Tomasz Protasowicki, Jerzy Stanik

# Big Data w analizie zagrożeń bezpieczeństwa narodowego

Ekonomiczne Problemy Usług nr 123, 275-286

2016

Ekonomiczne Problemy Usług nr 123

ISSN: 1896-382X | www.wnus.edu.pl/pl/epu/
DOI: 10.18276/epu.2016.123-26 | strony: 275-286

*TOMASZ PROTASOWICKI, JERZY STANIK*
Wojskowa Akademia Techniczna[1]

# BIG DATA W ANALIZIE ZAGROŻEŃ BEZPIECZEŃSTWA NARODOWEGO

**Streszczenie**

W artykule przedstawiono ogólny zarys modelu platformy przeznaczonej do pozyskiwania, wymiany i przetwarzania danych o zagrożeniach bezpieczeństwa narodowego RP. Proponowany system zakłada wykorzystanie współczesnych metod Big Data i wspierających je narzędzi informatycznych. Celem istnienia takiego systemu jest kompleksowe wspomaganie procesów decyzyjnych związanych z identyfikacją i oceną pojawiających się zagrożeń dla bezpieczeństwa narodowego.
**Słowa kluczowe:** e-administracja, Big Data, analiza danych, wspomaganie decyzji.

## Wprowadzenie

Współcześnie występujące na świecie trendy w obszarze kształtowania się zagrożeń dla bezpieczeństwa narodowego odznaczają się dużą dynamiką. Zjawiska występujące w środowisku bezpieczeństwa narodowego RP generują bogate zasoby danych. Prowadzone na ich podstawie procesy analizy i oceny mogą stanowić podstawę do prognozowania różnych scenariuszy dotyczących rozwoju sytuacji. Pozwala to na opracowanie odpowiednich strategii postępowania zorientowanych na minimalizację prawdopodobieństwa lub skutków wystąpienia zagrożenia. Wymagane jest w tym celu wdrożenie odpowiednich metod, narzędzi i technik kompleksowego wspomagania procesów informacyjno-decyzyjnych w obszarze bezpieczeństwa narodowego RP.

Pozyskiwanie, integracja i eksploracja niezbędnych danych o zagrożeniach bezpieczeństwa narodowego RP z mocno rozproszonych źródeł stanowi nadal duże

[1] Wydział Cybernetyki, Instytut Systemów Informatycznych.

wyzwanie praktyczne. Co więcej, dane te charakteryzują się spełnieniem paradygmatu Big Data, wymagają więc odpowiedniego podejścia związanego m.in. z ich przetwarzaniem, zarządzaniem ich spójnością semantyczną i retencją. W chwili obecnej nie istnieje w Polsce żaden kompleksowy system informatyczny, który umożliwiałby gromadzenie i przetwarzanie takich danych w oparciu o wspólną bazę danych, agregującą w sposób usystematyzowany informacje pochodzące z wielu źródeł o charakterze ustrukturyzowanym i nieustrukturyzowanym.

Celem przeprowadzonych prac badawczych przedstawionych w ramach niniejszego opracowania było opracowanie ogólnego modelu platformy przeznaczonej do pozyskiwania, wymiany i przetwarzania danych o zagrożeniach pomiędzy podmiotami tworzącymi System Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej. (SBN RP), która ponadto pozwalałaby na ich kompleksową eksplorację i analizę oraz budowanie prognoz rozwoju sytuacji w domenie bezpieczeństwa narodowego.

## 1. Istota bezpieczeństwa narodowego RP

Bezpieczeństwo narodowe oznacza zdolność państwa do zapewnienia warunków jego istnienia i rozwoju, zachowania integralności terytorialnej, niezależności politycznej, stabilności wewnętrznej oraz jakości życia obywateli. Zdolność ta jest kształtowana poprzez działania polegające na wykorzystaniu szans, podejmowaniu wyzwań, redukowaniu ryzyka oraz eliminowaniu zagrożeń zewnętrznych i wewnętrznych, co zapewnia trwanie, tożsamość, funkcjonowanie i swobody rozwojowe państwa i społeczeństwa (Zając i Zięba 2010).

SBN RP stanowi całość sił, środków i zasobów przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa, odpowiednio do tych zadań zorganizowana, utrzymywana i przygotowywana. Składa się z podsystemu kierowania i szeregu podsystemów wykonawczych, w tym podsystemów operacyjnych i podsystemów wsparcia (BBN 2013).

