STUDIA NAD BEZPIECZEŃSTWEM

NR 2

Akademia Pomorska w Słupsku

STUDIA NAD BEZPIECZEŃSTWEM

NR 2

Słupsk 2017

ISSN 2543–7321

Wersja papierowa jest wersją pierwotną.
Czasopismo w wersji on-line znajduje się na stronie:
zeszyty-bn.apsl.edu.pl

Wydawnictwo Naukowe Akademii Pomorskiej w Słupsku
ul. K. Arciszewskiego 22a, 76-200 Słupsk, tel. 59 84 05 378
www.wydawnictwo.apsl.edu.pl e-mail: wydaw@apsl.edu.pl

Druk i oprawa: volumina.pl Daniel Krzanowski
ul. Księcia Witolda 7-9, 71-063 Szczecin, tel. 91 812 09 08

Obj. 11,5 ark. wyd., format B5, nakład 100 egz.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 5–16 ROK 2017

ISSN 2543–7321

Wojciech Czajkowski
Jolanta Wąs-Gubała

Wyższa Szkoła Bezpieczeństwa Publicznego
i Indywidualnego „APEIRON”
Kraków
paksos@gmail.com
jolantawas-gubala@apeiron.edu.pl

BEZPIECZEŃSTWO PERSONALNE W PERSPEKTYWIE KULTUROWEJ

PERSONAL SECURITY IN CULTURAL PERSPECTIVE

***Zarys treści*:** Autorzy w prezentowanym opracowaniu podejmują kwestię mechanizmów regulujących zachowanie jednostki w warunkach sytuacji trudnej i sytuacji zagrożenia. Realizacja instynktownego i świadomego dążenia do zaspokojenia potrzeby bezpieczeństwa jest interpretowana poprzez przywołanie kategorii wiedzy osobistej stanowiącej istotny instrument radzenia sobie z wymaganiami otoczenia. W systemie funkcjonowania osobowości sytuuje się obecność i działanie standardów regulacyjnych stanowiących mechanizm oceny i wartościowania celów oraz sposobów własnego działania. Zwraca się także uwagę na relacje społeczne jednostki i społeczno-kulturowe uwarunkowania zachowań konstruktywnych i zachowań stanowiących akty manipulacji. Jest to szczególnie istotne w przypadku bezpieczeństwa personalnego, istotnie powiązanego z koncepcją human security i nawiązującego do fenomenologiczno-egzystencjalnej interpretacji relacji społecznych jednostki. Wskazując na kontekst bezpieczeństwa, sugeruje się potrzebę podejmowania problematyki wartości uwikłanych w możliwość oceny relacji z innymi ludźmi.

***Słowa kluczowe*:** bezpieczeństwo personalne, bezpieczeństwo człowieka, standardy regulacyjne osobowości, wartości

Key words: personal security, human security, personality regulative standards, values

Problematyka funkcjonowania człowieka w realiach sytuacji zagrożenia i sytuacji kryzysowej stanowi istotę analizy i badań w obszarze bezpieczeństwa personalnego. Poniekąd wynika to z faktu, że bezpieczeństwo jest fenomenem o charakterze

antropocentrycznym. Człowiek bezustannie pragnie swojego bezpieczeństwa nie tylko instynktownie, ale i w pełni świadomie. Koncentracja na dążeniu do uzyskania i utrzymania swojego dobrostanu stanowi zasadniczy motyw działania przeciętnego człowieka. Bezpieczeństwo rozumiane zarówno w kategoriach stanu, jak i procesu stanowi zasadniczą podstawę realizowania wskazanego dobrostanu. Wydaje się również, że dążenia takie stanowiły niezbywalny element funkcjonowania jednostek i grup społecznych w długim okresie rozwoju gatunku ludzkiego. W związku z powyższym człowiek wieloma różnymi metodami próbuje wykreować ten pożądany dla siebie stan. Związane z tym utrwalone doświadczenia, wiedza, umiejętności i ludzkie wytwory składają się na strukturę kultury bezpieczeństwa[1], która jest częścią domeny kultury stanowiącej istotne kryterium człowieczeństwa.

Działania jednostki w sytuacjach trudnych i w sytuacjach zagrożenia mają także uwarunkowania kulturowe uwikłane w problematykę wartości. Kwestia ta stanowi istotny element interpretacyjny podkreślany przez autorów pracy. Wydaje się także, że podniesiona kwestia zarówno instynktownego, jak i świadomego dążenia do zaspokojenia potrzeby bezpieczeństwa wymaga komentarza. W działaniu jednostki można zidentyfikować znaczenie tzw. wiedzy osobistej dla procesu radzenia sobie z wymaganiami otoczenia. W problematyce bezpieczeństwa wskazuje się na znaczenie szans, wyzwań, ryzyk i zagrożeń, które stanowią stałe, niezbywalne środowisko bezpieczeństwa, skłaniając jednostkę do aktywnych zachowań służących realizacji założonych celów[2]. W systemie funkcjonowania osobowości sytuuje się obecność i działanie standardów regulacyjnych stanowiących mechanizm oceny i wartościowania celów oraz sposobów własnego działania[3], a także celów i działania innych osób. Problematyka ta w sposób zasadniczy jest powiązana z kwestią działania jednostki i jej osobowości wraz z jej mechanizmami regulacyjnymi w trudnych warunkach sytuacji zagrożenia[4].

W poznawczej koncepcji osobowości identyfikuje się następujące funkcje osobowości:

- Konstruowanie poznawcze, nadawanie sensu doświadczeniom podmiotu poprzez kategoryzowanie napływających informacji za pomocą konstruktów osobistych, przewidywanie zdarzeń, konstruowanie modeli pojęciowych swojej przyszłości;
- Dostarczanie podstaw do ewaluacji, wartościowania zdarzeń, innych ludzi i samego siebie (ocena celów, kierunków i wyników działania, własnej przeszłości i przyszłości). Pozwala to na określenie tego, co wybierać i czego unikać, cele poprzez takie procesy są odnoszone do swoistych standardów regulacji;

[1] M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, Siedlce 2010.

[2] Por.: *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, red. S. Koziej i in., Biuro Bezpieczeństwa Narodowego, Warszawa 2013.

[3] W. Czajkowski, Interpersonal Framework of Establishing Contact in Psychotherapy, [w:] M. Kliś, J. Kossewska, W. Czajkowski, Studies on Communication and coping with Stress, Kraków 2006.

[4] Por.: W. Czajkowski, *Psychologiczne mechanizmy działania jednostki w sytuacji zagrożenia*, Katowice 2014, s. 9.

- Programowanie działań, ustanawianie celów, dobór strategii działania zgodnych z wymogami sytuacji oraz preferencjami i możliwościami jednostki (styl poznawczy, kompetencje);
- Sterowanie przebiegiem działania poprzez procesy samoregulacji (monitorowanie i regulowanie własnych emocji i stanów motywacyjnych; także procesów poznawczych – ukierunkowywanie uwagi, selektywne zapamiętywanie) tak, aby służyło to osiąganiu ważnych dla człowieka celów[5].

W ogólnej interpretacji osobowości jako systemu wiedzy osobistej zwraca się uwagę na ważką interpretację dotyczącą dwojakiego rodzaju wiedzy. Wskazuje się na wiedzę deklaratywną, nazywaną niekiedy „wiedzą, że" (wiedza faktualna), oraz wiedzę proceduralną, nazywaną „wiedzą, jak". Wiedza deklaratywna jest łatwo dostępna, łatwa do modyfikacji, jednakże przetwarzanie informacji z jej udziałem przebiega wolno. Wiedza proceduralna jest zawarta w procedurach przetwarzania informacji i sterowania zachowaniem. W przeciwieństwie do poprzedniej, wiedza ta jest zasadniczo niedostępna świadomości jednostki i trudna do modyfikacji. Niezależnie od tego, przy udziale tej wiedzy informacje są przetwarzane bardzo szybko. Z tymi dwoma rodzajami wiedzy są skojarzone dwa typy przetwarzania informacji: przetwarzanie kontrolowane i przetwarzanie automatyczne. Szczególnie interesujące są dla nas przykłady przetwarzania automatycznego, które ma zastosowanie w przypadku wiedzy proceduralnej. Dlatego też niżej wskażemy cechy przetwarzania automatycznego jej dotyczące:

- jest niezależne od zasobów poznawczych;
- ma charakter równoległy;
- przebiega bardzo szybko;
- przebiega bez wysiłku poznawczego.

Nie ma większych wątpliwości, że wiedza tego rodzaju będzie wykorzystywana przez jednostkę w warunkach zagrożenia.

Podjęcie problematyki znaczenia zmiennych osobowościowych dla funkcjonowania jednostki w sytuacji zagrożenia i w sytuacjach trudnych wydaje się uzasadnione w związku z typowymi elementami składającymi się na nie. Porządkując sytuacje trudne, wskazuje się zwykle na deprywacje, przeciążenia, zagrożenia i utrudnienia. W warunkach tworzonych przez wskazane rodzaje sytuacji trudnych najczęściej wymagane są od jednostki działania szybkie, dobrze opanowane i zautomatyzowane. Spełnianie wyróżnionych kryteriów daje szanse na sprostanie wymaganiom tych sytuacji. Działania te będą odnosić się w szczególności do myślenia szybkiego realizowanego bezwiednie i w sposób nieuświadamiany[6]. Umożliwiają one bardziej skuteczne działania w neutralizowaniu i zwalczaniu zagrożeń w kontakcie z agresorem, pozwalają także na bardziej skuteczne formy prowadzenia interakcji mających charakter negocjacji w sytuacjach kryzysowych. Kompetencje komunikacyjne mają szczególne znaczenie w warunkach zagrożenia bezpieczeństwa jednostki, grup społecznych i większych zbiorowości w postaci narodu czy też państwa. Pozwalają one

[5] Tamże, s. 27.
[6] D. Kahneman, *Pułapki myślenia. O myśleniu szybkim i wolnym*, tłum. P. Szymczak, Poznań 2012.

na sprawne rozpoznanie sytuacji, intencji działań agresora oraz użycie adekwatnych do określonych warunków instrumentów komunikacyjnych. Stąd też uznaje się, że kompetencje komunikacyjne stanowią kluczowe instrumentarium użyteczne w warunkach zagrożenia[7].

Problematyka bezpieczeństwa jest nieodłącznie związana z kształtowaniem przebiegu codziennej ludzkiej egzystencji. Problematyka ta dotyczy bowiem możliwości korzystania przez człowieka z przywileju niezaburzonej egzystencji i rozwoju, jak też możności właściwego funkcjonowania w określonym świecie społecznym, a jednocześnie w świecie natury oraz tworzonym przez ludzi przyjaznym im w założeniu otoczeniu.

Można w tym miejscu powiedzieć, że „bezpieczeństwo, stanowiąc jedno z praw społecznych, jest niezbywalnym prawem człowieka. Prawa społeczne są wytworem moralnych i politycznych uzgodnień, które ludzie zawierają pomiędzy sobą, są wyrazem kompromisu, który oddaje istotę rozwoju cywilizacyjnego człowieka"[8]. Postawienie i udowodnienie tezy o prawie jednostki ludzkiej do prowadzenia bezpiecznej egzystencji wydaje się bezsporne w kontekście założeń, jakie odnaleźć można w teorii nauk o bezpieczeństwie. Jednakowoż na przykład już w odniesieniu do codziennej praktyki stwierdzić można, że bezpieczeństwo, które w ujęciu aksjologicznym ujmowane jest jako wartość nadrzędna dla człowieka, nie jest pojmowane aż tak bardzo jednoznacznie, jak twierdzą badacze problemów należących do sfery filozofii bezpieczeństwa[9].

Różnorodność zjawiska bezpieczeństwa i multidyscyplinarność jego postrzegania oraz definiowania wskazują na konieczność badania tego zjawiska z perspektywy naukowej. Mimo że bezpieczeństwo zapewne od zawsze stanowiło przedmiot zainteresowania człowieka i tworzonych przez niego zbiorowości i organizacji, to formalnie dopiero na początku XX w. odniesiono do tego zjawiska perspektywę typową dla zainteresowania naukowego, w postaci ujęcia zaprezentowanego przez przedstawicieli środowiska badaczy *security studies*.

W Polsce, w wyniku rozwoju prac nad systematyzacją dziedzin naukowych, w 2011 r. w ramach obszaru nauk społecznych i dziedziny nauk społecznych wyodrębnione zostały przykładowo takie dyscypliny, jak nauki o bezpieczeństwie, nauki o obronności, nauki o polityce, nauki o poznaniu i komunikacji społecznej. Nauki o bezpieczeństwie uznane zostały w efekcie za autonomiczną dyscyplinę naukową. Badania problemów bezpieczeństwa przed wejściem w życie wyżej wspomnianego rozporządzenia[10] były prowadzone głównie w naukach wojskowych i dyscyplinach

[7] W. Czajkowski, *Psychologia bezpieczeństwa. Komunikacyjne instrumenty wpływu społecznego* [w druku].

[8] A. Czupryński, *Bezpieczeństwo* w *ujęciu* aksjologicznym, [w:] *Bezpieczeństwo* na lądzie, morzu i w powietrzu w XXI wieku, red. J. Zboina, Józefów 2014, s. 11.

[9] Por. R. Rosa, *Zarys polskiej filozofii bezpieczeństwa na tle europejskiej myśli polem*ologicznej i irenologicznej, Siedlce 2009; J. Piwowarski, *Bezpieczeństwo jako stan oraz jako wartość*, [w:] *Bezpieczeństwo jako wartość*, red. I. Pabisz-Zarębska, J. Szewczyk, Kraków 2010.

[10] Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8 sierpnia 2011 r. w sprawie obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych (Dz.U. 2011, nr 179, poz. 1228 oraz 2011, nr 84, poz. 455. 3); Por.: *Nauka o bezpieczeństwie: istota, prze*d-

pokrewnych, ale można zauważyć, że wyodrębnienie dyscypliny nauk o bezpieczeństwie zintensyfikowało procesy badawcze w tej sferze.

Z dydaktycznego oraz pragmatycznego punktu widzenia wystąpiły w związku z tym działania wprowadzające nową jakość – zostały otwarte nowe kierunki studiów, których istotę stanowi kształcenie do realizacji zadań dotyczących kwestii bezpieczeństwa. Wskazuje to również na duże zapotrzebowanie społeczne w zakresie: poznania, zdefiniowania i prognozowania charakteru procesów służących podnoszeniu bezpieczeństwa.

Intensyfikacja działalności badawczej i dydaktycznej wynika zapewne z nagłego zwiększenia się w niestabilnych, jeśli chodzi o system wartości, ponowoczesnych społeczeństwach ich świadomości dotyczącej wzrostu zapotrzebowania na holistycznie[11] pojmowane bezpieczeństwo. Aby zagwarantować właściwy, zgodny ze społecznymi oczekiwaniami poziom bezpieczeństwa, należy jednak nieustannie prowadzić w tej dziedzinie naukowe badania. Nauki o bezpieczeństwie stały się dyscypliną naukową, na którą istnieje znaczące zapotrzebowanie społeczne. Bezpieczeństwo na dodatek, ze względu na powszechnie występującą potrzebę jego istnienia, wymaga poszukiwania naukowo uzasadnionych sposobów jego kształtowania we wszelkich sferach życia społecznego człowieka.

Przy próbach udzielania odpowiedzi na pytanie „czym jest bezpieczeństwo" uciekamy się do posługiwania się ujęciem pozytywnym lub negatywnym definiowania, opisu, wyjaśniania, klasyfikowania i praktycznego stosowania wiedzy dotyczącej tego zjawiska. Przeciwstawne względem siebie pojęcia – zagrożenie i bezpieczeństwo – wzajemnie zaświadczają o sobie i nie mogą egzystować odrębnie od siebie, ponieważ gdyby je odseparować, wtedy każde z tych zjawisk straciłoby znaczenie. W tym rozumieniu przeciwstawienie ich sobie podkreśla istotę każdego z nich z osobna. Jest to szczególnie ważne w przypadku bezpieczeństwa personalnego, istotnie powiązanego z koncepcją *human security* i nawiązującego do fenomenologiczno-egzystencjalnej interpretacji relacji społecznych jednostki[12]. Wskazując na normatywne warunki nawiązania kontaktu sugerujmy, że istnieją jakieś kryteria pozwalające pewne sytuacje wejścia w kontakt interpersonalny traktować jako lepsze od innych. Kryteria te opisywane są w kategoriach ontologicznych, epistemologicznych i aksjologicznych, ponieważ dotyczą podstawowych kwestii opisujących istnienie i działanie podmiotu w relacji z innymi osobami. Poza perspektywą filozoficzną równie użyteczna okazuje się perspektywa psychologiczna dotykająca wglądu jednostki w swoje działanie oraz rozumienia i wartościowania swoich relacji z in-

---

miot badań i kierunki rozwoju: studia i materiały, red. L. Grochowski, A. Letkiewicz, A. Misiuk, t. 1, Szczytno 2011.

