

[23] *Ibidem*.

Bień-Kacała Agnieszka, Jirásek Jiří, Cibulka Ľubor, Drinóczi Tímea (red.). 2016. *Kategoria bezpieczeństwa w regulacjach konstytucyjnych i praktyce ustrojowej państw Grupy Wyszehradzkiej*. Toruń: Wydawnictwo Uniwersytetu Mikołaja Kopernika w Toruniu.

Biernacik Bartosz, Kalman Leszek. 2016. *Systemy i sieci teleinformatyczne Sił Zbrojnych Rzeczypospolitej Polskiej – wielorakie aspekty bezpieczeństwa cyberprzestrzeni*. Warszawa: Akademia Sztuki Wojennej.

Buczkowski Jerzy. 2012. *Zasady naczelne Konstytucji Rzeczypospolitej Polskiej.* W *Prawo konstytucyjne RP (instytucje wybrane)*. Red. Jerzy Buczkowski. Przemyśl–Rzeszów: Wyższa Szkoła Prawa i Administracji.

Chrobak Ryszard, Kubiński Marek. 2013. „Zagrożenia bezpieczeństwa państwa". *Zeszyty Naukowe AON* 4.

Czajkowski Marek. 2010. *Uwarunkowania polityki zagranicznej i bezpieczeństwa Federacji Rosyjskiej.* W *Międzynarodowe wyzwania bezpieczeństwa*. Red. Klemens Budzowski. Kraków: Oficyna Wydawnicza AFM.

Czaputowicz Jacek. 2010. *Kryteria bezpieczeństwa międzynarodowego państwa – aspekty teoretyczne.* W *Kryteria bezpieczeństwa międzynarodowego państwa*. Red. Sławomir Dębski, Beata Górka-Winter. Warszawa: Polski Instytut Spraw Międzynarodowych.

Cziomer Erhard. 2010. *Instytucjonalizacja współpracy transatlantyckiej: problemy i wyzwania*. W *Bezpieczeństwo międzynarodowe w XXI wieku. Wybrane problemy*. Red. Erhar Cziomer. Kraków: Oficyna Wydawnicza AFM.

Doroziński Dariusz. 2011. *Hakerzy. Technoanarchiści przestrzeni*. Gliwice: Helion.

Grenda Bogdan. 2016. *Obrona cyberprzestrzeni NATO*. W *Zarządzanie bezpieczeństwem danych*. Red. Remigiusz Wiśniewski, Kazimierz Waluch. Płock: Oficyna Wydawnicza Szkoły Wyższej im. Pawła Włodkowica NOVUM.

Herman Michael. 2002. *Potęga wywiadu*. Warszawa: Bellona.

Hypś Sławomir. 2014. *Granice odpowiedzialności funkcjonariusza publicznego za przestępstwa korupcyjne w świetle orzecznictwa sądowego.* W *Rola organów bezpieczeństwa publicznego w przeciwdziałaniu przestępczości: zagadnienia wybrane*. Red. Sławomir Hypś, Konrad Kołek. Lublin: KUL.

Jagusiak Bogusław. 2011. „Wpływ zagrożeń terrorystycznych na bezpieczeństwo międzynarodowe". *Studia bezpieczeństwa narodowego National Security Studies* 1 (2).

Kośmider Tomasz. 2014. „Kulturowy wymiar bezpieczeństwa państwa polskiego – wyzwania i zagrożenia". *Rozprawy Społeczne* 1 (8).

Kuliczkowski Marian. 2013. „Przygotowania obronne państwa w systemie bezpieczeństwa narodowego RP – podział i charakterystyka zadań obronnych". *Zeszyty Naukowe AON* 4.

Kuliczkowski Marian. 2016. *Pozamilitarne przygotowania obronne w Polsce. Próba systematyzacji procesualnych oraz funkcjonalnych aspektów przygotowań*. Warszawa: Akademia Sztuki Wojennej.

Kuźniar Roman. 2012. *Tradycyjne zagrożenia dla bezpieczeństwa międzynarodowego*. W *Bezpieczeństwo międzynarodowe.* Red. Roman Kuźniar i in. Warszawa: Wydawnictwo Naukowe Scholar.

Letkiewicz Arkadiusz. 2013. *Korupcja – społeczne zagrożenie bezpieczeństwa RP*. W *Nauka o bezpieczeństwie: istota, przedmiot badań i kierunki rozwoju*. T. 2. Red. Leszek Grochowski, Arkadiusz Letkiewicz, Andrzej Misiuk. Szczytno: Wyższa Szkoła Policji w Szczytnie.