Rolą SBN RP jest zapewnienie nienaruszalnego przetrwania państwa jako instytucji politycznej oraz trwałego i wolnego od zakłóceń istnienia i rozwoju społeczeństwa poprzez efektywne zaangażowanie i wykorzystanie dostępnych sił, środków i zasobów do realizacji działań zmierzających do redukowania ryzyka w dziedzinie bezpieczeństwa, eliminacji zagrożeń oraz prowadzenie aktywnej polityki wykorzystywania pojawiających się szans (Protasowicki 2014).

## 2. Pojęcie i istota Big Data

Jak podaje Szafrański (2014), pojęcie Big Data pierwotnie odnosiło się do danych charakteryzujących się dużą: objętością (ang. *volume*), zmiennością (ang.

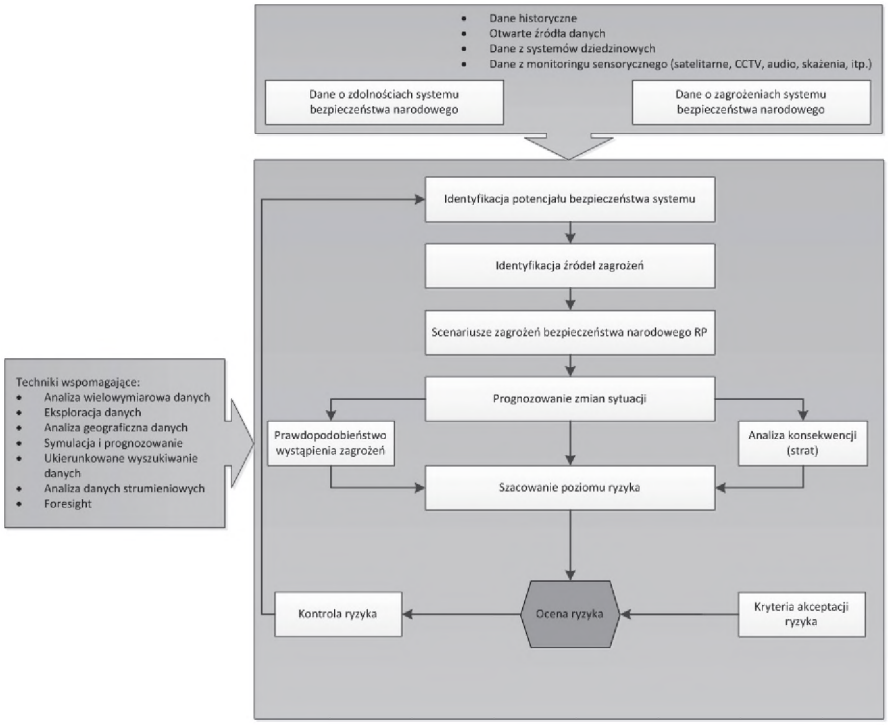
*velocity*) oraz różnorodnością (ang. *variety*). Kolejną cechą charakterystyczną, która została dostrzeżona z upływem czasu, jest wartość danych (ang. *value*). Obecnie nadal brak jest ostatecznie przyjętej ścisłej definicji Big Data. Jednak jak podaje Szafrański, większość teoretyków i praktyków zajmujących się tym obszarem definiuje Big Data jako zbiory danych (informacji) o bardzo dużej objętości, różnorodności i zmienności, których immanentną cechą jest to, że poddawane analizie bardzo szybko zmieniają swoją zawartość zarówno w zakresie zawartości, struktury, obszarów tematycznych, jak i objętości. Dane w tych zbiorach szybko znikają i przyrastają wskutek interakcji wielkiej liczby zazwyczaj nieznanych interesariuszy. Dane te mogą mieć charakter strumienia (zdarzeń, transakcji itp.). Termin Big Data można zatem postrzegać również jako odnoszący się do metod przetwarzania zasobów cyfrowych wytwarzanych w czasie rzeczywistym.

