Nowoczesne Systemy Zarządzania
Zeszyt 14 (2019), nr 3 (lipiec-wrzesień)
ISSN 1896-9380, s. 45-56

Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Modern Management Systems
Volume 14 (2019), No. 3 (July-September)
ISSN 1896-9380, pp. 45-56

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology

Narzędzia i techniki bezpiecznej wymiany informacji w zarządzaniu – studium przypadku

Tools and methods for secure exchange of information in management – case study

Michał Jurek
Wojskowa Akademia Techniczna
Wydział Bezpieczeństwa, Logistyki i Zarządzania

Piotr Zaskórski
Wojskowa Akademia Techniczna
Wydział Bezpieczeństwa, Logistyki i Zarządzania

Abstrakt. Celem artykułu jest pokazanie, jak nowoczesne technologie mogą wpływać na zapewnianie bezpieczeństwa informacji oraz na sposób wykorzystania związanych z tym mechanizmów w procesie dydaktycznym. Przedstawione w publikacji koncepcje można dostosować do podmiotów działających zarówno w sferze prywatnej, jak i w administracji publicznej. Prezentowane w pracy podstawy technologii *blockchain* pokazują możliwości praktycznego jej zastosowania w kontekście zapewniania informacyjnej ciągłości działania współczesnej organizacji.
Słowa kluczowe: zarządzanie, bezpieczeństwo, edukacja, *blockchain*, nowe technologie.

Abstract. The purpose of this article is to show, how modern technologies could influence the didactic process and information security. The concepts presented in it, could be adapted to entities operating in the private sphere or public administration. It presents the basics of blockchain technology. It exemplify the possibility of its practical application as a warrantor of information continuity.
Keywords: management, security, education, blockchain, new technologies.

Wstęp

Nowoczesne rozwiązania techniczno-technologiczne wymuszają na użytkownikach systemów, w tym na organizacjach prywatnych i publicznych, stosowanie

narzędzi, których zadaniem jest usprawnianie funkcjonowania działalności każdej organizacji. Warunkiem skutecznego ich wykorzystania jest odpowiednio przygotowany i przeprowadzony proces implementacji. Proces ten musi być realizowany stopniowo z pełnym zaangażowaniem wszystkich zainteresowanych użytkowników końcowych wdrażanego rozwiązania.

Jednym z ważniejszych etapów wprowadzania do użytku nowych rozwiązań jest proces edukacyjny, który stanowi nieodzowną część całego systemu adaptacji. Proces ten może być postrzegany w wąskim oraz szerokim zakresie. W pierwszym przypadku wiąże się to z przeprowadzaniem różnego rodzaju szkoleń, których wyniki wpływają jedynie na środowisko lokalne (np. daną firmę), w drugim zaś jego rezultaty rzutują na całokształt współdziałającego z daną organizacją otoczenia. Wpływ ten potęgowany jest przez bogate spektrum modeli i metod telekomunikacji, które po upowszechnieniu się zaczęły być używane nie tylko do komunikowania się wewnątrz organizacji, lecz także z klientem/odbiorcą usług. Ich wykorzystanie zapobiega również ograniczeniom związanym z dyslokacją przedsiębiorstwa.

Użycie nowoczesnych metod komunikacji oraz przetwarzania informacji może prowadzić do powstawania kryzysu zaufania (pewności działania) wśród uczestników (komponentów) sieci (klientów oraz serwera). Z powodu braku odpowiednich środków zaradczych utrata tej cechy może spowodować wystąpienie strat o znacznych rozmiarach. Problem minimalizacji poziomu ograniczonego zaufania może zostać rozwiązany dzięki wprowadzeniu jednolitego kanału komunikacji bazującego na technologii *blockchain*. W trakcie projektowania i implementacji tego rozwiązania należy zwrócić szczególną uwagę na już istniejące możliwości. Dobrym wzorcem projektowym może być narzędzie o nazwie X-Road wprowadzone przez rząd estoński (e-estonia, 2018). Rozwiązanie to integruje wszystkie e-usługi oferowane przez podmioty administracji publicznej oraz sektora prywatnego, tak aby wszyscy uprawnieni użytkownicy posiadali zawsze te same, aktualne dane, z zapewnieniem ich autentyczności i wiarygodności dzięki wprowadzeniu weryfikacji informacji za pomocą technologii łańcucha bloków.