[11] Holizm – filozoficzna koncepcja dotycząca rozwoju rzeczywistości, w której cały świat stanowi hierarchicznie ukształtowaną całość, złożoną z całości niższego rzędu, i podlega dynamicznej ewolucji, prowadzącej do powstawania coraz to nowych, jakościowo różnych całości, niedających się zredukować do sumy swych części składowych; za twórcę holizmu uważa się Jana Smutsa (1870–1950), wybitnego wojskowego, polityka i filozofa; Por.: J.C. Smuts, Holism and Evolution, London 1927.

[12] J. Piwowarski, W. Czajkowski, *Psychospołeczne i aksjologiczne determinanty kultury bezpieczeństwa służb mundurowych*, Słupsk 2015.

nymi[13]. Można oczekiwać, że normatywne warunki podjęcia kontaktu czynią bardziej prawdopodobnym nawiązanie konstruktywnych relacji społecznych, wolnych od wykorzystywania partnera. Z drugiej strony manipulowanie dotyczyć ma sytuacji sprowadzających się do realizowania własnych celów podmiotu, z dopuszczaniem intencjonalnego traktowania partnera w sposób przedmiotowy. Istotne jest również to, że partner w typowej sytuacji tak rozumianej manipulacji nie zdaje sobie sprawy z tego, że jest poddawany manipulowaniu. Kwestie te mają także odniesienia do problematyki poczucia bezpieczeństwa, które może być istotnie zaburzone podczas wejścia w kontakt z osobą manipulującą zachowaniem podmiotu.

We wskazanej koncepcji *human security* sygnalizuje się zmiany we współczesnym paradygmacie bezpieczeństwa w kierunku rozszerzenia jego zakresu podmiotowego i przedmiotowego oraz zmian w analizie jego aspektu obiektywnego i subiektywnego. Dotyczy to również redefinicji bezpieczeństwa narodowego w kierunku wyróżnienia dwu podmiotów: państwa i człowieka. W takim podejściu problematyka bezpieczeństwa państwa i bezpieczeństwa personalnego stanowią swoisty klucz do rozumienia funkcjonowania państwa i działań człowieka. Z drugiej strony człowiek i reprezentujące go grupy i zbiorowości społeczne (nie państwo) stanowi podstawowy podmiot bezpieczeństwa[14].

Badając bezpieczeństwo, badamy również zagrożenia jako czynniki mogące pozbawić podmiot bezpieczeństwa stanu stabilności i trwałości cenionych przez niego zasad, przekonań oraz wartości, w tym możliwości jego rozwoju. Dla świadomej identyfikacji i rozumienia poziomu zagrożeń i bezpieczeństwa podstawę stanowią założenia szwajcarskiego politologa Daniela Frei. Badacz ten postrzega następujące przypadki percypowania bezpieczeństwa:

1. stan braku bezpieczeństwa istnieje wówczas, gdy występuje względem *podmiotu bezpieczeństwa* duże rzeczywiste zagrożenie;
2. postrzeganie tego zagrożenia jest u podmiotu bezpieczeństwa prawidłowe;
3. stan obsesji występuje u podmiotu bezpieczeństwa wówczas, gdy nieznaczne zagrożenie jest postrzegane przez ten podmiot błędnie – jako zagrożenie duże;
4. stan fałszywego bezpieczeństwa ma miejsce wtedy, gdy zagrożenie względem podmiotu bezpieczeństwa ma poważny charakter, a postrzegane jest błędnie – jako niewielkie;
5. stan bezpieczeństwa występuje u danego podmiotu wówczas, gdy zagrożenie jest nieznaczne, zaś jego postrzeganie przez podmiot bezpieczeństwa jest prawidłowe[15].

Z analizy przytoczonych powyżej założeń wynika, że podstawą trafnego definiowania bezpieczeństwa jest jego postrzeganie oparte na istnieniu naukowych i ma-

[13] W. Czajkowski, *Poczucie bezpieczeństwa w relacji społecznej*, [w:] *Realizacja zadań bezpieczeństwa. Jakość, prakseologia, praworządność*, red. J. Piwowarski, A. Czop, J. Kaleta, Kraków 2014, s. 7–24.

[14] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa,* red. A. Urbanek, Słupsk 2013, s. 59.

[15] D. Frei, Sicherheit. Grundfragen der Weltpolitik, Stuttgart 1977, s. 17–21; podajemy za: J. Piwowarski, *Transdyscyplinarna istota kultury bezpieczeństwa narodowego*, Słupsk 2016, s. 360.

jących obiektywne podstawy przesłanek. Dlatego też w niniejszej pracy autorzy przedstawili różne aspekty procesu postrzegania bezpieczeństwa – począwszy od jego identyfikacji poprzez poznanie i definiowanie oraz określenie jego założeń badawczych. Niezależnie od podkreślenia obiektywnych podstaw opisu i wyjaśniania problematyki bezpieczeństwa, warto także pamiętać o potrzebie doceniania i uwzględniania jej subiektywnego wymiaru. W interpretacji psychologicznej poczucie zagrożenia należałoby definiować jako subiektywny stan podmiotu sprowadzający się do odczuwania negatywnych emocjonalnie doznań wynikających z działających na podmiot bodźców. W takiej interpretacji rozumie się szeroko działające na jednostkę bodźce, ujmując w tej kategorii również te, które ograniczają się wyłącznie do stanów wewnętrznych jednostki w postaci wrażeń, spostrzeżeń i wyobrażeń. Taka interpretacja jest istotna o tyle, że poczucie zagrożenia może być stanem subiektywnym, niemającym zobiektywizowanego, zewnętrznego uwarunkowania. Można wskazać sytuacje, w których ktoś doznaje ekstremalnie silnego poczucia zagrożenia wówczas, gdy inni nie odczuwają takiego stanu[16].

Pojęcie bezpieczeństwa ma zarówno charakter aksjologiczny, jak i ontologiczny, a z punktu widzenia nauki o poznaniu – charakter metodologiczny. W rozumieniu aksjologicznym bezpieczeństwo stanowi system wartości i ocen regulujących działania podmiotu. W sensie ontologicznym bezpieczeństwo rozpatruje się jako proces.

Natomiast z metodologicznego punktu widzenia określa się, jakimi metodami można badać problematykę dotyczącą kwestii bezpieczeństwa. Poniżej przytaczamy tak zwaną spektralną definicję fenomenu bezpieczeństwa sformułowaną przez Juliusza Piwowarskiego[17]. Definicja proponowana przez tego badacza identyfikuje bezpieczeństwo z użyciem czterech pomocniczych pojęć, pozwalających na wielorodzajowe ujęcie kategorii reprezentującej jeden z najważniejszych w egzystencji ludzkiej fenomenów.

Spektralna definicja bezpieczeństwa

Bezpieczeństwo dla jednostkowego lub zbiorowego podmiotu bezpieczeństwa to dotyczący go wieloaspektowy fenomen, którego spektrum tworzą następujące ujęcia**:**

- **pożądany stan**, który dla danego podmiotu określa poziom efektywności kontroli nad możliwymi w danym miejscu i przedziale czasu zagrożeniami wartości istotnych dla tego podmiotu; inaczej mówiąc, jest to stan wynikający z istniejącej w danym miejscu czasoprzestrzeni różnicy dwóch przeciwstawnych czynników – potencjału autonomicznej obronności podmiotu z jednej strony i potencjału zagrożeń dla realizacji spełnienia potrzeb podmiotu z drugiej (*aspekt epistemologiczny*);

[16] W. Czajkowski, *Psychologia bezpieczeństwa…*, s. 9.

[17] J. Piwowarski, Ochrona VIP-*a a czworokąt Bushido. Studium japońskiej k*ultury bez*pieczeństwa*, [w:] *Bezpieczeństwo osób podlegających ustawowo ochronie wobec zagrożeń XXI wieku*, red. P. Bogdalski, J. Cymerski, K. Jałoszyński, Szczytno 2014; J. Piwowarski, Prolegomena do ba*dań nad kulturą bezpieczeństwa*, „Security, Economy & Law" 2013, nr 2.

- **wartość**, która umożliwia podmiotowi bezpieczeństwa zaspokajanie jego potrzeb niższych i wyższych, w tym potrzeby nieustannego rozwoju, włącznie z samorealizacją znajdującą się na szczycie hierarchii potrzeb (*aspekt aksjologiczny*);
- **proces rozwoju**, dzięki któremu realizowany jest personalny i społeczny aspekt wzrostu potencjału autonomicznej obronności podmiotu bezpieczeństwa (*aspekt ontologiczny*);
- **konstrukt społeczny**, fenomen, który umożliwia przeciwstawienie się zagrożeniom, będący efektem istnienia społecznych więzów, współzależności oraz interakcji zachodzących w zbiorowości społecznej (*aspekt społeczny*).

We wskazanej spektralnej definicji bezpieczeństwa, w naszym rozumieniu, podejmuje się próbę wszechstronnej interpretacji opisywanego i wyjaśnianego problemu, pojmując go w kategoriach stanu, wartości, procesu rozwoju i konstruktu społecznego. Widać wyraźnie, że prezentowana definicja stanowić może dobry punkt wyjścia do konstruowania modelu działania jednostki w warunkach zagrożenia podstawowych wartości. Z drugiej strony definicja ta, jako swoisty punkt wyjścia, może służyć jako użyteczne narzędzie do opisu, wyjaśniania i przewidywania zachowań jednostki w takich sytuacjach. Wskazywana kategoria podstawowych wartości jest klarownie prezentowana w koncepcji S.H. Schwartza. Konstruowany model ma zawierać w sobie następujące piętra analizy kompetencji jednostki:

- nadawanie sensu doświadczeniom jednostki przez podmiot;
- nabywanie i doskonalenie kompetencji służących do oceny zdarzeń i obiektów;
- nabywanie i doskonalenie kompetencji służących planowaniu działań;
- nabywanie i doskonalenie kompetencji służących selekcji strategii działania;
- nadawanie struktury strategiom działania;
- analiza i interpretacja realizacji celów działania;
- nabywanie i doskonalenie kompetencji kontroli własnego działania i działania innych osób;
- nabywanie i doskonalenie kompetencji rozróżniania wartości jawnych i ukrytych jako odrębnych regulatorów działania.

Ostatnia z kategorii kompetencji wyróżniona w proponowanym modelu stanowić ma zasadnicze użyteczne narzędzie opisu, wyjaśniania i przewidywania zachowań jednostki.

Budowany model nawiązuje istotnie do koncepcji rozumienia i interpretowania wartości przez S.H. Schwartza[18], który definiuje je jako poznawczą reprezentację celu mającego motywacyjne znaczenie dla podmiotu oraz ponadsytuacyjny charakter. Zgodnie z interpretacją Schwartza większość autorów zgadza się w kwestii posiadania przez nie pięciu poniższych podstawowych charakterystyk.

Wartości są przekonaniami bądź pojęciami, które

- dotyczą pożądanych celów, opisujących ostateczne stany rzeczy lub zachowania;

[18] S.H. Schwartz, An Overview of the Schwartz Theory of Basic Values, "Online Readings in Psychology and Culture" 2012, 2(1), http://dx.doi.org/10.9707/2307-0919.1116 (dostęp: 15.12.2016).

- przekraczają konkretne sytuacje;
- kierują selekcją i oceną zachowań i zdarzeń;
- są uporządkowane według ważności;
- zachowaniem kieruje względna ważność wielu wartości[19].

W analizie kontekstów związanych z zagrożeniem bezpieczeństwa zakładamy kluczowe znaczenie czynników służących radzeniu sobie z zagrożeniami. Tworzymy modelowe pojęcie sytuacji/poczucia zagrożenia z eksponowaniem perspektywy subiektywnej, co jest sygnalizowane poprzez termin poczucie zagrożenia. Jest to niezbywalny warunek tworzenia modelu odniesionego do pojęcia bezpieczeństwa personalnego, zgodny z interpretacją podejmowaną w koncepcji *human security*. W modelu tym uwzględniamy wartości jako instrument radzenia sobie z poczuciem zagrożenia, podobnie traktujemy wzór zachowania A (WZA jako instrument radzenia sobie z poczuciem zagrożenia, którym też jest utrata bądź obniżenie kontroli otoczenia i swojego zachowania; odnosimy WZA do zmiennych behawioralnych). Kolejna zmienna uwzględniana w modelu to osobowość, następna to zawarta w powyższej zmienna temperamentu. Pamiętamy także o uwarunkowaniach kulturowych. Jeszcze jedna znacząca zmienna istotna dla budowy modelu dotyczy świadomości siebie i własnego działania przez podmiot.

Spostrzeganie i interpretacja problematyki bezpieczeństwa wymaga także przyjmowania perspektywy kulturowej i uwzględniania różnic międzykulturowych. Wydaje się to szczególnie istotne w przypadku budowania modelu bezpieczeństwa personalnego. Przyjmowanie uniwersalnego punktu widzenia może być zasadne w sytuacji dążenia do pewnej standaryzacji kategoryzowania problematyki bezpieczeństwa dotyczącej zgeneralizowanych norm kulturowych i prawnych, oderwanych od indywidualnych właściwości człowieka w postaci jego statusu, pochodzenia czy miejsca zamieszkania. Jednakże poziom bezpieczeństwa jednostki zwykle spostrzega się w kategoriach subiektywnych, ponieważ taka jest specyfika funkcjonowania jednostki i odczuwania jej właściwości i charakterystyk przez nią samą. Subiektywność spostrzegania bezpieczeństwa zasługuje na pozytywną kategoryzację, co związane jest z posiadaniem przez jednostkę swoistych potrzeb i oczekiwań wynikających ze znajdowania się przez nią na określonym poziomie stanu oraz procesu bezpieczeństwa. Obciążenia wynikające z subiektywności związanej z perspektywą spostrzegania rzeczywistości jednostki przez pryzmat swoich właściwości i cech są widoczne w wielu kontekstach i interpretacjach odniesionych do działania człowieka. Zwraca się uwagę na możliwości odwoływania się do swoistych kryteriów bezpieczeństwa, co pozwala na częściowe uniknięcie tego obciążenia związanego z subiektywnością. Czy możemy odnosić się do standardów bezpieczeństwa i czy możemy im przypisać wartości je klasyfikujące, np. wysoki, średni lub niski poziom bezpieczeństwa? Odpowiadając na takie pytanie, należy jednak wskazać na problem związany z faktem, że wybierane kryteria także podlegają obciążeniu związanemu z subiektywizmem.

[19] Por. J. Cieciuch, *Kształtowanie się systemu wartości od dzieciństwa do wczesnej dorosłości*, Warszawa 2013.

Dążenia do parametryzacji, klasyfikacji i uściślenia stają się współcześnie czymś typowym i jednocześnie stanowiącym swego rodzaju pożądany wzorzec działania. Wydaje się jednak, że realizowanie takiego podejścia, szczególnie w obszarze nauk społecznych i naukach o bezpieczeństwie, może się okazać bezzasadne. Wskazane obawy wynikają w głównej mierze z interpretacji dokonywanych w obszarze bezpieczeństwa personalnego. W takich interpretacjach wymiar indywidualny powiązany z subiektywnym punktem widzenia oraz dostrzeganiem perspektywy poczucia, w sensie psychologicznym, zasługuje na uwagę i docenienie. Równocześnie warto także wskazać na znaczenie metod jakościowych pozwalających na dostęp do informacji trudnych do uzyskania na drodze badań ilościowych. Indywidualne i grupowe funkcjonowanie jednostek ma swoją niezbywalną specyfikę, trudną do parametryzacji w związku z odczuciami subiektywnymi. Warto także wskazać na interpretację dokonywaną poza metodologią badań jakościowych w odniesieniu do tzw. klimatu bezpieczeństwa, który w dużej mierze może być wyznaczony kategoriami organizacyjnymi i kulturowymi[20].

Podjętą wyżej kwestię parametryzacji problematyki bezpieczeństwa należy odnieść do zasadniczego nurtu interpretacyjnego autorów pracy, którzy sugerują potrzebę uwzględniania zmiennych kulturowych w analizie bezpieczeństwa personalnego.

Bibliografia

Bezpieczeństwo osób podlegających ustawowo ochronie wobec zagrożeń XXI wieku, red. P. Bogdalski, J. Cymerski, K. Jałoszyński, Szczytno 2014.

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, red. S. Koziej i in., Biuro Bezpieczeństwa Narodowego, Warszawa 2013.

Cieciuch J., *Kształtowanie się systemu wartości od dzieciństwa do wczesnej dorosłości*, Warszawa 2013.