## 3. Uwarunkowania budowy platformy analizy danych o zagrożeniach

Zagrożenie to zjawisko, zdarzenie (lub ich ciąg), które jest spowodowane przyczynami losowymi lub nielosowymi. W kontekście bezpieczeństwa narodowego jego zaistnienie wywiera wpływ na funkcjonowanie państwa i jego równowagę wewnętrzną lub powoduje niekorzystne zmiany w jego otoczeniu zewnętrznym (Ficoń 2007). Kumulowanie się zagrożeń i brak stosownych reakcji na nie podjętych w odpowiednim czasie może powodować utratę warunków do niezakłóconego bytu lub naruszenie bądź utratę suwerenności państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych (Jakubczak 2003). Zagrożenia bezpieczeństwa narodowego mogą być klasyfikowane według różnych kryteriów: przedmiotowych, źródła zagrożenia, środowiska, zasięgu zagrożenia, skali zagrożenia, skutków zagrożenia, miejsca występowania zagrożenia, charakteru stosunków społecznych itd.

Zidentyfikowane zagrożenia inicjują proces zarządzania bezpieczeństwem narodowym RP. Wśród jego głównych determinant można wyróżnić występowanie różnego rodzaju zagrożeń i różnych stopni podatności na te zagrożenia poszczególnych obszarów, dziedzin i instytucji istotnych z punktu widzenia bezpieczeństwa narodowego. Niebagatelne znaczenie dla skuteczności tego procesu ma określenie metod i technik analizy oraz oceny zarówno prawdopodobieństwa, jak również szacowania intensywności występowania niepożądanych zdarzeń i rozmiaru możliwych konsekwencji ich zaistnienia. Częścią procesu zapewniania bezpieczeństwa jest stosowanie metod ewaluacji zagrożeń, podatności, konsekwencji zagrożeń na potrzeby analizy ryzyka zagrożeń bezpieczeństwa narodowego RP. Wraz z rozwojem cywilizacyjnym i zmieniającymi się warunkami gospodarczo-ekonomicznymi, politycznymi zarządzanie ryzykiem odgrywa coraz większą rolę w codziennym życiu. W sensie operacyjnym można zatem zarządzanie bezpieczeństwem narodo-

wym RP utożsamiać z zarządzaniem ryzykiem wystąpienia zidentyfikowanych zagrożeń przy pomocy zunifikowanych metod i technik (rysunek 1). Unifikacja wynika z potrzeby ujednolicenia szacowania ryzyka pod kątem porównywania poszczególnych ryzyk do celów decyzyjnych, a samo ryzyko stanowi w tym ujęciu miarę zagrożenia.



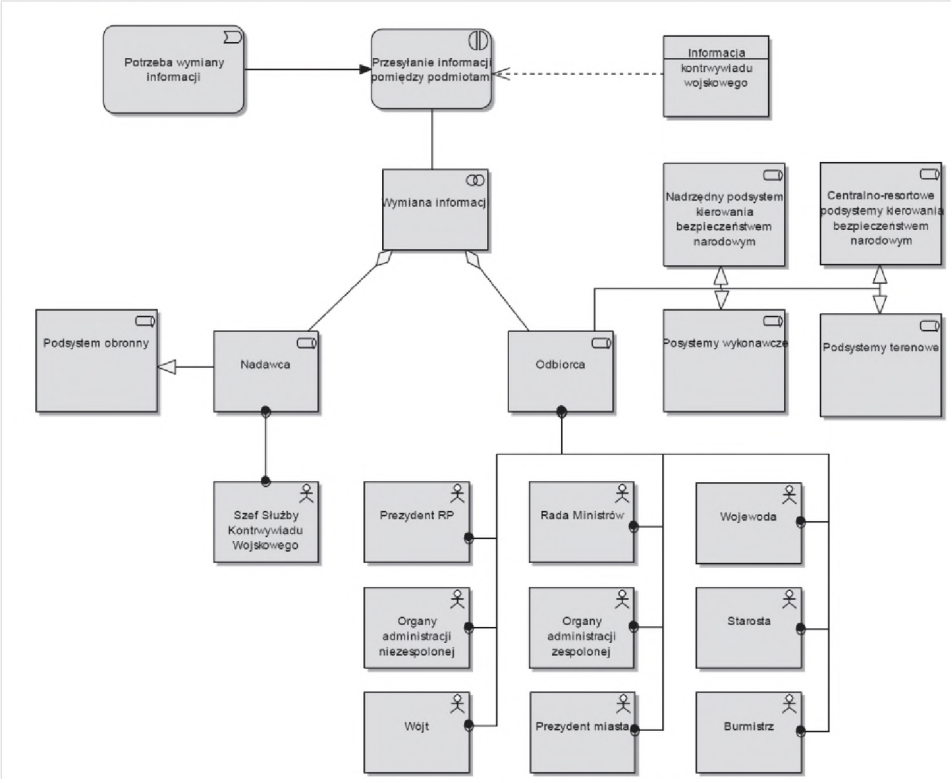

Rys. 1. Ilustracja procesu informacyjno-decyzyjnego opartego na analizie ryzyka

Źródło: opracowanie własne na podstawie: (Sienkiewicz 2006).