Celem niniejszej pracy jest wskazanie, jak nowe technologie mogą wpływać na zapewnianie bezpieczeństwa informacji oraz w jaki sposób mogą być wykorzystywane w procesie dydaktycznym (tj. kształcenia użytkowników), który jest jednym z czynników wspierających zarządzanie. Do realizacji założonego celu wykonana została kwerenda literatury przedmiotu oraz zaprezentowane zostały rozwiązania wykorzystywane przez różne organizacje i instytucje. Na tej podstawie została podjęta próba wykazania, że nowoczesne technologie są istotnym czynnikiem wpływającym na bezpieczeństwo informacji. Pomimo rozległego spektrum problematyki związanej z bezpieczeństwem informacji, również w procesach edukacyjnych, niniejsza publikacja skupia się na kwestii zapewniania bezpieczeństwa informacji przez tzw. zwykłego użytkownika.

1. Wymagania współczesnego procesu edukacyjnego

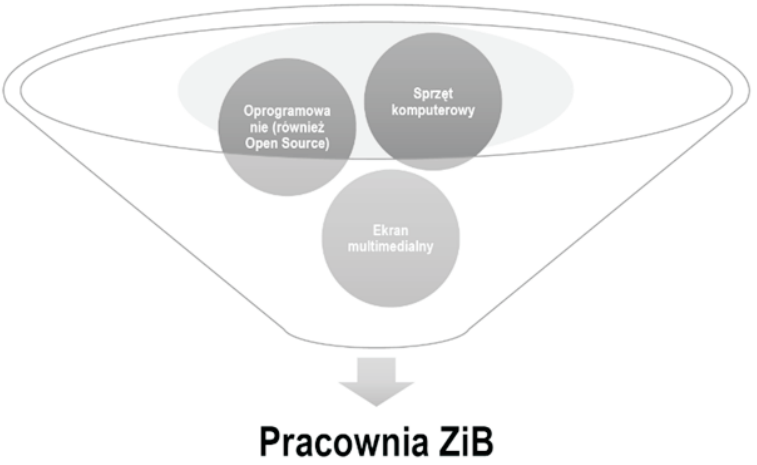
Użytkując oraz wprowadzając do użytku nowe technologie, zawsze należy mieć na uwadze stan wiedzy osób, które są/zostaną wyznaczone do ich obsługi. Niedostateczne umiejętności użytkowników mogą implikować nieakceptowalny poziom ryzyka. Mogą zatem wystąpić realne zagrożenia, które mogą niekorzystnie wpłynąć na działanie całego systemu informacyjnego i całej organizacji. To zjawisko ilustruje rysunek 1.

Rys. 1. Poziom wiedzy a zagrożenie
Źródło: opracowanie własne

Zagrożenia te mogą pochodzić zarówno ze źródeł zewnętrznych, jak i wewnętrznych. Pierwsze z nich będą wynikać z braku wiedzy użytkownika na temat niebezpieczeństw pochodzących z ogólnie rozumianej sieci, jaką jest Internet, takich jak ataki typu *phishing*, *spoofing* czy *DoS* (*Denial of Service*). Druga z wymienionych kategorii zagrożeń będzie miała związek z samym użytkowaniem systemu oraz jego nieumiejętną konfiguracją. Z powodu braku zmiany ustawień domyślnych urządzeń lub oprogramowania wchodzącego w skład danej konfiguracji istnieje prawdopodobieństwo pozyskania danych wrażliwych, które mogą zostać użyte do przeprowadzenia ataku zewnętrznego (w innym lub w tym samym podmiocie) albo wewnętrznego (pozyskanie danych wrażliwych/krytycznych z innego obszaru odpowiedzialności/kompetencji dziedzinowych).

Wskazane zagrożenia mogą mieć również wpływ na sam sposób realizacji procesu dydaktycznego, który w obecnych czasach jest w dużym stopniu wspierany przez nowoczesne rozwiązania multimedialne. Szczególny nacisk na rozwój umiejętności oraz kompetencji cyfrowych powinien być eksponowany w sektorze szkolnictwa wyższego, który przygotowuje przyszłe kadry pracownicze, naukowo-dydaktyczne

do funkcjonowania w warunkach postępującej cyfryzacji działalności człowieka. Odpowiedzią na to wyzwanie może być powołanie do życia odpowiednio wyposażonych laboratoriów (pracowni), których zadaniem będzie poszerzanie wiedzy oraz praktycznych umiejętności w tym względzie (zob. rys. 2).