Cieślarczyk M., *Kultura bezpieczeństwa i obronności*, Siedlce 2010.

Czajkowski W., *Interpersonal Framework of Establishing Contact in Psychotherapy*, [w:] M. Kliś, J. Kossewska, W. Czajkowski, *Studies on Communication and copping with Stress*, Kraków 2006.

Czajkowski W., *Poczucie bezpieczeństwa w relacji społecznej*, [w:] *Realizacja zadań bezpieczeństwa. Jakość, prakseologia, praworządność*, red. J. Piwowarski, A. Czop, J. Kaleta, Kraków 2014.

Czajkowski W., *Psychologiczne mechanizmy działania jednostki w sytuacji zagrożenia*, Katowice 2014.

[20] Profesor Dove Zohar opublikował wyniki badań dotyczących *klimatu bezpieczeństwa* (1980); zdefiniował pojęcie i zaproponował skale pomiaru, które są standardem w tej dziedzinie. Zohar prowadzi projekty badawcze w wielu krajach, koncentruje się na rozwoju klimatu organizacyjnego i kultury, nowych strategii przywództwa służących rozwojowi *klimatu bezpieczeństwa*; seria analiz (ponad 200 prac) wskazuje, że *klimat bezpieczeństwa* stanowi najistotniejszą zmienną w kontekstach mentalno-duchowych i społecznych, wpływających na wypadki w pracy – http://ie.technion.ac.il/Home/Users/dzohar.html (dostęp: 11.11.2016).

Czajkowski W., *Psychologia bezpieczeństwa. Komunikacyjne instrumenty wpływu społecznego* [w druku].
Czupryński A., *Bezpieczeństwo w ujęciu aksjologicznym*, [w:] *Bezpieczeństwo na lądzie, morzu i w powietrzu w XXI wieku*, red. J. Zboina, Józefów 2014.
Frei D., *Sicherheit. Grundfragen der Weltpolitik*, Stuttgart 1977.
Kahneman D., *Pułapki myślenia. O myśleniu szybkim i wolnym*, tłum. P. Szymczak, Poznań 2012.
Nauka o bezpieczeństwie: istota, przedmiot badań i kierunki rozwoju: studia i materiały, red. L. Grochowski, A. Letkiewicz, A. Misiuk, Szczytno 2011.
Piwowarski J., *Bezpieczeństwo jako stan oraz jako wartość*, [w:] *Bezpieczeństwo jako wartość*, red. I. Pabisz-Zarębska, J. Szewczyk, Kraków 2010.
Piwowarski J., *Prolegomena do badań nad kulturą bezpieczeństwa*, „Security Economy & Law" 2013, nr 2.
Piwowarski J., *Ochrona VIP-a a czworokąt Bushido. Studium japońskiej kultury bezpieczeństwa*, [w:], *Bezpieczeństwo osób podlegających ustawowo ochronie wobec zagrożeń XXI wieku*, red. P. Bogdalski J. Cymerski, K. Jałoszyński, Szczytno 2014.
Piwowarski J., *Transdyscyplinarna istota kultury bezpieczeństwa narodowego*, Słupsk 2016.
Piwowarski J., Czajkowski W., *Psychospołeczne i aksjologiczne determinanty kultury bezpieczeństwa służb mundurowych,* Słupsk 2015.
Rosa R., *Zarys polskiej filozofii bezpieczeństwa na tle europejskiej myśli polemologicznej i irenologicznej,* Siedlce 2009.
Smuts J.C., *Holism and Evolution*, London 1927.
Wybrane problem bezpieczeństwa. Dziedziny bezpieczeństwa, red. A. Urbanek, Słupsk 2013.

Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8 sierpnia 2011 r. w sprawie obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych (Dz.U. 2011, nr 179, poz. 1228 oraz 2011, nr 84, poz. 455. 3).

http://ie.technion.ac.il/Home/Users/dzohar.html (dostęp: 11.11.2016).
Schwartz S.H., *An Overview of the Schwartz Theory of Basic Values.* "Online Readings in Psychology and Culture" 2012*,* 2(1), http://dx.doi.org/10.9707/2307-0919.1116 (dostęp: 15.12.2016).

Summary

The authors of the present study examine the mechanisms regulating individual behavior under conditions of difficult and emergency situations. Instinctive and conscious activities, which are used to meet the need for security, are interpreted by invoking a category of personal knowledge and is an important instrument to deal with the requirements of the situation. In the personality structure, these are regulatory standards and mechanisms for assessing and evaluating objectives and ways of subjects' actions. Attention is also drawn to the social relations of the individual and socio-cultural conditions of constructive behaviors and behaviors which constitute acts of manipulation. This

is particularly important in the process of personal security interpretation and application and strictly connected with the human security concept related to the phenomenological and existential interpretation of subjects' social relations. In the security context the authors suggest the need to consider the issue of values involved in the ability to assess relationships with other people.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 17–32 ROK 2017

ISSN 2543–7321

Andrzej Urbanek

Akademia Pomorska
Słupsk
andrzej.urbanek@apsl.edu.pl

TSUNAMI – ZAGROŻENIE EKOLOGICZNE BEZPIECZEŃSTWA POWSZECHNEGO

TSUNAMI – AN ECOLOGICAL THREAT OF THE PUBLIC SAFETY

***Zarys treści*:** Bezpieczeństwo powszechne zaliczane jest obecnie do kluczowych dziedzin bezpieczeństwa narodowego. Jego głównym celem staje się ochrona ludności przed skutkami różnego rodzaju zagrożeń, które mogą się pojawić na terytorium Polski, ale także poza jej granicami. Do tego typu zagrożeń można zaliczyć niewątpliwie fale tsunami, które są najczęściej następstwem trzęsień ziemi czy wybuchów podwodnych wulkanów. Autor w artykule podjął się próby analizy omawianego zjawiska z perspektywy bezpieczeństwa powszechnego.

***Słowa kluczowe*:** bezpieczeństwo powszechne, bezpieczeństwo ekologiczne, zagrożenia naturalne, tsunami

Key words: public safety, ecological safety, natural threats, tsunami

Wstęp

Współczesny człowiek narażony jest każdego dnia na różnego rodzaju zagrożenia, które w zależności od okoliczności i skali wystąpienia określonego zjawiska mogą przybrać rozmiar klęski żywiołowej czy też katastrofy. Powszechność skutków tego typu zdarzeń i sytuacji powoduje, że stają się one przedmiotem zainteresowania ważnej dziedziny bezpieczeństwa narodowego, jaką jest niewątpliwie bezpieczeństwo powszechne.

Sam termin „bezpieczeństwo powszechne" nie doczekał się jeszcze jasnej i powszechnie uznanej definicji, zatem trudno jest jednoznacznie określić, jakie działania o charakterze obronnym, ochronnym czy ratowniczym wchodzą w zakres kompetencji instytucji zapewniających bezpieczeństwo wszystkim bez wyjątku obywatelom.

Brak powyższej definicji powoduje ponadto, że trudno jest jednoznacznie sklasyfikować wszystkie zagrożenia, które wpisują się w przestrzeń bezpieczeństwa powszechnego. Wątpliwości wśród teoretyków i praktyków bezpieczeństwa nie budzi jednakże fakt, że do zagrożeń bezpieczeństwa powszechnego zaliczyć można zagrożenia ekologiczne naturalnego pochodzenia, a wśród nich i zjawisko tsunami.

Tsunami, podobnie jak inne zagrożenia ekologiczne, które mogą przybrać postać klęski żywiołowej, interesuje specjalistów od bezpieczeństwa powszechnego w Polsce, pomimo że ryzyko powstania fal tsunami na Bałtyku, które mogłyby siać spustoszenie na polskim wybrzeżu jest niewielkie. Wynika to z faktu, że polscy obywatele, wykonując obowiązki zawodowe bądź w celach turystycznych coraz częściej znajdują się w tych rejonach naszego globu, gdzie ryzyko to jest stosunkowo wysokie. Poznanie istoty tego zjawiska z perspektywy sekuritologicznej staje się więc koniecznością, dlatego też autor artykułu dokonał jego analizy na podstawie dostępnej literatury i materiałów źródłowych, w tym materiałów prasowych, które szczegółowo informowały opinię publiczną o skali zagrożenia i skutkach fal tsunami, które pustoszyły wybrzeża państw na brzegach Oceanu Indyjskiego w 2004 r. czy wybrzeża Japonii w 2009 r.

Bezpieczeństwo powszechne i jego zagrożenia

Analizując zagrożenia z perspektywy systemu powszechnej ochrony ludności, nie sposób pominąć kwestii współczesnego podejścia do istoty bezpieczeństwa powszechnego. Bezpieczeństwo powszechne określa się najczęściej jako stan zapewniający ochronę życia i zdrowia obywateli oraz majątku publicznego i infrastruktury krytycznej przed skutkami klęsk żywiołowych czy też katastrof technicznych. Pojęcie bezpieczeństwa powszechnego jest przez to zbliżone do pojęcia bezpieczeństwa ekologicznego i różni się w praktyce przedmiotem zainteresowań wymienionych dziedzin bezpieczeństwa, bowiem o ile bezpieczeństwo ekologiczne zajmuje się szeroko rozumianym środowiskiem naturalnym, o tyle przedmiotem zainteresowań bezpieczeństwa powszechnego jest zdrowie i życie obywateli, a szerzej ochrona i obrona obywateli przed skutkami różnego rodzaju zagrożeń[1].

Z perspektywy bezpieczeństwa narodowego bezpieczeństwo powszechne jest traktowane jako proces obejmujący „[…] szereg różnorodnych działań (m.in. w dziedzinach: zdrowotnej, ekologicznej, edukacyjnej, społecznej, gospodarczej, prawnej, psychologicznej, weterynaryjnej i sanitarnej), którego zasadniczym celem jest zapewnienie bezpieczeństwa ludności cywilnej, a zarazem stanem uzyskanym w wyniku zorganizowanej ochrony życia i zdrowia ludzi, także dóbr materialnych i kulturalnych oraz środowiska naturalnego – w zakresie niezbędnym do przetrwania ludzi”[2].

---

[1] Zob.: *Bezpieczeństwo wewnętrzne RP w ujęciu systemowym i zadań administracji publi*cznej, red. B. Wiśniewski, S. Zalewski, Bielsko-Biała 2006, s. 32–33.

[2] W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe* kategorie. Uwarunkowania. System, Warszawa 2011, s. 56.

Analizując powyższe definicje można przyjąć tezę, że głównym przedmiotem zainteresowań bezpieczeństwa powszechnego jest system ochrony ludności, któremu próbuje się w Polsce nadać formalnoprawny charakter.

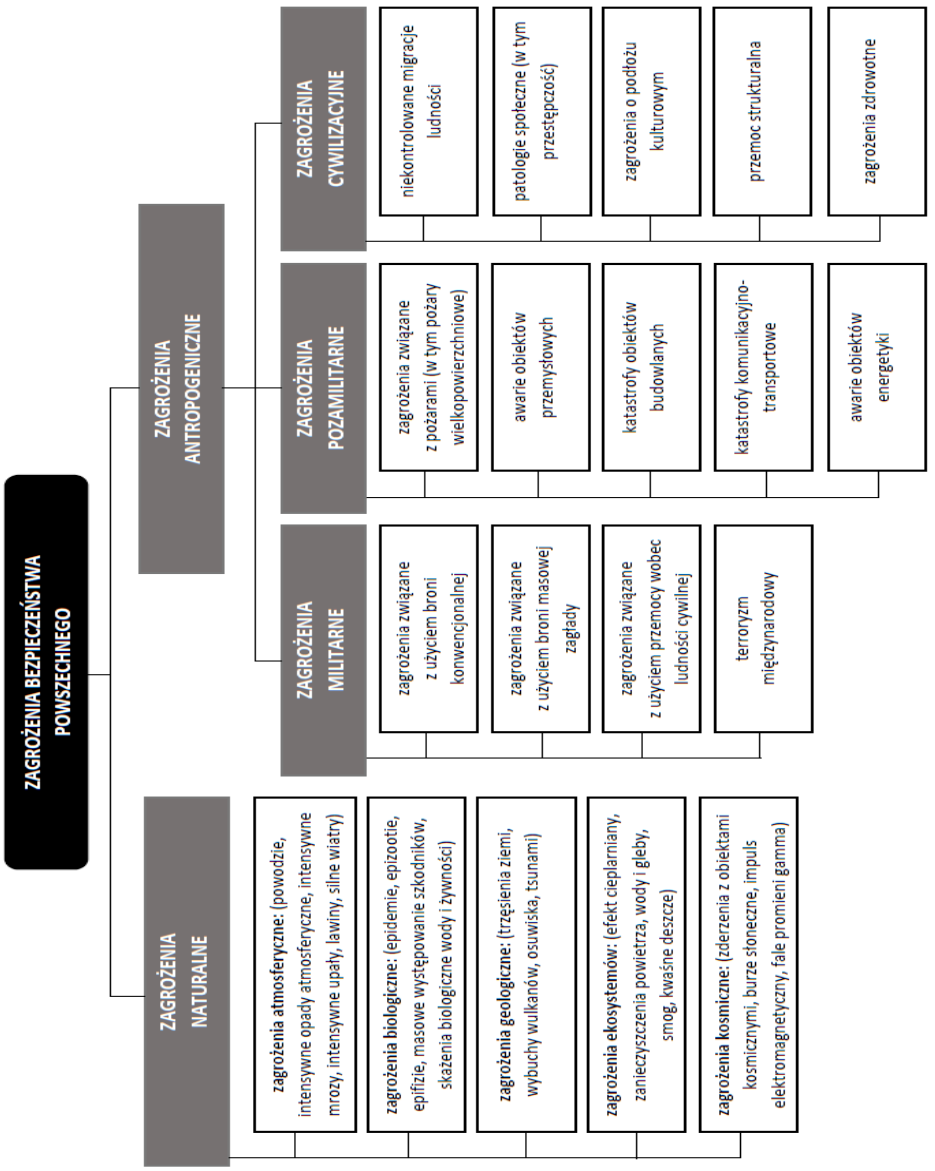
Pierwszej takiej próby podjęto się w 2006 r., kiedy w projekcie ustawy o bezpieczeństwie *obywateli i zarządzaniu kryzysowym* termin „ochrona ludności" zdefiniowano w kategoriach działań praktycznych jako „[…] podejmowanie niezbędnych przedsięwzięć ukierunkowanych na ochronę ludzi, mienia, środowiska i infrastruktury krytycznej przed skutkami katastrof naturalnych i awarii technicznych, zdarzeń o charakterze terrorystycznym, a w przypadkach bezpośredniego zewnętrznego zagrożenia państwa i wojny, zapewnienie warunków koniecznych do przetrwania". W takim ujęciu ochrona ludności, jak podaje się dalej w przedmiotowym projekcie ustawy, ma mieć „[…] charakter powszechny oraz interdyscyplinarny, wyrażający się w skoordynowanym użyciu sił i środków, będących w dyspozycji organów władzy publicznej, przedsiębiorców, organizacji społecznych i humanitarnych oraz poszczególnych obywateli"[3]. Nieco inaczej ochronę ludności definiuje się w projekcie *ustawy o ochronie ludności i obronie cywilnej* z 2016 r. W projekcie tym można przeczytać, że przez ochronę ludności należy rozumieć „[…] zintegrowaną działalność organów administracji publicznej właściwych w sprawach ochrony ludności i podmiotów realizujących zadania mających na celu ochronę życia i zdrowia ludności przebywającej na terytorium Rzeczypospolitej Polskiej oraz ochronę mienia, środowiska naturalnego i dziedzictwa kulturowego w przypadku wystąpienia zagrożenia, oraz obronę cywilną jako przygotowanie i realizacja zadań ochrony ludności po wprowadzeniu stanu wojennego i w czasie wojny określonych ustawą z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz.U. z 2015 r. poz. 827, z późn. zm.) oraz realizację zadań z zakresu zarządzania kryzysowego określonych w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2013 r. poz. 1166, z późn. zm.)"[4].

Z powyższych definicji wynika, że celem działań dotyczących ochrony ludności w ramach bezpieczeństwa powszechnego jest podejmowanie niezbędnych przedsięwzięć ukierunkowanych na ochronę ludzi, mienia, środowiska i infrastruktury krytycznej przed skutkami różnego rodzaju zagrożeń pojawiających się zarówno po wprowadzeniu stanu wojennego czy też już w czasie wojny, jak i zagrożeń pojawiających się w czasie pokoju i to nie tylko na terytorium naszego kraju, ale również poza jego granicami. Nakłada to na stosowne instytucje obowiązek analizy i oceny ryzyka różnego rodzaju zagrożeń, ostrzeganie o możliwości ich pojawienia, a także dostarczenie do powszechnej wiadomości informacji na temat zachowania się w sytuacji ich wystąpienia.