Z punktu widzenia SBN RP przedmiotem zarządzania są wszystkie zidentyfikowane zagrożenia dla funkcjonowania i rozwoju państwa, społeczeństwa i obywateli. Podstawą do całościowego i efektywnego zarządzania bezpieczeństwem narodowym jest identyfikacja i szacowanie wszystkich ryzyk w skali państwa uporządkowanych w oparciu o spójny katalog zagrożeń. Identyfikacja zagrożeń i ich przewidywanie wynika z prowadzonej w sposób ciągły oceny rozwoju i dokonywanych prognoz zmian sytuacji.

Wysokie wymagania stawiane SBN RP w warstwie identyfikacji i przeciwdziałania zagrożeniom wymagają sprawnego przebiegu procesów informacyjno-decyzyjnych na wszystkich szczeblach funkcjonowania państwa (tj. centralnym, wojewódzkim, powiatowym i gminnym). Proces informacyjno-decyzyjny rozumia-

ny jest jako cykl zorganizowanych działań, wyrażający się w postaci algorytmu identyfikacji i przygotowania działań, przedstawiającego logiczny układ następujących po sobie oraz uzależnionych od siebie etapów i czynności (Bieniok 1999). Przykład takiego procesu wymagający wsparcia informatycznego przedstawiono na poniższym diagramie (rysunek 2).




Rys. 2. Ilustracja wymiany informacji kontrwywiadu wojskowego

Źródło: opracowanie własne.

Zaprojektowanie platformy integracji i analizy danych o zagrożeniach w obszarze bezpieczeństwa narodowego RP pozwoli na zorganizowanie danych o zagrożeniach w jeden spójny i wydajny system, ze ściśle zdefiniowaną funkcjonalnością. Budowa takiego rozwiązania umożliwi zatem stworzenie solidnej podstawy dla efektywnego funkcjonowania SBN RP.

## 4. Wymagania

Główne wymagania biznesowe postulowane w stosunku do proponowanego rozwiązania obejmują w szczególności umożliwienie:

1) utworzenia jednego źródła danych usystematyzowanego pod kątem treści i zapewniającego bezpieczny dostęp do tych treści dla wielu różnych podmiotów tworzących SBN RP i ich upoważnionych przedstawicieli;
2) integracji danych wywiadowczych pochodzących z różnych źródeł (m.in. rozpoznania: osobowego, elektronicznego, pomiarowego i sygnaturowego, obrazowego, geoprzestrzennego, technicznego, cyberprzestrzeni, finansowego);
3) utworzenia repozytorium danych referencyjnych dotyczących kluczowych zagadnień z zakresu bezpieczeństwa narodowego, pozwalającego na unifikację wyników analiz przeprowadzanych przez różne podmioty;
4) przeszukiwania danych o charakterze nieustrukturyzowanym, dostępnych w źródłach otwartych, pod kątem zagadnień związanych z bezpieczeństwem narodowym;
5) prowadzenia wieloaspektowych analiz, pozwalających na identyfikowanie szans, wyzwań i zagrożeń oraz ocenę ich wpływu na bezpieczeństwo narodowe RP;
6) tworzenia prognoz na podstawie zgromadzonych danych oraz ich wykorzystania w podejmowaniu decyzji z zakresu zapewniania bezpieczeństwa narodowego RP;
7) adaptacji systemu do zmian w zakresie ilości i rodzaju przetwarzanych danych oraz do zmian danych referencyjnych (np. definicji zagrożeń, wartości chronionych, przyjętych kryteriów oceny bezpieczeństwa itp.);
8) automatyzacji procesu identyfikacji poszukiwania i zależności pomiędzy danymi opisującymi różne obiekty mogące wpływać na poziom bezpieczeństwa narodowego RP;
9) zasilania systemu danymi ustrukturyzowanymi i nieustrukturyzowanymi pochodzącymi ze źródeł o różnorodnym charakterze oraz intensywności, w tym danymi strumieniowymi (np. audio, wideo itp.).