Rys. 2. Główne komponenty Pracowni Zarządzania i Bezpieczeństwa Wydziału Cybernetyki WAT
Źródło: opracowanie własne

Aby sprostać wymaganiom stawianym przez potencjalnych użytkowników (dziś studentów) oraz nowoczesne technologie, na Wydziale Cybernetyki Wojskowej Akademii Technicznej, w ramach Instytutu Organizacji i Zarządzania, powołano do życia Pracownię Zarządzania i Bezpieczeństwa. Jej głównym celem jest podnoszenie umiejętności i kwalifikacji w zakresie technologii cyfrowych wszystkich zainteresowanych oraz przygotowanie kadr o odpowiednim poziomie kultury cyfrowej. Dotyczy to więc specjalistów z obszaru nauk społecznych, ze szczególnym uwzględnieniem nowoczesnych strategii oraz metod zarządzania w sytuacjach kryzysowych. Wykorzystanie dostępnych i wciąż wzbogacanych zasobów oraz narzędzi pozwala na przemodelowanie procesu kształcenia i działalności dydaktycznej w obszarze nauk o zarządzaniu i nauk o bezpieczeństwie, a także na prowadzenie prac naukowo-badawczych.

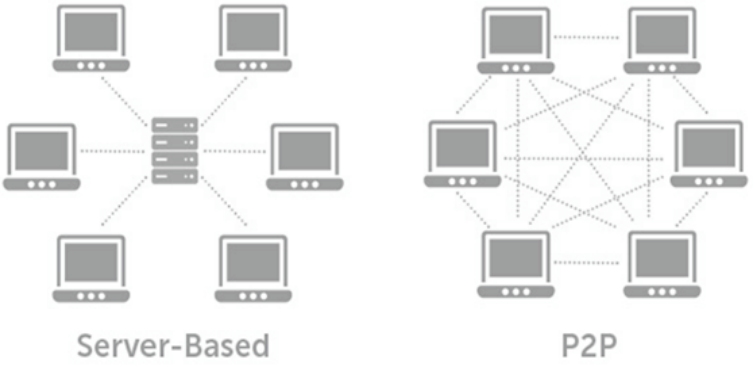
2. Istota funkcjonalności blockchain

Technologia *blockchain* jest pewnym modelem wzmacniającym zaufanie do autentyczności i wiarygodności danych. Technologia ta bazuje na ułożonych (w modelu łańcucha) następujących po sobie bloków danych (Biedrzycki, 2016a).

Każdy z nich ma ograniczoną pojemność zapisanych danych. Po jej zapełnieniu tworzy się nowy blok, który dodawany jest na początek kolejki. Wykorzystywana jest zatem *de facto* jakby globalna księga rachunkowa, która zawiera w sobie dane na temat przeprowadzonych transakcji (Biedrzycki, 2016b), przy czym pojęcie „transakcji" ma szerokie znaczenie i może odnosić się nie tylko do przepływu środków finansowych, lecz także przepływu innych zasobów, a w tym m.in.:

- podpisu cyfrowego;
- uwierzytelniania dokumentów;
- monitorowania stanu zasobów.

Można więc zauważyć, że zależnie od kontekstu użycia tej technologii będzie zmieniać się przeznaczenie rejestru (artefaktów, transakcji itp.) (Mougayar, Buterin, 2019).



Rys. 3. Różnica między działaniem sieci P2P a centralnie zarządzanej
Źródło: opracowanie na podstawie (Wowza, 2018)

Za bezpieczeństwo danych odpowiadają narzędzia kryptograficzne oraz decentralizacja składowania informacji o transakcjach. Rozproszenie sieci jest następstwem modelu komunikacji P2P (*Peer-to-Peer*). Model ten pozwala na bezpośrednią wymianę danych pomiędzy użytkownikami z ominięciem serwera centralnego jako „instytucji" zaufania publicznego, która poddaje weryfikacji przeprowadzane operacje (zob. rys. 3). Wykorzystanie tego modelu komunikacji zapewnia bezpośredni dostęp do księgi transakcji wszystkim zainteresowanym podmiotom. Przekłada się to na brak możliwości sfałszowania wprowadzonych zapisów, gdyż nieautoryzowana próba zmiany jednego z bloków zostanie odrzucona przez pozostałych użytkowników systemu.