W tym układzie lista zagrożeń bezpieczeństwa powszechnego jest bardzo długa. Zaliczamy do nich zarówno destrukcyjne działania, których sprawcą jest człowiek, jak i czynniki destrukcyjne będące efektem oddziaływania sił natury. Można je rów-

[3] Projekt ustawy o bezpieczeństwie obywateli z 2006 r., dostępny na stronie: http://orka.sejm.gov.pl/proc. nsf/projekty/805_p.htm (dostęp: 20.01.2017).

[4] Projekt ustawy o ustawy o ochronie ludności i obronie cywilnej z 2016 r., dostępny na stronie: www. ock.gov.pl/prawo/projekty_aktow_prawnych (dostęp 20.01.2017).



Rys. 1. Klasyfikacja zagrożeń bezpieczeństwa powszechnego
Fig. 1. Classification of ecological threats to public safety
Źródło: opracowanie własne.

nież klasyfikować przedmiotowo, chociażby w kategoriach zagrożeń politycznych, militarnych, ekonomicznych, społeczno-kulturowych czy ekologicznych[5]. Wpływ na omawianą dziedzinę bezpieczeństwa mają również zagrożenia asymetryczne, takie jak: terroryzm międzynarodowy, transnarodowa przestępczość zorganizowana, możliwość użycia broni masowego rażenia przez podmioty pozapaństwowe, a także zagrożenia cyberprzestrzeni, w tym cyberterroryzm. Ogólną klasyfikację zagrożeń bezpieczeństwa powszechnego zestawiono na rysunku 1.

Na liście zagrożeń bezpieczeństwa powszechnego na szczególną uwagę zasługują zagrożenia ekologiczne naturalnego pochodzenia. Lista takich zagrożeń jest bardzo długa. Stosując kryterium przedmiotowe, zagrożenia te można podzielić na naturalne (klęski i katastrofy żywiołowe) i cywilizacyjne (np. zanieczyszczenie powietrza, gleby, wód, awarie i katastrofy techniczne). Zagrożenia ekologiczne są groźne, złożone, występują z reguły na znacznych obszarach, są niezmiernie dynamiczne, zagrażają nie tylko zdrowiu i życiu człowieka, ale całej biosferze danego obszaru[6].

Szczególnym rodzajem zagrożeń ekologicznych są zagrożenia pochodzenia geologicznego, wśród których wyróżnia się: trzęsienia ziemi, wybuchy wulkanów, osuwiska czy też fale tsunami. W niniejszym opracowaniu podjęto się próby przybliżenia zjawiska tsunami, które stanowi dla wielu krajów poważny czynnik zagrożeń bezpieczeństwa powszechnego, a w dobie globalizacji i dużej intensywności chociażby ruchu turystycznego może dotknąć niemalże wszystkich mieszkańców naszej planety, o czym przekonaliśmy się w 2004 r.

Pojęcie i istota tsunami

Tsunami, jak wspomniano wcześniej, to zjawisko zaliczane do kategorii katastrof naturalnych o geologicznym pochodzeniu. Według powszechnie obowiązującej definicji fale tsunami to takie, które powstają za sprawą gwałtownego zaburzenia całej kolumny wody w zbiorniku. Mogą być one indukowane bądź od dołu (bottom-up) – między innymi poprzez zmianę ukształtowania dna morskiego w wyniku trzęsienia ziemi, wybuchu wulkanu lub podmorskiego osuwiska (typowych zjawisk geologicznych) – bądź też od góry (top-down) – za sprawą chociażby upadku meteorytu lub ruchów masowych na lądzie, ale równie dobrze w wyniku podwodnego lub nawodnego wybuchu ładunku jądrowego o dużej lub wielkiej mocy[7]. Fale rozchodzą się promieniście od źródła powstania z wielką prędkością (400–1000 km/h); na otwartym oceanie tsunami osiągają wysokość 1–2 m (maksymalnie 8 m), w pobliżu lądu do 30–50 m[8]. Pod względem genetycznym tsunami traktuje się jako fale sejsmiczne.

---

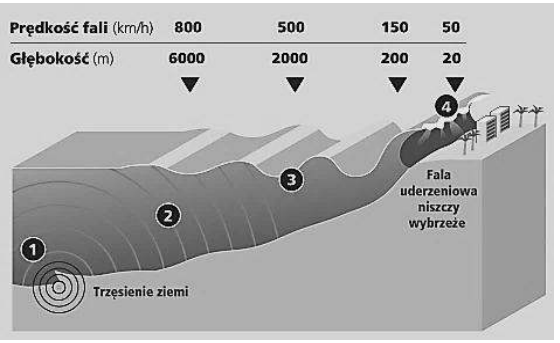
[5] Por.: *Niemilitarne zagrożenia bezpieczeństwa publicznego*, red. S. Kowalkowski, Warszawa 2011.

[6] E. Nowak, M. Nowak, Zarys teorii bezpi*eczeństwa narodowego*, Warszawa 2011, s. 127–128.

[7] Por. P. Łuczyński, *Problem tsunamitów. Dlaczego tak mało jest kopalnych osadów tsunami*?, „Przegląd Geologiczny" 2012, t. 60, nr 11, s. 598–604.

[8] http://encyklopedia.pwn.pl/haslo/3989752/tsunami.html (dostęp: 20.05.2014).

Fale tsunami charakteryzują się znaczną długością, rzędu kilkunastu – stukilkudziesięciu tysięcy metrów, a ich wysokość na otwartym, głębokim oceanie wynosi, jak wspomniano wcześniej, kilka metrów. Ze względu na ich wielkie długości prędkość przemieszczania tych fal jest stosunkowo duża (rzędu kilkuset km na godzinę) i nawet na dużych głębokościach przemieszczają się jako fale płytkowodzia. Stromość fal tsunami na otwartych, głębokich wodach jest bardzo mała, dlatego na takich akwenach nie stanowią jakiegokolwiek zagrożenia dla statków. Dopiero w chwili dojścia do strefy brzegowej poruszająca się z dużą prędkością fala długa staje się falą przyboju o stromym czole, a jej wysokość wzrasta. Wzrost wysokości fali tsunami uzależniony jest od początkowej wysokości (energii fali), szerokości i nachylenia strefy przybrzeża, w której zachodzi dyssypacja energii fali oraz od topografii linii brzegowej. W skrajnych przypadkach wysokość fali tsunami sięgać może kilkunastu metrów. Szczególnie wysokie fale tsunami obserwuje się w sytuacjach, gdy wąski, dość stromo nachylony szelf przylega do zatok w linii brzegowej. W zatoce dochodzi bowiem do dodatkowego spiętrzenia wody. Nadejście fali tsunami zazwyczaj poprzedzone jest szybkim obniżeniem lustra wody o 1–4 metry, które trwa od kilku do kilkunastu minut, po czym następuje gwałtowne i szybkie podnoszenie się poziomu morza, zakończone nadejściem fali tsunami wysokości kilku – kilkunastu metrów. Zazwyczaj najwyższa jest pierwsza fala tsunami, po której może przyjść kilka kolejnych, o coraz mniejszej wysokości[9]. Niszczycielskie działanie tsunami objawia się w strefie przybrzeżnej, gdzie tworzą one wysoki, stromy wał wody, uderzający w brzeg z dużą prędkością i zmiatający wszystko po drodze. Szczególnie narażone na zniszczenia są urządzenia hydrotechniczne, infrastruktura portowa, statki znajdujące się w portach i na płytkich, przyportowych redach. Mechanizm tworzenia się fal tsunami przedstawiono graficznie na rysunku 2.



Etapy powstawania fal tsunami inicjowanych od dołu (bottom-up):

1. Trzęsienie ziemi lub podwodny wybuch wulkanu powoduje powstanie fali.
2. Fale przemieszczają się swobodnie w kierunku lądu.
3. Fala załamuje się na płytkich wodach przybrzeżnych i osiąga duże rozmiary.
4. Fala tsunami uderza i zalewa wybrzeże z ogromną siłą, siejąc na swojej drodze spustoszenie.

Rys. 2. Mechanizm tworzenia się fal tsunami w wyniku podwodnego trzęsienia ziemi
Fig. 2. The mechanism of formation of a tsunami as a result of underwater earthquakes
Źródło: M. Grad, *Trzęsienia ziemi i tsunami*, „Przegląd Geofizyczny" 2005, nr 50(1-2), s. 47–58, grafika: http://infografika.wp.pl/title,Zabojcze-tsunami, wid,14401809, wiadomosc.html (dostęp: 20.07.2014).

[9] M. Grad, Fale tsunami, Katedra Meteorologii i Oceanografii Nautycznej WM WSM w Gdyni, http://ocean.am.gdynia.pl/student/oceano1/falo/fal_tsun.html (dostęp: 20.05.2014).

Wyróżnia się na ogół, uwzględniając genezę i miejsce powstania fali, trzy rodzaje tsunami[10]:

- lokalne – miejsce wzbudzenia fali znajduje się blisko wybrzeża, a czas jej przybycia do lądu wynosi do pół godziny;
- regionalne – fale mogą zagrozić większemu obszarowi przybrzeżnemu; czas przybycia do lądu wynosi do 5 godzin od wzbudzenia;
- ponadregionalne (pacyficzne) – mogą objąć wiele obszarów po obu stronach Pacyfiku; czas przybycia fali do lądu wynosi od kilku do kilkunastu godzin, w zależności od odległości wzbudzenia.

Większość wstrząsów, które zdolne są wygenerować fale tsunami, jest związana ze strefami kolizji płyt tektonicznych litosfery. Te zaś okalają cały Ocean Spokojny (80% wszystkich fal tsunami pojawia się na Pacyfiku), a także północno-wschodnią część Oceanu Indyjskiego. Występują także w basenie Morza Karaibskiego na Oceanie Atlantyckim[11]. Stosunkowo często, choć o niewielkiej sile, występują fale tsunami na Morzu Śródziemnym, zwłaszcza przy wybrzeżach Północnej Afryki (Algeria, Maroko), gdzie strefa przybrzeżna wykazuje stale niewielką aktywność sejsmiczną[12].

Skutki tsunami

Czynnikiem wywołującym bezpośrednie, destrukcyjne dla otoczenia skutki w przypadku tsunami są ogromne fale, które docierając do lądu mogą osiągać wysokość kilkudziesięciu metrów. Falom tsunami mogą towarzyszyć też zjawiska wtórne, takie jak skażenie środowiska wywołane np. przez uszkodzenia zakładów przemysłowych (przemysłu chemicznego), a nawet, jak to miało miejsce w Fukushimie, uszkodzenie reaktorów elektrowni jądrowej.

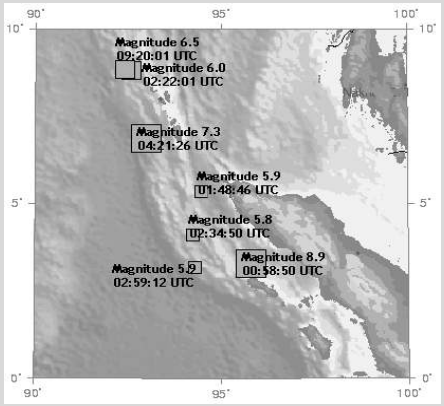
Skutki tsunami, podobnie zresztą jak trzęsień ziemi, można podzielić na bezpośrednie (natychmiastowe) i pośrednie (długoterminowe); mogą one mieć charakter skutków społecznych, ekonomicznych i ekologicznych.

Do **skutków bezpośrednich** zaliczyć można: utratę życia, trwałe kalectwo, utratę zdrowia, urazy psychiczne wśród ludności; całkowite lub częściowe zniszczenie budynków i ich wyposażenia na skutek zalania lub zasypania; zniszczenia infrastruktury komunikacyjnej (drogi, linie kolejowe, mosty); uszkodzenia sieci gazowej, wodociągowej, elektrycznej; zniszczenia infrastruktury portowej, w tym statków i łodzi.

Skutki pośrednie obejmują z kolei: wszelkie szkody wywołane samym żywiołem i towarzyszącymi mu zjawiskami wtórnymi; długotrwały proces odbudowy infrastruktury regionu; wysokie koszty pomocy humanitarnej; możliwość wybuchu epidemii w rejonach objętych działalnością żywiołu; skażenia, zniszczenia lub całkowitą destrukcję środowiska.

---

[10] M. Graniczny, W. Mizerski, Katastrofy przyrodnicze, Warszawa 2009, s. 80.
[11] Tamże, s. 79.
[12] M. Grad, Fale tsunami…



Data:	26 grudnia 2004
Godzina:	7:58:53 czasu lokalnego w Dżakarcie i Bangkoku
Przyczyna:	trzęsienie ziemi
Epicentrum trzęsienia:	Ocean Indyjski
Siła trzęsienia:	9,1 w skali Richtera
Państwa dotknięte kataklizmem:	Indonezja, Sri Lanka, Tajlandia, Indie, Malediwy, Somalia, Birma, Malezja
Liczba ofiar:	około 300 tys.

Trzęsienie ziemi o magnitudzie 9,1 w skali Richtera, którego epicentrum znajdowało się 30 km pod dnem Oceanu Indyjskiego w pobliżu zachodniego wybrzeża północnej Sumatry wywołało fale tsunami, które w ciągu trzech godzin uderzyły w wybrzeża kilku państw Azji Południowo-Wschodniej, a później także Afryki. Sięgające 15 m fale zniszczyły nadmorskie wsie i miasteczka, a także kąpieliska odwiedzane o tej porze roku przez zagranicznych turystów.

Kraje najbardziej dotknięte tsunami.
Źródło: http://commons.wikimedia.org/wiki/2004_Indian_Ocean_earthquake

Skutki: około 300 tysięcy ofiar śmiertelnych. Dziesiątki tysięcy osób zaginęły. Miliony straciły dach nad głową oraz miejsca pracy. Organizacje humanitarne stwierdziły, że co trzecia ofiara kataklizmu była dzieckiem. Wśród ofiar znalazły się tysiące turystów z całego świata, którzy spędzali razem z dziećmi Boże Narodzenie na słonecznych plażach Oceanu Indyjskiego. Woda zniszczyła plaże, roślinność, miasta i wioski leżące na wybrzeżu. W Indonezji zniszczeniu uległo miasto Banda Aceh, stolica prowincji Aceh. Straty i koszty odbudowy oceniono na kilka bilionów dolarów.

Ramka 1. Niszczycielskie tsunami na Oceanie Indyjskim z 2004 r.
Frame 1.The devastating tsunami in the Indian Ocean in 2004

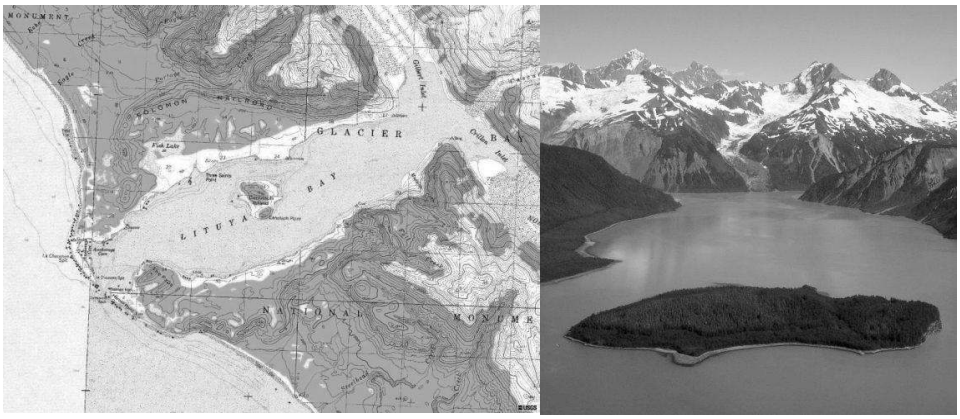
Źródło: http://walrus.wr.usgs.gov/tsunami/sumatraEQ/, http://earthquake.usgs.gov/ earthquakes/ eqinthenews/ 2004/us2004slav/ (dostęp: 20.07.2014).

W przypadku zmian środowiskowych istotnym problemem staje się erozja terenów dotkniętych kataklizmem. Erozja spowodowana falą tsunami dotyczy przede wszystkim przybrzeża, plaży, przylądków oraz ujść rzek i kanałów. Zasoleniu ulega ponadto grunt i wody podziemne. Są to zmiany, których skutki mogą być odczuwalne przez wiele lat, a niektóre mogą być nieodwracalne[13].

[13] W. Szczuciński, *Potencjalne skutki geologiczne i środowiskowe tsunami na wybrzeżu Bałtyku*, [w:] Holoceńskie przemiany wybrzeży *i wód po*łudniowego Bałtyku – przyczyny, uwarunkowania i skutki, red. K. Rotnicki, J. Jasiewicz, M. Woszczyk, Poznań–Bydgoszcz 2008, s. 121–127.