W celu zaspokojenia ww. wymagań biznesowych platforma integracji i analizy danych musi dostarczać standardowych funkcjonalności umożliwiających co najmniej:

1) gromadzenie dużego wolumenu danych ustrukturalizowanych i nieustrukturalizowanych oraz zarządzanie nimi przy zachowaniu wymaganego poziomu ich bezpieczeństwa i jakości;
2) integrację i zarządzanie danymi pochodzącymi ze wszystkich pożądanych źródeł;

3) analizę i wizualizację gromadzonych danych oraz odkrywanie i analizowanie zależności występujących pomiędzy nimi;
4) przetwarzanie i analizowanie danych strumieniowych w czasie rzeczywistym;
5) zarządzanie danymi referencyjnymi;
6) tworzenie aplikacji i zarządzanie systemem i jego podsystemami;
7) wytwarzanie i współdzielenie reużywalnych: funkcji analitycznych, schematów, zestawów narzędzi i innych artefaktów umożliwiających szybkie dostarczanie wartościowych informacji wymaganych w procesach decyzyjnych.

Oprócz spełnienia ww. wymagań biznesowych i funkcjonalnych projektowany system musi również implementować zintegrowany model zagrożeń bezpieczeństwa narodowego oraz spójny model oceny ryzyka.

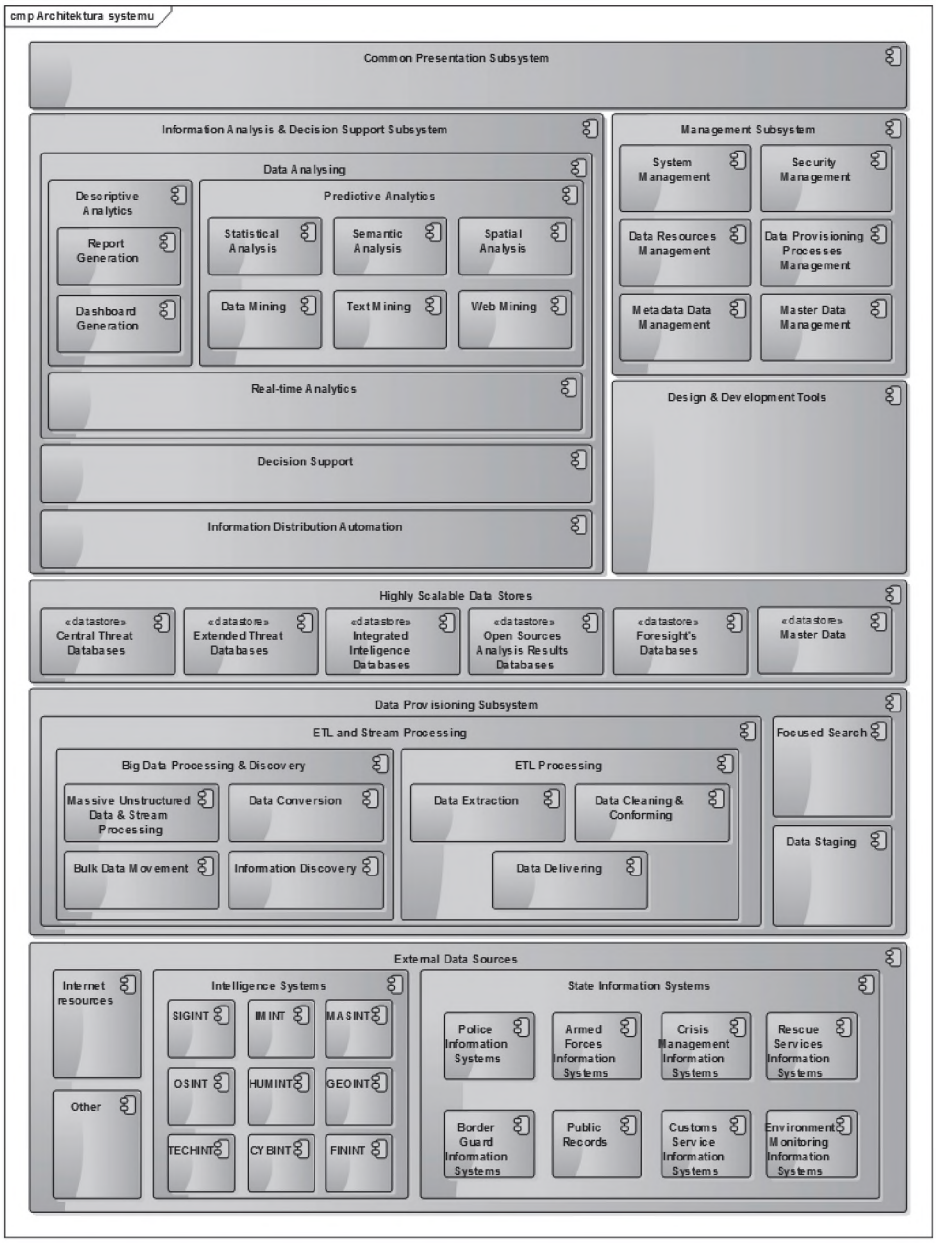
## 5. Koncepcja architektury systemu

Wykorzystywane obecnie w Polsce narzędzia i rozwiązania informatyczne nie są w stanie sprostać wyzwaniom związanym z identyfikacją i analizą występujących współcześnie złożonych zagrożeń bezpieczeństwa narodowego. Architektura platformy wymiany i analizy danych o zagrożeniach bezpieczeństwa narodowego przedstawiona poniżej ma w intencji autorów wyeliminować istniejące ograniczenia.

Poniżej przedstawione zostały informacje o wysokopoziomowych aspektach architektury proponowanego rozwiązania. Głównym celem jest opracowanie takiej architektury, która zapewni pełne pokrycie postawionych wymagań biznesowych i spowoduje dostarczenie odpowiedniego zestawu narzędzi, będącego w stanie dostarczyć wyniki analiz, pozwalające na identyfikowanie pojawiających się szans, wyzwań i zagrożeń oraz wskazywanie ich potencjalnych źródeł oraz szacowanie prawdopodobieństwa ich wystąpienia. Zestaw narzędzi będących elementami składowymi platformy powinien zawierać komponenty implementujące najlepsze sprawdzone wzorce z obszaru m.in. hurtowni danych, integracji danych, zarządzania jakością danych, zarządzania danymi referencyjnymi, Big Data, Business Intelligence, Data Mining, przetwarzania strumieniowego itd.