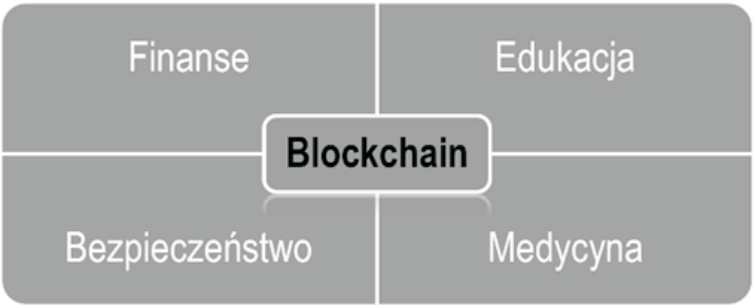
Obecnie technologia *blockchain* może mieć zastosowanie w czterech głównych obszarach działalności państwa (przedsiębiorstwa)(zob. rys. 4). Z racji ograniczonych w tym zakresie doświadczeń (powstała w roku 2008) sposoby jej wykorzystania ciągle są w fazie projektowania/rozwoju. Należy jednak spodziewać się, że z największym

przyrostem nowych rozwiązań będziemy mieli do czynienia w sektorze finansów (Dihillon, Metcalf, Hooper, 2018, s. 244-247).

Jedynym ograniczeniem wdrożenia tej technologii na szeroką skalę okazuje się moc obliczeniowa potrzebna do weryfikacji transakcji. Ze względu na złożoność przeprowadzanych obliczeń, by zapewnić odpowiednią wydajność (przepustowość), należy dobrać odpowiednie rozwiązania techniczne, w których można wyróżnić rozwiązania jednostkowe i grupowe.

Do sposobów indywidualnych można zaliczyć przeprowadzenie obliczeń za pomocą (Dihillon, Metcalf, Hooper, 2018, s. 31):

- **mikroprocesora (CPU)** – najstarszy, najmniej wydajny i zarazem najprostszy sposób weryfikacji transakcji;
- **karty graficznej (GPU)** – najodpowiedniejsza i najbardziej rozpowszechniona metoda wśród użytkowników domowych;
- **programowalnych macierzy bramek oraz układów specjalizowanych (FPGA, ASIC)** – nowoczesny i ciągle rozwijany sposób na budowę wysoko wydajnych oraz nisko kosztowych urządzeń do przeprowadzania zaawansowanych obliczeń.



Rys. 4. Przykładowe obszary wykorzystania technologii łańcucha bloków
Źródło: opracowanie własne na podstawie (Dihillon, Metcalf, Hooper, 2018, s. 6-8)

Techniki grupowe opierają się na połączeniu sposobów indywidualnych w sprzężone ze sobą sieci mogące funkcjonować jako swoistego rodzaju spółdzielnie, których moc obliczeniowa jest sumowana i wykorzystywana we wspólnym działaniu. Mogą to być również usługi bazujące na rozwiązaniach CC (*Cloud Computing*), których celem jest udostępnianie konkretnej mocy obliczeniowej do danego celu. Odbywa się to na podstawie umowy na czas określony oraz ustalonej ceny (Dihillon, Metcalf, Hooper, 2018, s. 31-32).

3. Informacyjna ciągłość działania

Ciągłość działania organizacji, czyli zapewnianie dostępu do krytycznych usług i funkcji w razie wystąpienia sytuacji kryzysowej, w dobie społeczeństwa informacyjnego można oprzeć na następujących filarach:

- bezpieczeństwo informacji;
- bezpieczeństwo teleinformatyczne;
- bezpieczeństwo infrastruktury krytycznej.

Bezpieczeństwo informacji możemy określić jako pewien poziom (ustalony np. dzięki przeprowadzonej analizie ryzyka) zaufania co do braku strat w wyniku nieuprawnionego dostępu do informacji (Zaskórski, Zaskórski, 2017, s. 71).

Bezpieczeństwo teleinformatyczne zaś możemy definiować jako bezpieczeństwo informacji w odniesieniu do danych, które są przechowywane, przetwarzane oraz przesyłane za pomocą systemów teleinformatycznych (Zaskórski, Zaskórski, 2017, s. 71). Można zatem zauważyć, że bezpieczeństwo teleinformatyczne jest podzbiorem bezpieczeństwa informacji (zob. rys. 5).