Najtragiczniejsze w skutkach w ciągu ostatnich lat było tsunami na Sumatrze w 2004 r. Wywołało je podwodne trzęsienie ziemi o magnitudzie 9,1 stopnia w skali Richtera, którego hipocentrum znajdowało się ok. 30 km pod dnem Oceanu Indyjskiego w pobliżu zachodniego wybrzeża północnej Sumatry. Główny wstrząs nastąpił 26 grudnia 2004 r. o godzinie 07.58 czasu lokalnego w Dżakarcie i w Bangkoku. Według sejsmologów było to czwarte pod względem siły trzęsienie ziemi od roku 1900, od którego prowadzi się ciągłe obserwacje sejsmiczne. Trzęsienie ziemi wywołało fale tsunami, które w ciągu trzech godzin uderzyły w wybrzeża kilku państw Azji Południowo-Wschodniej, a później także Afryki. Sięgające 15 m fale zniszczyły nadmorskie wsie i miasteczka, a także kąpieliska odwiedzane o tej porze roku przez zagranicznych turystów. Szacuje się, że liczba osób zabitych i zaginionych wynosi ponad 300 tysięcy i nie jest to ostateczny bilans tragedii. Kilka milionów straciło dach nad głową[14]. Informacje dotyczące kataklizmu zestawiono w ramce 1.

Megatsunami miało jednak miejsce nie na Oceanie Indyjskim, a w Zatoce Lituya na Alasce 9.06.1958 r. O potraktowaniu tego zjawiska w kategorii „mega" zadecydowało odnotowanie nieznanej do tej pory wysokości fali, która osiągnęła wartość 524 m. Lituya Bay to fiord leżący w amerykańskim stanie Alaska. Zatokę odkrył w 1786 r. Jean-François de La Pérouse[15].



Rys. 3. Zatoka Lituya na Alasce
Fig. 3. Lituya Bay in Alaska

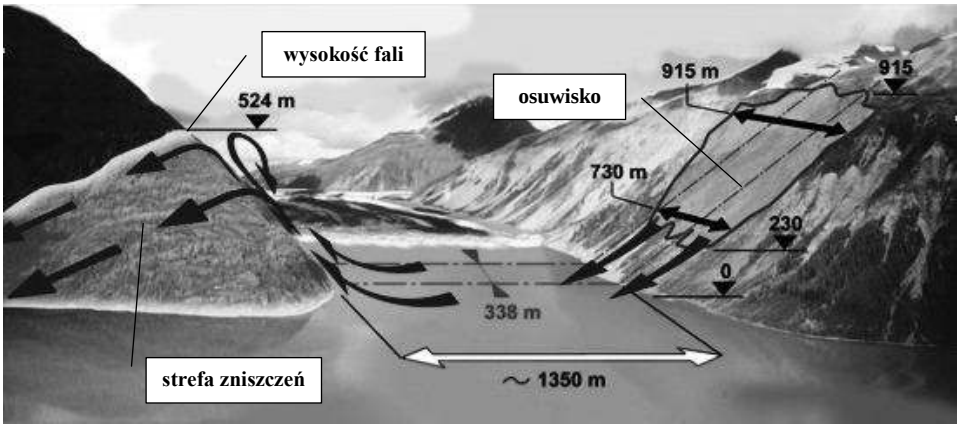
Źródło: mapa: Wenatchee Valley College, Introduction to Physical Geology, http://commons.wvc.edu/ rdawes/G101OCL/Labs/GlaciersLab.html (dostęp: 20.05.2014); zdjęcie: Northwest Coast Archaeology, http://qmackie.com/ 2010/02/22/la-perouse-at-port-des-francais-lituya-bay/ (dostęp: 20.05.2014).

[14] Opracowano na podstawie danych z NOAA's National Weather Service. www. tsunami.gov/ (dostęp: 20.05.2014).

[15] J-F. La Pérouse, A Voyage Around the World, t. 1, London 1799, s. 364–416. Zob.: E.W. Eickelberg, Lituya Bay, Gulf of Alaska, "U.S. Coast and Geodetic Survey FIELD ENGINEERS BULLETIN" No. 10, December 1936, dostępny na stronie: NOAA, http://www.history.noaa.gov/stories_tales/lituya.html (dostęp: 20.05.2014).

Lituya Bay ma około 11,3 km długości i 3,2 km szerokości. Największa głębokość zatoki to 219 m, przy czym ujście do Zatoki Alaska mierzy zaledwie 9,7 m głębokości i ma około 500 m szerokości. Zatoka jest miejscem zejścia trzech lodowców: dwóch mniejszych Kaskadowego i Crillon oraz największego z nich – Lituya. W centrum zatoki leży wyspa Cenotaph, która w znaczący sposób wpływa na kształt prądów. Zatoka jest częścią Parku Narodowego Glacier Bay na Alasce[16] (zob.: rys. 3).

W nocy 9 lipca 1958 r. trzęsienie ziemi wzdłuż uskoku Fairweather wywołało osunięcie się do zatoki Gilberta około 30 mln m^3 skał o wadze ponad 900 mln ton. Obryw skał z wysokości blisko 900 m wywołał lokalne tsunami, które z największą siłą uderzyło w przeciwległy brzeg i podążyło dalej w kierunku otwartego oceanu, zdzierając ze zbocza miliony drzew i glebę. Trzęsienie ziemi miało siłę 7,9 stopnia w skali Richtera z epicentrum 21 km na północny wschód od zatoki. Niszczycielska fala osiągnęła wielkość 524 m[17] (zob.: rys. 4).



Rys. 4. Mechanizm niszczycielskiego działania tsunami w zatoce Lituya na Alasce
Fig. 4. The mechanism of the destructive action of the tsunami in Lituya Bay in Alaska

Źródło: G. Pararas-Carayannis, Mega-Tsunami 9 lipca 1958 roku w Lituya Bay, Alaska, Analiza mechanizmu, http://www. drgeorgepc.com /Tsuna-mi1958LituyaB.html (dostęp: 20.05.2014).

Zagrożenie tsunami w Polsce

Czy Polska jest wolna od zagrożenia tsunami? To pytanie nie jest wcale bezzasadne. Co prawda prawdopodobieństwo wystąpienia tego zjawiska jest znikome, ale nie można go całkowicie wykluczyć. Przy spełnieniu pewnych warunków towarzyszących trzęsieniu ziemi, fale tsunami mogłyby się na Bałtyku pojawić, jednak by-

[16] http://en.wikipedia.org/wiki/Lituya_Bay (dostęp: 20.05.2014).
[17] Szerzej o mechanizmie powstania największej zanotowanej fali tsunami: G. Pararas-Carayannis, Mega-Tsunami 9 lipca 1958 roku w Lituya Bay, Alaska, Analiza mechanizmu, www.drgeorgepc. com /Tsuna-mi1958LituyaB.html (dostęp: 20.05.2014).

łyby to fale o niedużej wysokości. Tsunami mogłoby wywołać trzęsienie ziemi o magnitudzie 5–6 lub większej w skali Richtera, z epicentrum pod dnem morskim, a do takich zjawisk już na Bałtyku dochodziło[18], o czym świadczą zapiski w kronikach[19]:

- w 1625 r. nastąpiło zapadnięcie murów miejskich i jednego budynku w Szczecinie;
- 25 lutego 1648 r. jedna z wież kościelnych w rejonie Szczecina został przesunięta o 7 metrów;
- 16–17 maja 1888 r. trzęsienia ziemi objęły zachodni Bałtyk;
- w grudniu 1912 r. wystąpił silny wstrząs sejsmiczny w okolicach Łeby i Smołdzina.

Według historycznych zapisków tsunami, zwane przez historyków „Morskim Niedźwiedziem", wystąpiło w Polsce przynajmniej dwukrotnie: w 1497 oraz w 1779 r.

Jeden z opisów historycznych „Morskiego Niedźwiedzia" powstał w Darłowie (Zachodniopomorskie) i dotyczy roku 1497. Jego autorem jest jeden z mnichów zamieszkujących tamtejszy klasztor kartuzów. Przetłumaczony przez Mariana Czernera zapis brzmi następująco: „Ósmego dnia po Narodzinach Maryi, roku 1497, w piątek w południe, zerwał się sztorm z północnego zachodu i trwał do późnego wieczora wywołując powódź. W Darłówku zostały całkowicie zniszczone nabrzeża portowe, paraliżując na długi czas handel. Ich odbudowa pociągnęła za sobą wysokie koszty. Prawie wszystkie domy zostały rozmyte, wszystko bydło potonęło, a rzeczka (Lutowa łącząca Wieprzę z jeziorem Kopań) została zapiaszczona. Cztery cumujące w porcie statki, w tym duży 'Kreyer' zostały wyrzucone na ląd. Jeden koło Żukowa Morskiego, dwa koło klasztoru kartuzów, jeden aż w pobliżu kaplicy Św. Gertrudy. W klasztorze woda stała w krużgankach i w kościele do wysokości ołtarzy"[20]. Szacuje się, że wysokość tego tsunami wynosiła około 20 metrów, bowiem jeden ze statków wylądował prawie na szczycie miejscowego wzgórza Kopa, które liczy 22 metry n.p.m.

W kwietniu 1779 r. tsunami nawiedziło z kolei Wybrzeże Trzebiatowskie. Jak podaje kronikarz L. W. Brueggemann: „Bałtyk posiada także często swoją własną pogodę, która z pogodą lądową nie ma związku; czasami jednakże tylko rzadko, występuje podwodna burza w tymże (Bałtyku), o czym można wnioskować z tego, że przy czystym i spokojnym niebie, daje się słyszeć wzdłuż pomorskich brzegów morskich toczący się grzmot, a na ląd wyrzucane są nieżywe lub na wpół żywe ryby morskie i przybrzeżne. Tak było np. 3 kwietnia 1757 r. około południa przy spokojnej i jasnej pogodzie, brzeg Bałtyku koło Trzebiatowa nad Regą stał się nagle tak wzburzony, że wysokie fale zerwały duży prom zacumowany w porcie i przeniosły daleko na ląd. Po czym kiedy to (falowanie) się trzykrotnie powtórzyło morze stało się znowu spokojne"[21]. Inny historyczny przekaz mówi o tym, że w marcu 1779 r.

[18] Zob.: Tsunami w Polsce, za: www.ekologia.pl (dostęp: 15.04.2015).
[19] M. Graniczny, W. Mizerski, *Katastrofy przyrodnicze…*, s. 86.
[20] Podaję za: *Badania: przez Bałtyk przeszło tsunami – przekazy kronikarzy potwierdzają się*, PAP – Nauka w Polsce, http://naukawpolsce.pap.pl/ (dostęp: 15.04.2015).
[21] Za: *Sejsmiczny Bałtyk*, http://szkolnictwo.pl/ (dostęp: 15.04.2015).

wysokie fale zalały Łebę i uniosły zacumowany w tamtejszym porcie statek do miejskich ogrodów, zaś trzy godziny później w Kołobrzegu nastąpił nagły odpływ wód, odsłaniający dno morza[22].

Przyczyną tsunami w Darłowie, zdaniem niektórych naukowców, było oddalone o 500 km na północ trzęsienie ziemi w rejonie jeziora Wener w Szwecji. Siła trzęsienia ziemi była tam jednak zbyt mała, aby bezpośrednio spowodować tsunami. Można przyjąć najbardziej prawdopodobną tezę, że to słabe trzęsienie wywołało eksplozję metanu uwięzionego w warstwach tworzących dno Morza Bałtyckiego. Eksplozji metanu towarzyszył grzmot, huk, czyli „pomruk niedźwiedzia morskiego" – jak dawniej określano efekty dźwiękowe poprzedzające nadejście fali tsunami. Najbardziej prawdopodobny jest scenariusz powtórzenia się wybuchu tej specyficznej „bomby metanowej" i powstania tsunami na Bałtyku. Nie zlokalizowano jednak na razie pod Bałtykiem złóż mogących zagrażać w najbliższym czasie naszemu bezpieczeństwu. Inną przyczyną tsunami może być upadek meteorytu do Morza Bałtyckiego, niemniej jednak ryzyko takiego zdarzenia jest niewielkie.

Ochrona przed tsunami

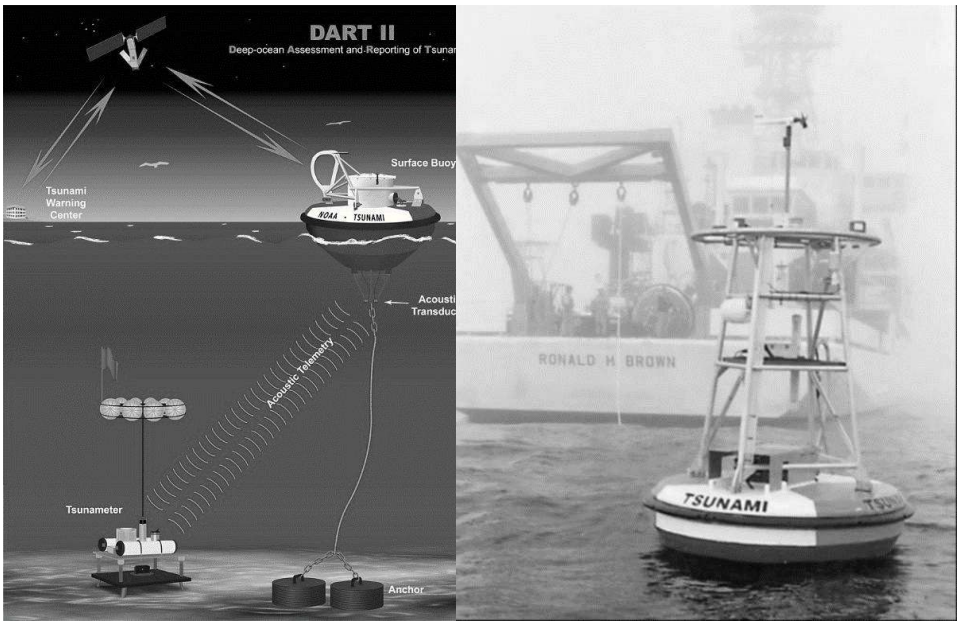
Ochrona przed tsunami ma na celu ograniczenie jego skutków i obejmuje działania związane z monitoringiem, tworzeniem systemu ostrzegania i alarmowania, a także rozmieszczaniem i utrzymaniem w sprawności urządzeń zabezpieczających wybrzeża przed niszczycielskim działaniem ogromnych mas wody (falochronów, nasypów, ścian betonowych na morzu, ścian na wybrzeżu).

Najważniejszym, a jednocześnie o największym zasięgu systemem monitorowania i ostrzegania przed tsunami jest amerykański system DART (Deep-ocean Assessment and Reporting of Tsunami). Obejmuje on obecnie (od 2008 r.) sieć 39 stacji, zainstalowanych m.in. w regionie Hawajów i Wysp Salomona, dostarczających informacji o groźbie fal tsunami w czasie rzeczywistym, jakie mogą dosięgnąć wybrzeży Oceanu Spokojnego, Zatoki Meksykańskiej, Karaibów, Indonezji i Australii. W realizację projektu zaangażowanych jest 26 krajów. Systemem tym zawiaduje Amerykańska Narodowa Służba Oceaniczna i Meteorologiczna – NOAA (National Oceanic and Atmospheric Administration). Obecnie wdrożono do użytku już drugą generację systemu – DART II.

System DART II to technologia opracowana przez NOAA Pacific Marine Environmental Lab (PMEL) w Seattle. Opiera się ona na integracji pomiarów w czasie rzeczywistym i technologii modelowania zagrożeń. System ten umożliwia wczesne wykrywanie w czasie rzeczywistym tsunami na otwartym oceanie. System DART składa się głównie z tsunamometru i boi umieszczonej na powierzchni. Tsunamometr usytuowany jest na dnie oceanu i zawiera komputer, modem i przetwornik akustyczny (komunikacji), czujnik ciśnienia, czujnik pochylenia (do ustalenia nachylenia tsunamometru) oraz baterie. W stanie czuwania tsunamometr monitoruje głębokość wody do pławy umieszczonej na powierzchni co 15 minut. Boja przekazuje do sate-

[22] Za: Tsunami w Polsce, www.ekologia.pl (dostęp: 15.04.2015).

litów informacje, które są następnie przekazywane do ośrodków ostrzegania i alarmowania o tsunami (ośrodek taki znajduje się na Hawajach). Gdy tsunamometr wyczuwa trzęsienie ziemi, przechodzi w tryb alarmowy i rozpoczyna pomiar oraz raportowanie wysokości powierzchni morza nawet co 15 sekund (zob. rys. 5)[23].