Rozwiązanie powinno zapewnić wysoką jakość i dostępność danych oraz dostarczać skalowalne komponenty do raportowania, tworzenia kokpitów i wykonywania obliczeń statystycznych z wykorzystaniem zgromadzonych danych. Niezwykle istotna jest również możliwość zasilania rozwiązania ze źródeł nieustrukturyzowanych i stosowania metod wzbogacania danych. Należy zauważyć, że ogólna architektura proponowanego systemu analitycznego radykalnie różni się od architektury typowych systemów informatycznych zarówno o charakterze transakcyjnym (OLTP), jak i analitycznym (OLAP, DWH, BI).

Poniższy rysunek (rysunek 3) przedstawia widok architektury logicznej proponowanego rozwiązania.




Rys. 3. Architektura platformy integracji i analizy danych o zagrożeniach bezpieczeństwa narodowego

Źródło: opracowanie własne.

Wyróżniono w niej siedem zasadniczych warstw:

1) źródeł danych,
2) dostarczania danych,
3) wysoko skalowalnych mechanizmów składowania danych,
4) analizy danych i wspomagania decyzji,
5) zarządzania systemem,
6) narzędzi do projektowania i implementacji,
7) wspólnego interfejsu użytkownika.

Źródłami danych dla projektowanej platformy są m.in.: systemy dziedzinowe i eksperckie eksploatowane przez różne podmioty tworzące SBN RP (m.in. wojsko, policja, służby ratownicze, straż graniczna, służba celna, służby ochrony środowiska, centra zarządzania kryzysowego itp.), sieci sensorów dostarczające danych strumieniowych (np. wideo, audio, sygnały elektromagnetyczne, pomiary: stężenia czynników chemicznych, promieniowania, poziomu wód w rzekach i zbiornikach retencyjnych itp.), systemy dostarczające dane graficzne (obrazy satelitarne, zdjęcia lotnicze), rejestry państwowe, systemy wspomagania ochrony infrastruktury krytycznej, systemy ochrony sieci telekomunikacyjnych, systemy wspomagania służb wywiadu i kontrwywiadu (cywilnego i wojskowego), źródła otwarte (np. strony i fora internetowe, portale ogłoszeniowe, grupy dyskusyjne, Facebook, Twitter, Instagram, platformy handlowe itp.) oraz inne niewymienione systemy mogące dostarczyć potencjalnie cennych danych wejściowych. Ww. źródła dostarczają zarówno danych ustrukturalizowanych, częściowo ustrukturalizowanych, jak również nieustrukturalizowanych. Rodzi to szereg wyzwań natury technicznej związanych z ich przygotowaniem do późniejszego wykorzystania w procesach decyzyjnych.