Rys. 5. Bezpieczeństwo informacji a bezpieczeństwo teleinformatyczne
Źródło: opracowanie własne

Z kolei **bezpieczeństwo infrastruktury** (jej ochrona) zostało opisane w ustawie regulującej zasady zarządzania kryzysowego. Ochrona infrastruktury krytycznej to zbiór działań, których celem jest zapewnienie funkcjonalności, ciągłości działania oraz integralności infrastruktury krytycznej, by zapobiegać zagrożeniom oraz niwelować ich skutki dla szybkiego jej odtworzenia (DzU 2007 nr 89, poz. 590 ze zm.).

W przypadku wystąpienia sytuacji kryzysowej zapewnianie ciągłości działania można tlumaczyć jako niezakłócony przebieg akcji zapobiegawczej (np. ratunkowej). W trakcie jej przeprowadzania należy zwrócić szczególną uwagę na aspekt przepływu informacji pomiędzy podmiotami, które są w nią zaangażowane. Zakłócenia mogą być spowodowane m.in.:

- ingerencją osób trzecich – celowe działanie zmierzające do przerwania komunikacji (np. atak terrorystyczny);
- uszkodzeniami sprzętu – celowe (sabotaż) lub niecelowe (zużycie sprzętu);
- błędami ludzkimi – powodowane zmęczeniem;
- szumem informacyjnym – jako wynik nadmiaru spływających informacji mogących powodować utrudnienia w wyodrębnianiu informacji istotnych (niedobór czasu).

Zależnie od rangi zdarzenia i występujących zakłóceń należy wcześniej opracować i wdrażać plan naprawczy, którego zadaniem będzie wspieranie obecnie stosowanych procesów przez redukcję wpływających na nie czynników niepożądanych oraz niwelowanie możliwości ich wystąpienia w przyszłości.

Rys. 6. Zjawiska kreujące powstanie systemów klasy *big data*
Źródło: opracowanie własne

Powyższe zadania mogą być trudne do zrealizowania w rzeczywistości postępującej cyfryzacji, digitalizacji oraz danetyzacji (w tzw. zalewie informacyjnym). Zjawiska te potęgują ilość wytwarzanych danych, które muszą być przetwarzane w systemach informatycznych (zob. rys. 6). Duża ilość i objętość tych danych (Mayer-Schönberger, Cukier, 2017, s. 19) powoduje konieczność wdrożenia i wykorzystywania nowoczesnych rozwiązań zapewniających nieprzerwany obieg informacji. Metody i techniki zapewniania ciągłości działania o już ugruntowanej pozycji (kopie zapasowe, rezerwy sprzętowe, szkolenia, dokumentacja) (Liderman, 2012, s. 158-159) w tej nowej rzeczywistości mogą nie spełniać swojej funkcji w akceptowalnym wymiarze. Będzie to przekładać się na braki w procesach zapewniania bezpieczeństwa informacji, które mogą skutkować załamaniem się ładu informacyjnego i powstaniem strat znacznych rozmiarów. Zagrożenia te (biorąc pod uwagę ich urzeczywistnienie) mogą skutkować nawet całkowitym załamaniem się działalności danego podmiotu (ciągłości działania).

4. Wykorzystanie technologii *blockchain* do zapewniania informacyjnej ciągłości działania

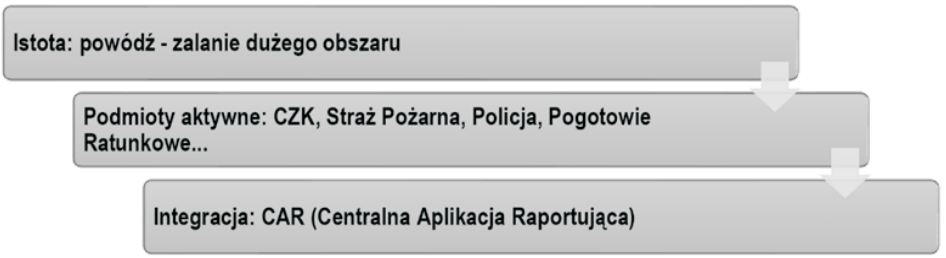
Jak wcześniej wspomniano, w celu ochrony przed potencjalną ingerencją w przetwarzane dane można wykorzystać technologię blockchain, która jest dynamicznie rozwijana i obecnie zyskuje status rozwiązania wykorzystywanego także w administracji publicznej (por. Attaran, Gunasekaran, 2019). Przykładem tego jest jej wykorzystanie przez estoński rząd. Dostosował on tę technologię do wsparcia zabezpieczeń platformy X-Road, której celem jest bezpieczna wymiana danych pomiędzy podmiotami sektora publicznego i prywatnego. Koncepcja ta integruje usługi (e-estonia, 2018):

- e-school;
- i-Voting;
- e-Banking;
- e-Tax oraz inne.