Liedel Krzysztof, Piasecka Paulina, Aleksandrowicz Tomasz (red.). 2011. *Bezpieczeństwo w XXI wieku: asymetryczny świat*. Warszawa: Difin.

Madej Marek. 2007. *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego.* Warszawa: Polski Instytut Spraw Międzynarodowych.

Marszałek Maciej, Denysiuk Irmina. 2013. „Elementy wsparcia procesu stabilizacji i odbudowy państwa". *Zeszyty Naukowe AON* 4.
Natorska Katarzyna. 2014. *Bezpieczeństwo informacyjne a służby specjalne.* W *Bezpieczeństwo narodowe i międzynarodowe wobec wyzwań współczesnego świata.* Red. Waldemar Kitler, Maciej Marszałek. Warszawa: AON.
Olszewski Ryszard. 2006. *Bezpieczeństwo współczesnego świata*. Toruń: Wydawnictwo Adam Marszałek.
Rychard Andrzej. 2015. *Wprowadzenie.* W *Co się stało 16 listopada?* Red. Joanna Załuska. Warszawa: Fundacja im. Stefana Batorego.
Shukuralieva Nartsiss. 2011. *The People and Its Leader: The cultural images of political events in Kyrgyzstan*. W *Porządek prawno-społeczny a problemy współczesnego świata*. Red. Sławomir Dąbrowa, Michał Czakowski. Bydgoszcz: Kujawsko-Pomorska Szkoła Wyższa w Bydgoszczy.
Urbanek Andrzej. 2013. *Zagrożenia asymetryczne czy asymetryczność zagrożeń.* W *Edukacja dla bezpieczeństwa: wyzwania i zagrożenia w XXI wieku. Aspekty militarne i niemilitarne*. Red. Mirosław Borkowski, Margot Stańczyk-Minikiewicz, Ilona Ziemkiewicz-Gawlik. Poznań: Wyższa Szkoła Bezpieczeństwa.
Wrzalik Magdalena. 2015. „Instytucja mężów zaufania w polskim prawie wyborczym". *Zeszyt Studencki Kół Naukowych Wydziału Prawa i Administracji UAM* 5.
Zakrzewska Janina. 2014. *Bezpieczeństwo narodowe – 15 lat w NATO.* Tom I. Warszawa: Biuro Bezpieczeństwa Narodowego.

AKTY NORMATYWNE

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. 2021 poz. 2345 ze zm.).
Ustawa z dnia 5 stycznia 2011 r. Kodeks wyborczy (t.j. Dz. U. 2020 poz. 1319 ze zm.).
Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. poz. 1129 ze zm.).

ŹRÓDŁA INTERNETOWE

EU vs DiSiNFO, https://euvsdisinfo.eu/
Małecki-Tepicht Łukasz. 2014. *Po wyborach samorządowych 2014 roku – o efektywności i przejrzystości procesu wyborczego*, http://www.obserwatorkonstytucyjny.pl/artykul/po-wyborach-samorzadowych-2014-roku-o-efektywnosci-i-przejrzystosci-procesu-wyborczego/ (dostęp 6.01.2022).
Palczewski Szymon. 2019a. *Największy cyberatak w historii Niemiec. Bezpieczna tylko skrajna prawica*, https://www.cyberdefence24.pl/dane-niemieckich-politykow-w-sieci-bezpieczna-tylko-skrajna-prawica (dostęp 24.01.2022).
Palczewski Szymon. 2019b. *Rosyjscy hakerzy w gotowości. Eurowybory zagrożone?*, https://www.cyberdefence24.pl/rosyjscy-hakerzy-w-gotowosci-eurowybory-zagrozone (dostęp 22.01.2022).
Palczewski Szymon. 2019c. *Wybory staną się w pełni bezpieczne. Specjaliści tworzą innowacyjny system*, https://www.cyberdefence24.pl/wybory-stana-sie-w-pelni-bezpieczne-specjalisci-tworza-innowacyjny-system (dostęp 24.01.2022).
PKW kupiła system za 429 tysięcy złotych, który nie działa. Firma miała zbyt mało czasu?, http://www.gazetaprawna.pl/artykuly/835823,pkw-kupila-system-za-429-tysiecy-zlotych-ktory-nie-dziala-firma-miala-zbyt-malo-czasu.html (dostęp 4.01.2022).