Dane ze źródeł trafiają do repozytoriów systemu przy pomocy podsystemu zasilania. Podlegają one w tej warstwie licznym przekształceniom przy użyciu znajdujących się w niej specjalizowanych narzędzi i algorytmów. Celem tych działań jest nadanie surowym danym postaci odpowiedniej do dalszego przetwarzania analitycznego. W warstwie zasilania systemu danymi można wyróżnić następujące główne komponenty:

1) podsystem przetwarzania danych typu Big Data – odpowiedzialny za wydobywanie i przekształcanie danych nieustrukturalizowanych do postaci analitycznej oraz operacje masowego przemieszczania danych do repozytoriów nierelacyjnych;
2) podsystem ETL – odpowiedzialny za wydobywanie i przekształcanie danych ustrukturalizowanych;
3) podsystem ukierunkowanego wyszukiwania – odpowiedzialny za przeszukiwanie zasobów Internetu w poszukiwaniu stron WWW spełniających określone predykaty;

4) podsystem przechowywania danych tymczasowych – odpowiedzialny za składowanie danych pomiędzy ich pozyskaniem z systemu źródłowego a zasileniem przy ich pomocy zbiorów analitycznych.

Możliwe jest zastosowanie następujących mechanizmów ładowania danych:

1) cykliczne ładowanie danych – dla ustrukturalizowanych danych wolnozmiennych;
2) ładowanie danych online – pobierane na bieżąco z systemów źródłowych (w trybie pull lub push), dzięki czemu dane w momencie wprowadzenia ich do systemu źródłowego będą równocześnie dostępne w systemie analitycznym;
3) ładowanie ustrukturalizowanej zawartości z repozytoriów nierelacyjnych do relacyjnych na podstawie zdefiniowanych algorytmów wydobywania encji danych ze źródeł tekstowych, obrazów i sekwencji wideo;
4) wzbogacanie danych źródłowych rezultatami wykonanych analiz.

Warstwa składowania danych odpowiada za przechowywanie i udostępnianie warstwie narzędzi analitycznych danych zgromadzonych w: centralnych bazach danych o zagrożeniach, rozszerzonych bazach danych o zagrożeniach, zintegrowanych bazach danych wywiadowczych, wynikowych bazach danych analiz źródeł otwartych, bazach danych foresightu, bazach danych referencyjnych.

Ze względu na wolumen oraz niejednorodny charakter danych zgromadzonych w tych zbiorach do ich składowania należy wykorzystać wysoce skalowalne mechanizmy dostarczane przez technologie takie jak:

1) NoSQL – pozwalające na przechowywanie: obrazów, zapisów sygnałów, strumieni danych, szeregów czasowych, tekstu i innych danych nieustrukturalizowanych;
2) relacyjnych baz danych – pozwalające na przechowywanie danych w postaci struktur analitycznych (schematów hurtowni danych, data martów);
3) In Memory Data Grids – pozwalające na przechowywanie danych w pamięci RAM w celu przyspieszenia analiz w czasie rzeczywistym na dużych wolumenach danych.