Umożliwia to obywatelom tego państwa korzystanie z bezpiecznej, zintegrowanej platformy cyfrowej, dzięki której większość spraw administracyjnych mogą realizować z prywatnych miejsc.

Doświadczenia z różnych implementacji tej technologii mogą stanowić bazę do kreowania podobnego systemu stosowanego do zapewniania bezpieczeństwa przetwarzania informacji na potrzeby nie tylko zarządzania, lecz także obsługi sytuacji kryzysowych. Żeby stworzyć taki system, należy:

- zdefiniować parametry geograficzno-zasobowe danej sytuacji kryzysowej;
- określić podmioty aktywne w razie wystąpienia sytuacji kryzysowej;
- wyszukać możliwości integracji z już działającymi rozwiązaniami.



Rys. 7. Schemat czynników wpływających na utworzenie systemu przetwarzania informacji wspieranego technologią łańcucha bloków

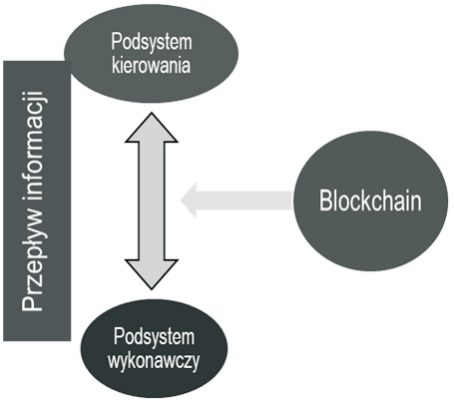
Źródło: opracowanie własne

Przykładowo w sytuacji kryzysowej spowodowanej powodzią schemat wyżej wymienionego postępowania ilustruje rysunek 7. Potrzeba wymiany odpowiedniej ilości danych z zapewnieniem jej wiarygodności może sprzyjać zastosowaniu przedmiotowej technologii. Widać więc, że bez zdefiniowania istoty (natury) sytuacji kryzysowej niemożliwe jest wyodrębnienie konkretnych podmiotów (służb i straży), które oczekują na właściwą informację do zwalczania jej skutków. Należy dodać, że sytuacją kryzysową może być nie tylko zdarzenie pochodzenia naturalnego, lecz także wszelkiego rodzaju zdarzenia wywołane przez człowieka lub maszynę (np. zła interpretacja algorytmu, błąd ludzki).

Jak już wspomniano, technologia *blockchain* może powodować dość znaczne koszty i dlatego w celu ich minimalizacji należy szukać możliwości integracji tej klasy rozwiązań z już istniejącymi rozwiązaniami sprzętowo-programowymi. Takie rozwiązanie nie tylko będzie racjonalne z ekonomicznego punktu widzenia, lecz również pozwoli na maksymalizację efektywności oraz minimalizację czasu przygotowania i wykonania konkretnych zadań. Ponadto implementacja łańcucha bloków (zob. rys. 8) pozwoli na zabezpieczenie informacji przed zakłóceniami pochodzenia ludzkiego (ingerencja osób trzecich), gdyż zmienione dane będą weryfikowane i odrzucane przez innych użytkowników systemu funkcjonujących w ramach wspólnego repozytorium danych.

Naturalne rozproszenie (replikacja) rejestru do każdego z użytkowników systemu może chronić przed błędami ludzkimi mogącymi mieć wpływ na stabilność systemu. Odzyskanie konfiguracji lub włączenie podmiotu do konkretnej konfiguracji może wówczas odbywać się nieinwazyjnie i w miarę efektywnie. Aby przeprowadzić cały proces, wymagany będzie jedynie dostęp do Internetu oraz dane dostępowe do projektowanego systemu. Warto jednak zauważyć, że konfiguracja ta powinna zostać zbudowana na podstawie zasobów i usług (rozwiązań) oferowanych na platformie chmury obliczeniowej. Pozwoli to na obniżenie kosztów związanych z utworzeniem oraz eksploatacją systemu w ramach mniejszych podmiotów. Zapewni to również

możliwość integracji wytworzonych rozwiązań między obecnymi uczestnikami konfiguracji a użytkownikami (podmiotami), którzy będą chcieli przystąpić do takiej struktury.