Rys. 5. System monitorowania i wczesnego ostrzegania przed tsunami DART II
Fig. 5. Deep-ocean Assessment and Reporting of Tsunamis DART II
Źródło: http://www.srh.noaa.gov/srh/jetstream/tsunami/images/dartbuoyth.jpg, http://www. magazine.noaa.gov/stories/images/dart_tsunamicover.jpg (dostęp: 20.05.2016).

W 2005 r., z inicjatywy Komisji Oceanograficznej UNESCO, 31 zainteresowanych krajów atlantyckich i śródziemnomorskich zaczęło tworzyć system ostrzegania podobny do amerykańskiego DART. System został już przetestowany. UNESCO uruchomiło też Międzynarodowe Centrum Informacji o Tsunami (International Tsunami Information Center)[24].

Podsumowanie i wnioski

Tsunami należy niewątpliwie do jednych z poważniejszych zagrożeń naturalnego pochodzenia zagrażających mieszkańcom wybrzeży dużych zbiorników wodnych, głównie mórz i oceanów. W warunkach globalizacji, a przede wszystkim swobodnego przemieszczania się wielu milionów ludzi w celach zawodowych czy turystycz-

[23] Za: www.ndbc.noaa.gov/dart/dart.shtml (dostęp: 15.04.2015).
[24] Zob.: http://itic.ioc-unesco.org/index.php (dostęp: 15.04.2015).

nych, nabiera ono powszechnego charakteru i to w skali globalnej. Poznanie tego zjawiska i tworzenie skutecznych systemów ochrony ludności przed jego destrukcyjnym działaniem wpisuje się w problemy, które powinny być analizowane z perspektywy bezpieczeństwa powszechnego. Problem ten nie może być bagatelizowany czy marginalizowany przez stosowne służby w Polsce, dlatego warto pokusić się o pewne wnioski, które nasuwają się w wyniku analizy powyższego problemu przedstawionej przez jej autora:

1. Ryzyko pojawienia się fal tsunami na Bałtyku jest niewielkie, niemniej jednak nie można tego zagrożenia wykluczyć z katalogu zagrożeń bezpieczeństwa powszechnego i należy przygotować odpowiednie służby do działania w sytuacji, gdyby sprawdziły się najczarniejsze scenariusze.
2. Polska powinna aktywnie uczestniczyć w programach o charakterze globalnym (Globalny monitoring środowiska i bezpieczeństwa – GMES) czy regionalnym (Europejska Sieć Informacji i Obserwacji Środowiska Morskiego – EMODnet) zajmujących się monitoringiem i analizą środowiska morskiego, a także różnego rodzaju zagrożeń pojawiających się w tej przestrzeni. Przykładem takiego programu jest program SatBałtyk, w którym uczestniczy między innymi Akademia Pomorska w Słupsku. Warto zastanowić się, czy w projekcie tym nie uwzględnić również obserwacji dotyczących zjawiska tsunami.
3. Nie mniej ważnym problemem jest kwestia edukacji społeczeństwa o zagrożeniach powodowanych tsunami, a przede wszystkim o odpowiednich sposobach zachowania się w rejonach, gdzie tego typu zjawiska mogą wystąpić. Informacje takie powinny być dostępne chociażby na stronach internetowych Ministerstwa Spraw Zagranicznych czy też polskich placówek dyplomatycznych funkcjonujących w krajach, gdzie zjawisko to może wystąpić. Informacje tego typu powinny być dostępne głównie dla osób, które udają się rejony zagrożone wystąpieniem tego kataklizmu.
4. Informacje, w tym ostrzeżenia o zagrożeniu tsunami, powinny być również przekazywane przez polskie media, aby dać możliwość zapoznania się z nimi osobom przebywającym w rejonach o wysokim stopniu ryzyka lub udającym się tam.

Bibliografia

*Bezpieczeństwo wewnętrzne RP w ujęciu systemowym i zadań administracji publicz*nej, red. B. Wiśniewski, S. Zalewski, Bielsko-Biała 2006.

Graniczny M., Mizerski W., Katastrofy przyrodnicze, Warszawa 2009.

Kitler W., *Bezpieczeństwo narodow*e RP. Podstawowe kategorie. Uwarunkowania. System, Warszawa 2011.

Łuczyński P., *Problem tsunamitów. Dlaczego tak mało jest kopalnych osadów ts*unami?, „Przegląd Geologiczny" 2012, t. 60, nr 11.

Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.

Niemilitarne zagrożenia bezpieczeństwa publicznego, red. S. Kowalkowski, Warszawa 2011.

Szczuciński W., *Potencjalne skutki geologiczne i środowiskowe tsunami na wybrzeżu*

Bałtyku, [w:] *Holoceńskie przemiany wybrzeży i wód południowego Bałtyku* – przyczyny, uwarunkowania i skutki, red. K. Rotnicki, J. Jasiewicz, M. Woszczyk, Poznań–Bydgoszcz 2008.

Projekt ustawy o bezpieczeństwie obywateli z 2006 r., http://orka.sejm.gov.pl/ proc. nsf/projekty/805_p.htm (dostęp: 20.01.2017).

Projekt ustawy o ustawy o ochronie ludności i obronie cywilnej z 2016 r., www.ock. gov.pl/prawo/projekty_aktow_prawnych (dostęp: 20.01.2017).

Eickelberg E. W., Lituya Bay, Gulf of Alaska, "U.S. Coast and Geodetic Survey FIELD ENGINEERS BULLETIN" no. 10, December 1936, NOAA, www.history.noaa. gov/ stories_tales/lituya.html (dostęp: 20.05.2014).

Grad M., Fale tsunami, Katedra Meteorologii i Oceanografii Nautycznej WM WSM w Gdyni, http://ocean.am.gdynia.pl/student/oceano1/falo/fal_tsun.html (dostęp: 20.05.2014).

Pararas-Carayannis G., Mega-Tsunami 9 lipca 1958 roku w Lituya Bay, Alaska, Analiza mechanizmu, www.drgeorgepc.com/Tsuna-mi1958LituyaB.html (dostęp: 20.05.2014).

Sejsmiczny Bałtyk, http://szkolnictwo.pl (dostęp: 15.04.2015).

Tsunami w Polsce, www.ekologia.pl (dostęp: 1504.2015).

http://encyklopedia.pwn.pl/haslo/3989752/tsunami.html (dostęp: 20.05.2014).

http://itic.ioc-unesco.org/index.php (dostęp 15.04.2015).

http://en.wikipedia.org/wiki/Lituya_Bay (dostęp: 20.05.2014).

www.ndbc.noaa.gov/dart/dart.shtml (dostęp: 15.04.2015).

www. tsunami.gov/ (dostęp: 20.05.2014).

Summary

Public safety is included in the key areas of national security. The main objective is to protect the population against the effects of the various risks that may threaten Polish territory, but also territory outside Polish borders. In these type of threats we can undoubtedly include tsunami waves, which are often the consequence of earthquakes and eruptions of underwater volcanoes. In the article, the author attempts to analyze this phenomenon from the perspective of public safety.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 33–44 ROK 2017

ISSN 2543–7321

Anna Rychły-Lipińska

Akademia Pomorska
Słupsk
arychly@wp.pl

MODEL BEZPIECZEŃSTWA JEDNOSTKI WE WSPÓŁCZESNYM ZMIENIAJĄCYM SIĘ OTOCZENIU – WSTĘPNE ROZWAŻANIA

THE MODEL OF HUMAN SECURITY IN THE TURBULENT ENVIRONMENT – PRELIMINARY CONSIDERATIONS

***Zarys treści*:** Bezpieczeństwo to pewien stan, który gwarantuje istnienie jednostki oraz możliwość jej rozwoju. Jest to jedna z podstawowych potrzeb człowieka, której niezaspokojenie wywołuje niepokój i poczucie zagrożenia. Współczesne pojęcie bezpieczeństwa ma coraz większy wymiar. Obecnie bezpieczeństwo to nie tylko aspekty polityczne, wojskowe, gospodarcze, techniczne, ekologiczne czy społeczne. W artykule przedstawiony został model ukazujący bezpieczeństwo jednostki (człowieka) funkcjonującej w danym otoczeniu.
***Słowa kluczowe*:** bezpieczeństwo człowieka, otoczenie, model bezpieczeństwa jednostki
Key words: human safety, environment, human security model

Wstęp

Z czym kojarzy się termin bezpieczeństwo? Pierwsze skojarzenie z nim związane to brak jakiegokolwiek zagrożenia, a szczególnie brak zagrożenia ze strony innych państw, z zapewnieniem porządku publicznego, z właściwym funkcjonowaniem organów państwowych. Pierwsze skojarzenie to spojrzenie na ten termin w sposób ogólny – makroekonomiczny, ze szczególnym uwzględnieniem stosunków politycznych, prawnych, administracyjnych. Przy próbie dokładniejszego wyjaśnienia pojęcia bezpieczeństwo pojawiają się określenia, iż bezpieczeństwo to również stabilność ekonomiczna danego państwa gwarantująca zapewnienie podstawowych warunków bytowych społeczeństwu. Z zapewnieniem tych warunków związane jest właśnie bezpieczeństwo jednostki, czyli człowieka. Odczucia poszczególnych ludzi dotyczące bezpieczeństwa, jakie daje im państwo są świadectwem jego prawidłowego lub

nieprawidłowego funkcjonowania. W związku z powyższym śmiało można uznać, iż na poczucie bezpieczeństwa jednostki składa się nie tylko brak zagrożeń zewnętrznych, ale również inne czynniki, do których można m.in. zaliczyć:

- stabilną sytuację materialną, czyli stałe zatrudnienie i wynagrodzenie wystarczające na zapewnienie średniego standardu życia,
- zapewnioną opiekę medyczną oraz socjalną,
- właściwie funkcjonujące służby ustanowione do zapewnienia porządku publicznego, zapobiegania i ścigania przestępczości,
- perspektywę godziwego życia w wieku emerytalnym,
- możliwość egzekwowania prawa.

Niedostateczne zapewnienie przez państwo realizacji któregokolwiek z tych czynników powoduje frustrację, zmuszając jego obywateli do poszukiwania lepszych warunków bytowych poza granicami kraju, co związane jest często z destabilizacją życia rodzinnego, frustracją spowodowaną brakiem możliwości aktywnego, bezpośredniego uczestniczenia w codziennych sprawach rodziny[1].

Bezpieczeństwo znajduje się w sferze podstawowych potrzeb człowieka, stojąc wysoko w hierarchii wartości egzystencjalnych. Można je rozpatrywać w kategoriach jednostkowych, grupowych, narodowych i międzynarodowych. Bezpieczeństwo jednostki w dużej mierze zależy od kondycji gospodarczej kraju, w którym ona funkcjonuje, od środowiska naturalnego, czynników społecznych i kulturowych[2].

Andrzej Urbanek[3] opisuje szeroko tematykę dotyczącą bezpieczeństwa jednostki, czyli bezpieczeństwa osobistego, ludzkiego czy inaczej personalnego (human security). Teorię human security dzieli się na dwie szkoły: japońską oraz kanadyjską (popularyzowaną przez Norwegię). Japonia zaadaptowała koncepcję bezpieczeństwa personalnego w 1997 r., jej przedstawiciele koncentrują się na kwestii freedom from want (dotyczy wzmocnienia wysiłków na rzecz radzenia sobie z takimi zagrożeniami dla ludzkiego życia, jak np. ubóstwo, degradacja środowiska, handel narkotykami, choroby zakaźne, napływ uchodźców). Natomiast podejście kanadyjskie skłania się w kierunku freedom from fear (nacisk na wojskowe interwencje humanitarne w celu ochrony życia i praw jednostek).

Termin human security upowszechnił Program Narodów Zjednoczonych ds. Rozwoju (UNDP) z 1994 r., w którym przyjęto między innymi, że:

- jest to koncepcja uniwersalna, dotycząca wszystkich ludzi na świecie,
- wszystkie jego wymiary są współzależne i ściśle ze sobą powiązane,
- bezpieczeństwo jednostki jest łatwiejsze do zapewnienia przez wcześniejszą prewencję niż późniejszą interwencję,
- human security koncentruje się na bezpieczeństwie człowieka, a nie państwa.

---

[1] A. Fiałkowska, *Bezpieczeństwo człowieka wobec współczesnych zagrożeń*, Europejski Instytut Bezpieczeństwa, http://eib.edu.pl/bezpieczenstwo-czlowieka-wobec-wspolczesnych-zagrozen/ (dostęp: 12.01.2015).

[2] M. Tryboń, I. Grabowska-Lepczak, M. Kwiatkowski, *Bezpieczeństwo człowieka w obliczu zagrożeń XXI wieku*, www.zn.sgsp.edu.pl/41/12.pdf (dostęp: 03.04.2017).

[3] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, red. A. Urbanek, Słupsk 2013, s. 41–59; tenże, *Współczesny człowiek w przestrzeni bezpieczeństwa*, Słupsk 2015, s. 129–172.

Autorka, studiując literaturę z zakresu bezpieczeństwa stara się odpowiedzieć na pytanie: Co składa się na poczucie bezpieczeństwa jednostki i czy jesteśmy w stanie wymienić pewne jego elementy składowe?

Podstawowe definicje opisujące model bezpieczeństwa jednostki

Bezpieczeństwo ekonomiczne – związane jest z osiągnięciem podstawowego dochodu zapewniającego przetrwanie, zrównoważony rozwój i godność osobistą. W tym znaczeniu mowa jest o stałym dochodzie z pracy, pewności zatrudnienia, ubezpieczeniu emerytalnym[4].

Bezpieczeństwo żywnościowe (food security) – oznacza stały dostęp fizyczny i ekonomiczny do podstawowej żywności[5]. W tym znaczeniu dostęp fizyczny związany jest z wystarczającą ilością żywności zapewniającą gwarancje pokrycia co najmniej minimalnego zapotrzebowania fizjologicznego. Ekonomiczna dostępność do żywności jest równoznaczna z tym, iż najsłabsze ekonomicznie gospodarstwa domowe mają dostęp do niezbędnej żywności[6].

W ramach bezpieczeństwa żywnościowego wyróżnia się pojęcie: **bezpieczeństwo żywności** (food safety), czyli zdrowotnej odpowiedniości pojedynczego produktu żywnościowego (brak zanieczyszczeń) oraz spożywanej racji żywnościowej (niezbędny poziom energii i właściwa proporcja składników pokarmowych)[7].

Bezpieczeństwo osobiste (personalne) – można zdefiniować jako stan wolny od zagrożeń; zapewnienie ochrony przed wszelkiego rodzaju przemocą fizyczną; związane jest z takimi wartościami, jak: życie, zdrowie, nietykalność osobista i mienia, wolność, swoboda przekonań i głoszenia poglądów, prawo do pracy[8].

W obecnych dyskusjach nad bezpieczeństwem personalnym można wyróżnić następujące koncepcje: orientacja liberalna (ujmuje bezpieczeństwo jednostki z perspektywy i w kategoriach praw naturalnych i rządów prawa, opiera się na założeniach uznania praw człowieka do życia, wolności, szczęścia i bezpieczeństwa), orientacja humanitarna (zmierzająca do poprawy podstawowych warunków życia uchodźców, wsparcia ofiar przemocy, interwencja w sytuacji pojawienia się takich zjawisk, jak ludobójstwo, czystki etniczne), orientacja krytyczna (akcentuje szerokie podejście do bezpieczeństwa, wskazując na zróżnicowane formy zagrożeń, problemów mających wpływ na jakość życia i bezpieczeństwo jednostki, np. kwestie ekonomiczne, społeczne, zdrowotne, ekologiczne)[9].

Bezpieczeństwo ekologiczne – rozumiane jako bezpieczeństwo środowiska naturalnego, czyli ochrona przed takim jego użytkowaniem i degradacją, które w efek-

[4] Human Development Report 1994, United Nations Development Programme (UNDP), New York–Oxford 1994, s. 23–25.
[5] Tamże, s. 27.
[6] J. Małysz, *Bezpieczeństwo żywnościowe strategiczną potrzebą ludzkości*, Warszawa 2008, s. 88.
[7] *Bezpieczeństwo żywności w erze globalizacji*, red. S. Kowalczyk, Warszawa 2009, s. 15.
[8] www.wsie-projekty.eu/edukacja/files/1413/4762/0731/Wprowadzenie_do_bezpieczestwa.pdf (dostęp:17.12.2015).
[9] A. Urbanek, *Współczesny człowiek w przestrzeni…*, s. 140–141.

cie może zagrażać istnieniu pojedynczych ludzi i całych społeczeństw. Można mówić tutaj o poziomie zanieczyszczenia, dostępności do czystej wody, zdolności rządu do rozwiązywania problemów środowiskowych związanych z naturalnymi katastrofami oraz gotowości do inwestowania w ochronę środowiska[10].