Zastosowanie aplikacji analitycznych dostarczających standardowych funkcjonalności pozwala na uniknięcie konieczności tworzenia od podstaw złożonych algorytmów analizy danych. W warstwie analizy danych i wspomagania decyzji można wyróżnić:

1) podsystem analityki opisowej – odpowiedzialny za dostarczanie mechanizmów raportowania;
2) podsystem analityki predykcyjnej – odpowiedzialny za analizę danych w celu odnalezienia w nich wzorców oraz zależności, obejmuje m.in. analizę statystyczną, eksplorację danych tekstowych (w tym WWW, np. w zakresie analizy publikacji dotyczących działań niezgodnych z prawem), analizy semantyczne, eksplorację danych przestrzennych analizy danych

pogodowych, analizy rozprzestrzeniania się skażeń i epidemii, analizy sieci społecznościowych (w tym analizę powiązań między osobami i organizacjami) itp.;
3) podsystem analizy danych w czasie rzeczywistym – odpowiedzialny za przetwarzanie analityczne online danych strumieniowych;
4) podsystem wspomagania decyzji – odpowiedzialny za wykonywanie zdefiniowanych procesów wnioskowania i generowanie scenariuszy rozwoju sytuacji oraz planów działania dla decydentów;
5) podsystem automatyzacji dystrybucji informacji – odpowiedzialny za dostarczanie zdefiniowanym odbiorcom powiadomień o zdarzeniach, wyników analiz lub predefiniowanych cyklicznych raportów.

## Podsumowanie

Celem przeprowadzonych prac badawczych, których wyniki przedstawiono w niniejszym artykule, było opracowanie ogólnego modelu platformy przeznaczonej do pozyskiwania, wymiany i przetwarzania danych o zagrożeniach bezpieczeństwa narodowego RP. Przeprowadzone w toku prac badawczych analizy pozwoliły przedstawić koncepcję architektury takiego rozwiązania. Założono przy tym zastosowanie współczesnych metod i narzędzi informatycznych do kompleksowego wspomagania procesów decyzyjnych związanych z identyfikacją i oceną pojawiających się zagrożeń dla bezpieczeństwa narodowego. Postulowany system umożliwi wieloaspektowe badanie wpływu szeregu różnorodnych czynników (zjawisk, zdarzeń) na szeroko pojęte bezpieczeństwo narodowe. Będzie to możliwe poprzez fuzję danych pochodzących z różnych źródeł. Sprzyja temu zastosowanie na etapie projektowania systemu najlepszych praktyk i wzorców projektowych z obszaru m.in.: hurtowni danych, integracji danych, zarządzania danymi referencyjnymi, Big Data, Business Intelligence, Data Mining, przetwarzania strumieniowego. Praktyczne wdrożenie proponowanego rozwiązania przyczyni się do poprawy stanu bezpieczeństwa narodowego RP przez daleko idące usprawnienie procesów informacyjno-decyzyjnych zachodzących w państwie.

## Literatura

1. BBN (2013), *Biała Księga Bezpieczeństwa Narodowego RP*, Warszawa: Biuro Bezpieczeństwa Narodowego.
2. Bieniok H. (1999), *Metody sprawnego zarządzania*, Warszawa: Placet.
3. Ficoń K. (2007), *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa: BEL Studio.

4. Kimball R., Ross M. (2002), *The Data Warehouse Toolkit*, New Jersey: Wiley.
5. Protasowicki T. (2014), *Wybrane aspekty zastosowania koncepcji architektury korporacyjnej w transformacji Systemu Bezpieczeństwa Narodowego RP*, Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług, vol. 112.
6. Protasowicki T., Stanik J. (2014), *The concept of maintaining functional security of an integration platform*, w: *Information Managemen*, red. B.F. Kubiak, A. Sieradz, Gdańsk: Gdańsk University Press.
7. Sienkiewicz P. (2006), *Zarządzanie ryzykiem w sytuacjach kryzysowych*, Warszawa: AON.
8. Szafrański B. (2014), *Realizacja zadań publicznych a Big Data*, w: *Internet. Publiczne bazy danych i Big Data*, red. G. Szpor, Warszawa: C.H. Beck.
9. Zając J., Zięba R. (2010), *Budowa zintegrowanego systemu bezpieczeństwa narodowego Polski*, Warszawa.

## BIG DATA WITHIN NATIONAL SECURITY THREAT ANALYSIS

### Summary

The paper presents a generic model of a platform intended for the exchange of threat-related data between the participants of the NSS of RP. The system proposed will allow the use of modern IT methods and tools so as to provide an all-inclusive support to decision-making processes associated with the identification and evaluation of threats to national security. The main purpose of analyses performed within the system will be to investigate the impact of a number of factors (circumstances, events) on national security in the broadest meaning of the term.
**Keywords:** e-government, big data, data analysis, decision support.

*Translated by Tomasz Protasowicki and Jerzy Stanik*