PKW nie patronuje stronom www zbierającym dane osobowe kandydatów na członków komisji wyborczych, https://pkw.gov.pl/337_Informacje/1/33870_PKW_nie_patronuje_stronom_www_zbierajacym_dane_osobowe_kandydatow_na_czlonkow_komisji_wyborczych (dostęp 24.01.2022).

PKW ogłosiła oficjalne wyniki II tury wyborów i podała się do dymisji, 1.12.2014 r., https://wiadomosci.dziennik.pl/wybory-samorzadowe/artykuly/476708,wybory-2014-wyniki-ii-tury-dymisja-pkw.html (dostęp 4.01.2022).

PKW podała się do dymisji, http://www.gazetaprawna.pl/artykuly/838927,pkw-podala-sie-do-dymisji.html (dostęp 4.01.2022).

Prokurator generalny USA: raport Muellera nie przedstawia dowodów na zmowę między sztabem Trumpa a Rosją, 24.03.2019 r., https://wiadomosci.onet.pl/swiat/prokurator-generalny-usa-raport-muellera-nie-przedstawia-dowodow-na-zmowe-miedzy/v61myml (dostęp 27.01.2022).

Report On The Investigation Into Russian Interference In The 2016 Presidential Election Volume I of II Special Counsel Robert S. Mueller, III, Washington 2019, https://cdn.cnn.com/cnn/2019/images/04/18/mueller-report-searchable.pdf (dostęp 24.01.2022).

Stanowisko Państwowej Komisji Wyborczej z dnia 8 października 2018 r. w sprawie materiałów wyborczych mogących wprowadzać wyborców w błąd, https://pkw.gov.pl/345_Wyjasnienia_stanowiska_komunikaty/1/29858_Stanowisko_Panstwowej_Komisji_Wyborczej_z_dnia_8_pazdziernika_2018_r_w_sprawie_materialow_wyborczych_mogacych_wprowadzac_wyborcow_w_blad (dostęp 24.01.2022).

Suchorabski Maciej. 2018. *Problemy z głosowaniem: Obywatele korzystający z ePUAP nie zostali dopisani do rejestru*, https://serwisy.gazetaprawna.pl/samorzad/artykuly/1312309,wybory-samorzadowe-2018-brak-nazwiska-w-rejestrze-epuap.html (dostęp 25.01.2022).

Wybory samorządowe: W lokalach wyborczych nie będzie kamer, https://www.rp.pl/Wybory-samorzadowe/180529360-Wybory-samorzadowe-W-lokalach-wyborczych-nie-bedzie-kamer.html (dostęp 14.01.2022).

Wyzwania cyberbezpieczeństwa na wschodniej flance NATO, https://www.cyberdefence24.pl/wyzwania-cyberbezpieczenstwa-na-wschodniej-flance-nato-analiza (dostęp 24.01.2022).

INNE ŹRÓDŁA

NIK, Wystąpienie pokontrolne, druk KBF – 4114-004-01/2014, I/14/006, Warszawa 2014.

Streszczenie

Bezpieczeństwo każdego państwa związane jest z zapewnieniem ograniczenia dostępu do pewnych informacji istotnych dla jego funkcjonowania. Dlatego też tworzone są systemy ochrony informacji. We współczesnym świecie, w XXI w., informacja towarzyszy człowiekowi na każdym etapie jego aktywności czy to o charakterze zawodowym, czy prywatnym. Informacja podlega przetwarzaniu oraz utrwalaniu w różnorodnych formach, począwszy od formy ustnej, przez pisemną w tradycyjnym wymiarze, po zastosowanie środków elektronicznych. Do nadrzędnych celów państwa należy zatem zaliczyć zapewnienie należytej ochrony informacji, tj. bezpieczeństwa informacji.

Słowa kluczowe: informacja, przestępstwa, wybory

DISRUPTIONS IN THE FLOW OF INFORMATION AND INCIDENTS IN THE ELECTION PROCESS (summary)

The security of each country is related to ensuring that access to certain information essential for its functioning is limited. Therefore, information protection systems are created. In the modern world, in 21st century, information accompanies man at every stage of his activity, be it of a professional or private nature. Information is processed and recorded in various forms, ranging from oral, written in the traditional dimension, to the form using electronic means. Therefore, the overriding objectives of the state include ensuring adequate protection of information, i.e. information security.

Keywords: information, crimes, election