Bezpieczeństwo informacyjne – związane jest z zarządzaniem i ochroną zasobów informacyjnych stanowiących tajemnice społeczności oraz informacji prawnie chronionych[11].

Bezpieczeństwo społeczne – obejmuje całokształt działań prawnych i organizacyjnych realizowanych przez podmioty rządowe (krajowe i międzynarodowe), pozarządowe i samych obywateli, które mają na celu zapewnienie określonego poziomu życia osobom, rodzinom i grupom społecznym oraz niedopuszczenie do ich marginalizacji i wykluczenia społecznego[12].

Bezpieczeństwo społeczne (socjalne) ma na celu ochronę przed utratą własnej tożsamości oraz przed różnymi formami patologii w życiu społecznym[13].

Bezpieczeństwo społeczne można postrzegać przez pryzmat dwu obszarów – kulturowego oraz socjalnego. Obszar kulturowy dotyczy zbiorowości w postaci np. społeczności lokalnych lub narodów, które traktowane są jako całość i odnoszone do innych, odmiennych kulturowo grup społecznych. Za sprawą kultury oraz relacji międzykulturowych mogą powstawać ewentualne podziały na tle religijnym, rasowym lub językowym, a przez to oddziaływać na spójność poszczególnych grup społecznych[14].

Drugi obszar bezpieczeństwa społecznego – socjalny – dotyczy pojedynczych ludzi i ekonomicznych aspektów ich życia, co może wpływać na poziom identyfikacji ze społeczeństwem, poczynając od pełnego uczestnictwa w życiu społecznym, a kończąc na marginalizacji i wykluczeniu. Bezpieczeństwo socjalne wiązane jest przede wszystkim z brakiem lub niedostatkiem materialnych środków utrzymania, co skutkuje koniecznością zabezpieczenia społecznego.

Bezpieczeństwo socjalne jest warunkowane przez różnorodne problemy, takie jak np. bezrobocie, ubóstwo, postawy roszczeniowe, bezdomność czy patologie społeczne (alkoholizm, narkomania, prostytucja). Problemy te negatywnie oddziałują na funkcjonowanie społeczeństwa i destabilizują porządek społeczny przez stwarzanie warunków do pojawiania się sytuacji konfliktowych, zachowań przestępczych, a także migracji.

---

[10] Human Development Report 1994…, s. 28–30.

[11] R. Borowiecki, M. Kwieciński, *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Zakamycze 2003.

[12] M. Leszczyński, *Bezpieczeństwo społeczne Polaków wobec wyzwań XXI wieku*, Warszawa 2011.

[13] A. Urbanek, *Podstawy bezpieczeństwa państwa. Wymiar społeczno-polityczny*, Słupsk 2013, s. 128.

[14] M. Brzeziński, *Bezpieczeństwo społeczne z perspektywy bezpieczeństwa wewnętrznego*, „Zeszyty Naukowe WSOWL" 2013, nr 3 (169) s. 8–9.

1. Model bezpieczeństwa jednostki (J)

„Pod koniec XIX wieku słynny angielski fizyk Lord Kelvin (Ketoin lord of Largs, a właściwie William Thomson 1824–1907) oświadczył, że nie jest w stanie zrozumieć jakiegokolwiek zjawiska, dopóki nie potrafi go przedstawić w postaci modelu. Wywołało to wówczas zdziwienie i podejrzenie o jego konserwatywne podejście. Obecnie modelowanie, jako główna konstrukcja myślowa systemowego podejścia, można uznać za jedno z największych osiągnięć metodycznych nauki zarówno na polu badań podstawowych, jak i stosowanych.

Modelowanie stało się jedynym skutecznym narzędziem poznawczym współczesnych zjawisk społecznych i gospodarczych”[15].

Każdą sytuację problemową, a także sytuację dotyczącą problemów badawczych, można przedstawić w następującej postaci[16]:

$$\mathbf{V = } f\mathbf{(X_i , Y_j)},$$

gdzie:

V – oznacza miarę wykonania lub spełnienia czegoś, co chcemy zmaksymalizować lub zminimalizować,

X_i – oznacza zmienne „decyzyjne” (sterowanie),

Y_j – oznacza konspekt zewnętrzny problemu (aspekty sytuacji, którymi nie możemy sterować).

Rozwiązanie problemu polega na znalezieniu takich wartości zmiennych X_i, wyrażonych jako funkcja Y_j, które maksymalizują lub minimalizują V.

Każda jednostka (człowiek) charakteryzuje się indywidualnymi cechami odróżniającymi ją od innych, np. osobowością, temperamentem, inteligencją, stylem poznawczym, zmysłem uwagi, procesem uczenia się[17]. Każda z tych jednostek, pomimo różniących ją cech, funkcjonuje w określonym otoczeniu. Korzysta z produktów, usług oferowanych przez różne organizacje, funkcjonuje na rynku pracy, będąc elementem pewnej organizacji, jest członkiem różnych grup formalnych i nieformalnych. Śmiało można stwierdzić, iż każda jednostka jest częścią systemu[18], czyli zestawu wzajemnie powiązanych elementów stanowiących całość. Każda jednostka funkcjonująca w danym otoczeniu ma również potrzeby dotyczące szeroko pojmowanego bezpieczeństwa.

Model ukazujący bezpieczeństwo danej jednostki **(J)** funkcjonującej w danym środowisku (rys. 3) zależy od otoczenia zewnętrznego, tzw. makrootoczenia **(Ozm)**,

---

[15] J. Habr, J. Vepřek, *Systemowa analiza i synteza,* tłum. A. Kusto, Warszawa 1976, s. 304, 305, za: A.D. Rychły-Lipińska, *System zarządzania jakością w jednostkach administracji publicznej*, Olsztyn 2007, s. 75.

[16] W. Kasprzak, B. Łysik, *Analiza wymiarowa. Algorytmowe procedury obsługi eksperymentu*, Warszawa 1988.

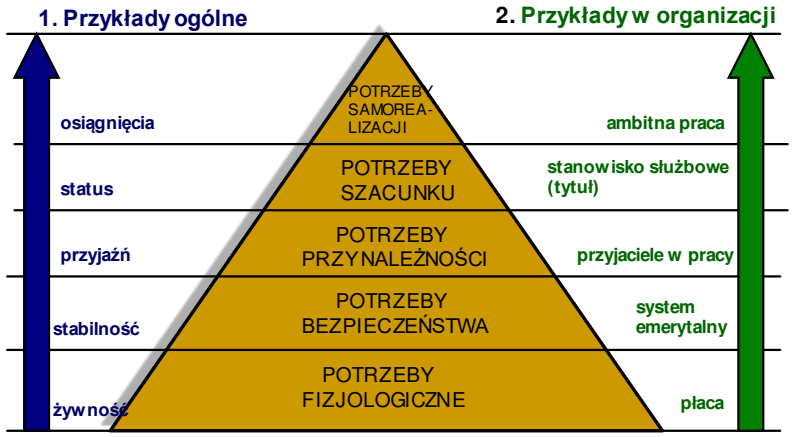
[17] Zob.: *Zachowania organizacyjne. Wybrane zagadnienia*, red. A. Potocki, Warszawa 2005.

[18] A.H. Maslow, *A Theory of Human Motivation*, „Psychological Review” 1943, t. 50, s. 370–396, za: R.W. Griffin, *Podstawy zarządzania organizacjami*, tłum. M. Rusiński, Warszawa 1999, s. 87.

otoczenia zewnętrznego bliższego danej jednostce **(Ozb)** oraz od wewnętrznego poczucia bezpieczeństwa tej jednostki **(Ow)**. Wewnętrzne poczucie bezpieczeństwa jednostki można spróbować przedstawić jako piramidę (rys. 2), której fundament tworzony jest przez trzy rodzaje bezpieczeństwa: bezpieczeństwo osobiste **(Bos)**, bezpieczeństwo żywnościowe **(Bża)** oraz bezpieczeństwo ekonomiczne **(Bek)**. Poszczególne rodzaje bezpieczeństwa można pokrótce zdefiniować jako:

- Bezpieczeństwo osobiste – zapewnienie ochrony przed wszelkiego rodzaju przemocą fizyczną,
- Bezpieczeństwo żywnościowe – zapewnienie w każdej chwili dostępu do podstawowej żywności,
- Bezpieczeństwo ekonomiczne – zapewnienie podstawowych dochodów umożliwiających przetrwanie.

Zauważyć można, iż potrzeba zaspokojenia tych trzech rodzajów bezpieczeństwa stanowiących fundament piramidy jest bezpośrednio powiązana z piramidą potrzeb wg Maslowa.



Rys. 1. Piramida potrzeb wg A. Maslowa
Fig. 1. The pyramid needs according to A. Maslow

Źródło: A.H. Maslow, A Theory of Human Motivation, „Psychological Review" 1943, t. 50, s. 370–396, za: R.W. Griffin, *Podstawy zarządzania organizacjami*, tłum. M. Rusiński, Warszawa 1999.

Amerykański psycholog Abraham Maslow twierdził, że ludzie dążą do zaspokojenia pięciu poziomów potrzeb[19] (rys. 1). Na samym dole hierarchii znajdują się potrzeby fizjologiczne, czyli podstawowe sprawy przetrwania i biologicznego funkcjonowania, np. potrzeby dotyczące żywności. Potrzeby te muszą zostać zaspokojone, zanim w ogóle weźmie się pod uwagę inne ich rodzaje. W organizacjach potrzeby fizjologiczne są na ogół zaspokajane przez odpowiednie płace i samo środowisko pracy, które zapewnia odpowiednie oświetlenie, dogodną temperaturę i wentylację na stanowiskach pracy.

[19] R.W. Griffin, *Podstawy zarządzania organizacjami…*, s. 461–463.

Następne w kolejności są *potrzeby bezpieczeństwa*, czyli te, które są związane ze stabilnym środowiskiem psychicznym i emocjonalnym, np. potrzeba posiadania dachu nad głową, odzienia oraz potrzeba życia wolnego od troski o pracę na chronionym przed zwolnieniem stanowisku. Potrzeby te mogą zostać zaspokojone w miejscu pracy przez ciągłość zatrudnienia (tzn. zatrudnienia bez zwolnień), odpowiednio funkcjonujący system rozpatrywania i załatwiania skarg (dla ochrony przed różnymi działaniami przełożonych, np. mobbingiem) oraz odpowiedni program świadczeń ubezpieczeniowych i emerytalnych. Ważność potrzeby bezpieczeństwa widoczna jest w sytuacjach, kiedy recesja w pewnych gałęziach przemysłu i ogólny spadek gospodarczy pozbawiają ludzi pracy.

Potrzeby przynależności odnoszą się do procesów społecznych. Dotyczą one potrzeb miłości i przywiązania oraz akceptacji ze strony kolegów. U większości jednostek potrzebę tę zaspokaja rodzina, stosunki towarzyskie poza pracą oraz stosunki w pracy (chęć jednostki przynależenia do różnych grup formalnych i nieformalnych).

Potrzeby szacunku w rzeczywistości obejmują dwa różne rodzaje potrzeb:

1. potrzebę pozytywnego obrazu we własnych oczach, szacunku i uznania dla samego siebie oraz
2. potrzebę uznania i szacunku w oczach innych.

W miejscu pracy potrzeby te mogą zostać zaspokojone poprzez zapewnienie jednostce – pracownikowi rozmaitych zewnętrznych symboli, np. tytułów służbowych, przyjemnych pomieszczeń biurowych, opracowanego systemu nagród, charakteru pracy, tzn. przydzielania pracownikowi ambitnych i ciekawych zadań, możliwości odniesienia przez pracownika sukcesu (a to doprowadzi jednostkę do zaspokojenia potrzeb przynależności).

Na samym szczycie hierarchii znajdują się potrzeby samorealizacji, które obejmują realizację możliwości osiągania przez jednostkę ciągłego, nieustannego indywidualnego rozwoju.

Maslow sugerował, że pięć kategorii potrzeb układa się w pewną hierarchię. Jednostka dąży przede wszystkim do zaspokojenia potrzeb fizjologicznych. Dopóki nie zostaną one zaspokojone, są jej główną troską, a po ich zaspokojeniu przestają działać jako czynnik motywacyjny. Jednostka „wspina się" w hierarchii i dąży do zaspokojenia potrzeb bezpieczeństwa, a potem kolejnych, aż na końcu potrzeby samorealizacji.

W modelu bezpieczeństwa jednostki ukazanym na rysunku 3 w momencie zaspokojenia przez nią potrzeby związanej z poczuciem wymienionych wcześniej: bezpieczeństwa osobistego, żywności oraz ekonomicznego, powstaje nowa potrzeba – poczucia przez jednostkę bezpieczeństwa społecznego **(Bsp)**.

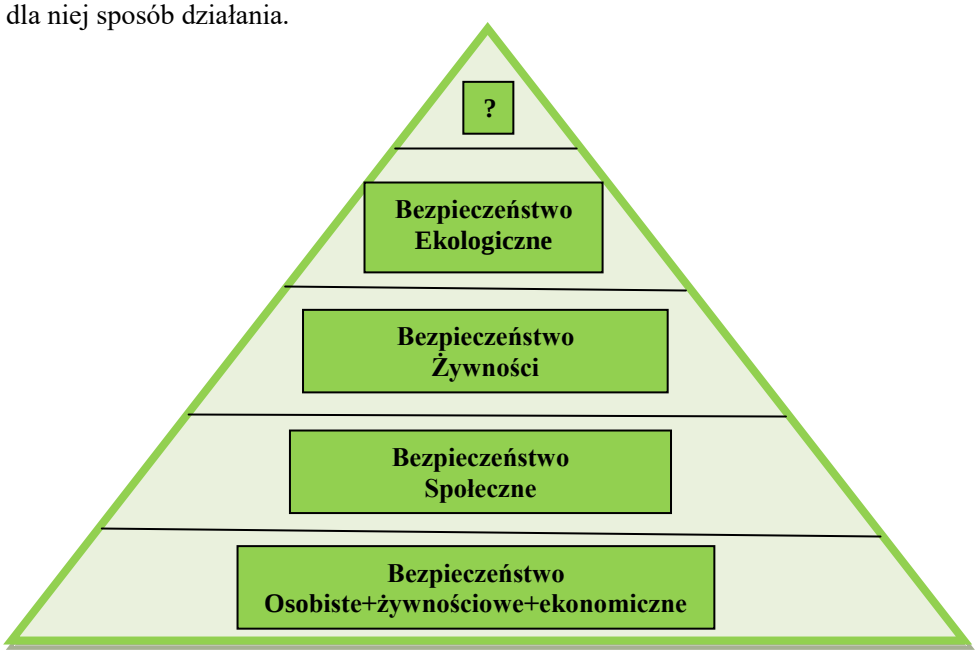
Społeczny aspekt bezpieczeństwa związany jest również z różnymi rodzajami stosunków społecznych, które ze względu na duże zróżnicowanie tworzą różnorodne grupy społeczne: małe i duże (wyróżniane ze względu na strukturę i wielkość), pierwotne i wtórne (wyróżniane na podstawie typów więzi łączących członków grupy), formalne i nieformalne[20].

[20] A. Urbanek, *Podstawy bezpieczeństwa państwa…*, s. 95.

Rozwój cywilizacji spowodował, że coraz mniejsze problemy sprawia zaspokojenie potrzeb fizjologicznych. Niestety, z zaspokojeniem potrzeby bezpieczeństwa jest trudniej. Bezpieczeństwo w najbliższej okolicy, bezpieczeństwo dzieci w szkole, bezpieczeństwo w domu oraz podczas podróży staje się coraz częściej wyzwaniem, od którego zależy rozwój społeczeństwa[21].

Po zaspokojeniu potrzeby bezpieczeństwa społecznego (Bsp) pojawia się kolejna potrzeba w postaci poczucia bezpieczeństwa żywności **(Bżi)** oraz bezpieczeństwa ekologicznego **(Beg)**. Na szczycie piramidy potrzeb związanych z wewnętrznym poczuciem bezpieczeństwa jednostki (rys. 2) znajduje się przestrzeń **'?'** przeznaczona na powstanie i zidentyfikowanie nowej potrzeby, która pojawi się nie tylko po zaspokojeniu poczucia bezpieczeństwa ekologicznego, ale pod wpływem zmian zachodzących w otoczeniu zewnętrznym jednostki. Każda jednostka oprócz posiadania wewnętrznej piramidy bezpieczeństwa funkcjonuje w otoczeniu, którego integralną częścią jest przepływ coraz większej masy informacji, w pewien sposób selekcjonowanych przez każdą jednostkę, tzn. część informacji zostaje przeznaczona do natychmiastowego użycia, część zatrzymana do ewentualnego dalszego użycia, inne informacje grupuje się w celu utworzenia nowych, a jeszcze inne zostają odrzucone. Z przepływem informacji związane jest bezpieczeństwo informacyjne **(BIf)**.