Rys. 8. *Blockchain* w zapewnianiu informacyjnej ciągłości działania
Źródło: opracowanie własne

Podsumowanie

W dobie szybko postępującego rozwoju technologicznego należy szukać sprawdzonych oraz bezpiecznych rozwiązań. Ten warunek dotyczy nie tylko sektora prywatnego, lecz także publicznego. W dzisiejszych czasach administracja publiczna wykorzystuje technologie sektora prywatnego, które obecnie są wymieniane na nowocześniejsze, zweryfikowane rozwiązania.

Zmiany te są konieczne, by sprostać coraz większym oczekiwaniom obywateli oraz podmiotów, które na co dzień biorą udział w kształtowaniu sfery ogólnospołecznej, gospodarczej i bezpieczeństwa państwa. Ewolucji muszą zostać poddane nie tylko fizyczne struktury organizacji, lecz także ich systemy informacyjne i rozwiązania teleinformatyczne.

Informacja bowiem to towar o kluczowym znaczeniu dla funkcjonowania zarówno pojedynczych przedsiębiorstw, jak i całych korporacji oraz podmiotów państwowych. Wymagane jest więc jak najlepsze jej zabezpieczenie. Nowoczesne rozwiązania powstające na rynku FinTech (Szymański, 2017), takie jak *blockchain*, mogą wspomagać proces (procesy) ochrony informacji. Ich uniwersalność pozwala na zastosowanie tych typów rozwiązań techniczno-technologicznych nie tylko w sektorze finansów, lecz także w szeroko rozumianym sektorze bezpieczeństwa państwa.

BIBLIOGRAFIA

[1] Attaran M., Gunasekaran A, 2019, *Applications of Blockchain Technology in Business: Challenges and Opportunities*, Springer International Publishing, Basel.

[2] Dhillon V., Metcalf D., Hooper M., 2018, *Zastosowania technologii blockchain*, Wydawnictwo Naukowe PWN, Warszawa.

[3] Liderman K., 2012, *Bezpieczeństwo Informacyjne*, Wydawnictwo Naukowe PWN, Warszawa.

[4] Liderman K., Zaskórski P., 2011, *Klasyfikacja i wartościowanie zagrożeń dla zasobów informacyjnych organizacji*, [w:] P. Zaskórski (red.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, Wojskowa Akademia Techniczna, Warszawa.

[5] Mayer-Schönberger V., Cukier K., *Big Data. Rewolucja, która zmieni nasze myślenie, pracę i* życie, MT Biznes, Warszawa.

[6] Mougayar W., Buterin V., 2019, *Blockchain w biznesie. Możliwości i zastosowania łańcucha bloków*, Wydawnictwo Helion, Gliwice.

[7] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU 2007 nr 89, poz. 590 ze zm.).

[8] Zaskórski P., Zaskórski W., 2017, *„Big-Data" Systems in Improving Modern Organizations*, „Nowoczesne Systemy Zarządzania", vol. 12, nr 2.

NETOGRAFIA

[1] Biedrzycki N., 2016a, *Blockchain – wszystko, co trzeba o nim wiedzieć* (dostęp: 20.01.2019), https://norbertbiedrzycki.pl/blockchain-trzeba-o-nim-wiedziec/.

[2] Biedrzycki N., 2016b, *Blockchain – wszystko, co warto o nim wiedzieć* (dostęp: 20.01.2019), https://businessinsider.com.pl/technologie/blockchain/blockchain-co-to-jest/vlfytn4.

[3] e-estonia, 2018, *X-Road®* (dostęp: 22.01.2019), https://e-estonia.com/solutions/interoperability-services/x-road/.

[4] Szymański D., 2017, *Fintechy robią furorę w internecie. Ale trzeba na nie uważać. „Niektóre mogą doprowadzić do katastrofy"* (dostęp: 25.01.2019), https://businessinsider.com.pl/finanse/co-to-jest-fintech-jak-wygladaja-finanse-w-internecie/08f7r1j.

[5] Wowza, 2018, *Wowza Blog Six Benefits of P2P Unicast Streaming* (dostęp: 28.01.2019), https://www.wowza.com/blog/six-benefits-of-p2p-unicast-streaming.