Każda jednostka funkcjonuje również w określonej kulturze **(KIII)**, rozumianej na tym poziomie jako zwyczajowy sposób myślenia jednostki i charakterystyczny dla niej sposób działania.



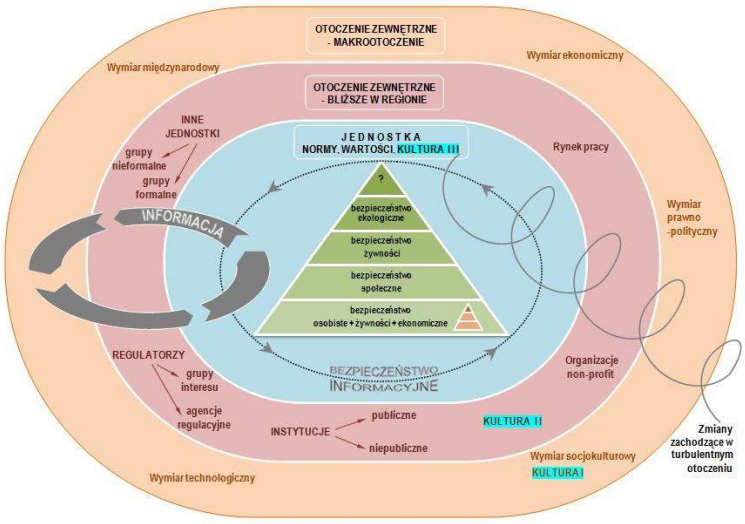
Rys. 2. Wewnętrzne poczucie bezpieczeństwa danej jednostki
Fig. 2. Internal sense of Individual's security
Źródło: Opracowanie własne.

[21] A. Urban, Bezpiecz*eństwo społeczności lokalnych*, Warszawa 2009, s. 23–24.

Otoczenie zewnętrzne bliższe jednostki (**Ozb**) tworzą:

- Rynek pracy **(Rp)** rozumiany jako ogół form i procesów zatrudniania pracowników przez pracodawców, a także ogół instytucji, uwarunkowań oraz czynników negocjacji warunków zatrudnienia, pracy i płac; ekonomiczny, społeczny i polityczny obszar, na którym rozgrywają się wszelkie procesy z zakresu szeroko rozumianego zatrudnienia i bezrobocia[22].
- Instytucje publiczne (w tym instytucje administracji publicznej) i niepubliczne **(I)**.
- Regulatorzy **(R)**, czyli organizacje, które mogą regulować lub w inny sposób wpływać na organizacje oraz jednostki działające na rynku. Regulatorzy dzielą się na dwie grupy. Do pierwszej zaliczyć można tzw. agencje regulacyjne, czyli agencje powołane przez rząd w celu ochrony społeczności przed pewnymi praktykami gospodarczymi albo ochrony jednej organizacji przed innymi. Drugą grupę regulatorów tworzą tzw. grupy interesu, czyli grupy i organizacje utworzone przez swoich członków w celu zabiegania o wpływ na działalność gospodarczą. Grupy interesu nie dysponują oficjalnymi atrybutami władzy, w jakie wyposażone są agencje regulacyjne, jednak mogą wywierać znaczny wpływ, wykorzystując środki masowego przekazu do zwrócenia uwagi opinii publicznej na pewne problemy[23].
- Inne jednostki, które mogą tworzyć grupy formalne bądź nieformalne **(Jn)**.
- Kultura **(KII)**, rozumiana na tym poziomie jako kultura danego regionu, więzi, wartości, normy i wzory wynikające z różnych kręgów kulturowych, w których funkcjonuje dana jednostka. Na tym poziomie różne kręgi kulturowe mogą się wzajemnie przenikać oraz wywierać na siebie wpływ[24].
- Otoczenie zewnętrzne – makrootoczenie **(Ozm)**, obejmuje wymiary i siły, wśród których funkcjonuje dana jednostka i które mogą mieć wpływ na jej działania. Wymiary i siły składające się na ten element otoczenia to[25]:
- Wymiar ekonomiczny **(We)** – ogólna kondycja systemu gospodarczego, w którym działa jednostka (inflacja, stopy procentowe, bezrobocie itp.).
- Wymiar prawno-polityczny **(Wpp)** – odnosi się do państwowej regulacji działalności gospodarczej i stosunków pomiędzy gospodarką i państwem, w którym żyje, pracuje dana jednostka. Wymiar ten związany jest również ze stabilnością polityczną państwa, w którym funkcjonuje jednostka.
- Wymiar socjokulturowy **(KI)** – obejmuje religię, zwyczaje, nawyki, wartości i demograficzne cechy społeczeństwa, w którym funkcjonuje jednostka.
- Wymiar międzynarodowy – to zakres, w jakim organizacje danego państwa uczestniczą w działalności gospodarczej w innych krajach lub pozostają pod jej wpływem **(Wm)**.
- Wymiar techniczny **(Wt)** – dostępne metody, technologie, know-how pozwalające przekształcić zasoby w produkty i/lub usługi, umożliwiające rozwój gospodarki kraju, w którym funkcjonuje jednostka.

[22] http://biznes.pwn.pl/index.php?module=haslo&id=3970479 (dostęp:22.01.2016).
[23] R.W. Griffin, *Podstawy zarządzania organizacjami…*, s. 113.
[24] Zob.: *Zachowania organizacyjne…*, s. 163–193.
[25] Na podstawie: R.W. Griffin, *Podstawy zarządzania organizacjami…*, s. 104–115.



Rys. 3. Model bezpieczeństwa jednostki we współczesnym otoczeniu
Fig. 3. Individual's Security Model in contemporary conditions
Źródło: Opracowanie własne.

Autorka, wykorzystując wyżej zdefiniowane zależności ukazujące funkcjonowanie jednostki w turbulentnym otoczeniu, które charakteryzuje się czterema właściwościami[26]:

1. Wzrostem nowości zmian otoczenia, co oznacza, że istotne i ważne wydarzenia, które mają wpływ na funkcjonowanie organizacji są coraz nowsze i nie pokrywają się z dotychczasowymi doświadczeniami;
2. Wzrostem intensywności otoczenia, co oznacza coraz większy wpływ zmieniającego się otoczenia na organizacje, które w nim funkcjonują, a dalej na jednostki;
3. Wzrost szybkości zmian otoczenia, który związany jest z rosnącą innowacyjnością podmiotów gospodarczych. Czas potrzebny im na wprowadzanie nowości jest coraz krótszy;
4. Złożoność otoczenia oznacza, iż następuje ciągły wzrost liczby elementów otoczenia. Elementy te stają się coraz bardziej zróżnicowane, a wpływ ich na funkcjonujące organizacje oraz jednostki coraz trudniejszy do przewidzenia,

sformułowała następujący zapis zależności:

$$\mathbf{J = \mathit{f}(Ow, Ozb, Ozm)},$$

gdzie:
J – poczucie bezpieczeństwa danej jednostki
Ow – wewnętrzne poczucie bezpieczeństwa danej jednostki
Ozb – Otoczenie zewnętrzne bliższe w środowisku
Ozm – Otoczenie zewnętrzne – makrootoczenie.

[26] http://cytaty.mfiles.pl/index.php/keyword/7401/0/turbulencja (dostęp:12.01.2016).

Szczegółowo zapis można przedstawić w następujący sposób:

Ow = *f*[(Bos, Bża, Bek, Bsp, Bżi, Beg, '?'), (KIII), (BIf)]
Ozb = *f*(Rp, I, R, Jn, KII)
Ozm = *f*(We, Wpp, KI, Wm, Wt)

} Wpływ turbulentnego otoczenia

Opisane powyżej zależności są opisowym (w oparciu o funkcję wielowymiarową) oraz przedstawionym graficznie modelem ukazującym bezpieczeństwo danej jednostki funkcjonującej w danym środowisku.

Objaśnienia do modelu ukazującego bezpieczeństwo danej jednostki:

Beg – bezpieczeństwo ekologiczne
Bek – bezpieczeństwo ekonomiczne
BIf – bezpieczeństwo informacyjne
Bos – Bezpieczeństwo osobiste
Bsp – bezpieczeństwo społeczne
Bża – bezpieczeństwo żywienia
Bżi – bezpieczeństwo żywnościowe
I – instytucje funkcjonujące w danym otoczeniu jednostki
Jn – inne jednostki funkcjonujące na danym rynku
KII – kultura danego regionu
KI – wymiar socjokulturowy
KIII – zwyczajowy sposób myślenia jednostki i charakterystyczny dla niej sposób działania
Ow – poczucie bezpieczeństwa wewnętrznego danej jednostki
Ozb – otoczenie zewnętrzne bliższe w danym regionie
Ozm – otoczenie zewnętrzne – makrootoczenie
R – regulatorzy
Rp – rynek pracy
We – wymiar ekonomiczny
Wm – wymiar międzynarodowy
Wpp – wymiar prawno-polityczny
Wt – wymiar techniczny
'?' – nowa potrzeba

Podsumowanie

Bezpieczeństwo to pewien stan, który gwarantuje istnienie jednostki oraz możliwość jej rozwoju. Poczucie bezpieczeństwa jest jedną z podstawowych potrzeb człowieka, której brak wywołuje niepokój i poczucie zagrożenia. Współczesnie pojęcie bezpieczeństwa ma coraz większy wymiar. Obecnie bezpieczeństwo to nie tylko aspekty polityczne, wojskowe, gospodarcze, techniczne, ekologiczne czy społeczne. Bezpieczeństwo jednostki tworzą czynniki na wielu płaszczyznach, które można przedstawić w postaci pewnej hierarchii, zależne również od czynników zewnętrznych (od otoczenia). Autorka starała się przedstawić graficzny model ukazujący bezpieczeństwo danej jednostki funkcjonującej w danym otoczeniu.

Bibliografia

Bezpieczeństwo żywności w erze globalizacji, red. S. Kowalczyk, Warszawa 2009.
Borowiecki R., Kwieciński M., *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Zakamycze 2003.
Brzeziński M., *Bezpieczeństwo społeczne z perspektywy bezpieczeństwa wewnętrznego*, „Zeszyty Naukowe WSOWL" 2013, nr 3 (169).
Griffin R.W., *Podstawy zarządzania organizacjami*, tłum. M. Rusiński, Warszawa 1999.
Human Development Report 1994, United Nations Development Programme (UNDP), New York–Oxford 1994.
Kasprzak W., Łysik B., *Analiza wymiarowa. Algorytmowe procedury obsługi eksperymentu*, Warszawa 1988.
Leszczyński M., *Bezpieczeństwo społeczne Polaków wobec wyzwań XXI wieku*, Warszawa 2011.
Małysz J., *Bezpieczeństwo żywnościowe strategiczną potrzebą ludzkości*, Warszawa 2008.
Maslow A.H., *A Theory of Human Motivation*, „Psychological Review" 1943, t. 50.
Rychły-Lipińska A.D., *System zarządzania jakością w jednostkach administracji publicznej*, Olsztyn 2007.
Urban A., *Bezpieczeństwo społeczności lokalnych,* Warszawa 2009.
Urbanek A., *Współczesny człowiek w przestrzeni bezpieczeństwa,* Słupsk 2015.
Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa, red. A. Urbanek, Słupsk 2013
Zachowania organizacyjne. Wybrane zagadnienia, red. A. Potocki, Warszawa 2005.

Fiałkowska A., *Bezpieczeństwo człowieka wobec współczesnych zagrożeń*, Europejski Instytut Bezpieczeństwa, http://eib.edu.pl/bezpieczenstwo-czlowieka-wobec-wspolczesnych-zagrozen/ (dostęp: 12.01.2016).
Tryboń M., Grabowska-Lepczak I, Kwiatkowski M., *Bezpieczeństwo człowieka w obliczu zagrożeń XXI wieku* www.zn.sgsp.edu.pl/41/12.pdf (dostęp: 03.04.2017).
http://biznes.pwn.pl/index.php?module=haslo&id=3970479 (dostęp:22.01.2016).
http://cytaty.mfiles.pl/index.php/keyword/7401/0/turbulencja (dostęp:12.01.2016).
www.wsie-projekty.euwww.wsie-projekty.eu/edukacja/files/1413/4762/0731/Wprowadzenie_do_bezpieczestwa.pdf (dostęp:17.12.2015).

Summary

Security is an important concept. A sense of security ensures the proper functioning of human beings and the possibility of development. It is one of the basic human needs. Insecurity causes anxiety. The modern concept of "security" is increasingly complex. Currently, security is not restricted to the political, military, economic, technical, environmental, or social spheres. The paper presents a model of human security functioning in turbulent environments.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 45–56 ROK 2017

ISSN 2543–7321

Aneta Kamińska-Nawrot

Akademia Pomorska
Słupsk
aneta.kaminska-nawrot@apsl.edu.pl

KONTROLA OSOBISTA – RACJONALNOŚĆ USTAWODAWCY

PERSONAL SEARCH – LEGISLATOR RATIONALITY

***Zarys treści*:** Niniejsza publikacja przedstawia problematykę kontroli osobistej dokonywanej przez funkcjonariuszy Policji jako czynności zbędnej i niezgodnej z Konstytucją RP. Autorka wskazuje zagrożenia zarówno dla obywatela, którego konstytucyjnie chronione prawa nie są właściwe realizowane, jak i dla organu ścigania, który nie jest w stanie podjąć właściwej decyzji z uwagi na brak spójnych i szczegółowych przepisów. Wyposażenie organów ścigania w dodatkowe uprawnienia zbliżone do uprawnień do przeszukania osoby, bez określenia szczegółowych instrukcji postępowania, pozostawia tym organom pełną swobodę działania i wprowadza ogólny chaos w praktyce tychże organów. Dlatego też przepisy, które uprawniają te organy do wkraczania w konstytucyjne prawa jednostki i przeprowadzania czynności pozaprocesowych, bez możliwości skontrolowania celowości i prawidłowości tych decyzji, pozostają w sprzeczności z zasadami demokratycznego państwa i powinny zostać uchylone.
***Słowa kluczowe*:** kontrola osobista, sprawdzenie, przeszukanie osoby, prawa człowieka, prawa konstytucyjne, system prawa
Key words: personal search, check, body search, human rights, constitutional rights, legal system

Wprowadzenie

Zasada demokratycznego państwa prawnego, określona w art. 2 Konstytucji RP, oparta jest na trzech filarach, które są ze sobą nierozerwalnie związane. Filary te to demokracja, państwo prawne i sprawiedliwość społeczna. Adresowana jest zarówno do organów władzy publicznej, jak i do każdej jednostki, której prawa i wolności mogą zostać zagrożone. Stanowi szczególną normę, na podstawie której interpretowane może być istnienie tych wszystkich praw i wolności, które nie zostały wprost zapisane w innych przepisach Konstytucji[1].

[1] Zob.: Wyrok TK z dnia 23 listopada 1998 r., SK 7/98, OTK 1998, nr 7, poz. 114; W. Osiatyński, *Prawa czł*owieka i ich granice, Kraków 2011, s. 127.

Sama idea państwa prawnego jest w różny sposób definiowana, ale w literaturze najczęściej pojawia się ujęcie generalne definiujące państwo prawne jako takie, w którym prawo stoi ponad państwem i ma pierwszeństwo wobec wszystkich innych norm czy reguł postępowania[2]. Niemniej jednak można wskazać pewne warunki, które muszą zostać spełnione, aby można było uznać, że dane państwo jest państwem prawa. Realizacji tej idei służą przede wszystkim zasada związania państwa z prawem, zasada zagwarantowania obywatelom prawa do sądu, a także do rzetelnego postępowania oraz zasada precyzyjnego rozgraniczania kompetencji organów państwowych[3]. Zasada związania państwa z prawem oznacza między innymi, że normy, które dopuszczają do ingerencji w sferę praw obywateli, muszą być ujęte w jednolitym i spójnym systemie prawnym, natomiast akty wykonawcze mogą te kwestie regulować tylko i wyłącznie na mocy upoważnienia ustawy i tylko w celu skonkretyzowania ustawy, nigdy zaś w celu jej uzupełnienia.

Do ograniczeń w zakresie korzystania z konstytucyjnych wolności i praw, oprócz tego, że mogą być wprowadzane tylko ustawą, może dojść tylko wówczas, gdy jest to niezbędne między innymi dla zapewnienia bezpieczeństwa lub porządku publicznego (art. 31 ust. 3 Konstytucji RP). Ponadto wolności osobiste mogą być ograniczone dopiero wtedy, gdyby bez tego doszło do powstania szkody większej niż ta, jaką to ograniczenie wyrządza[4]. Zasada ta nakazuje zachowanie proporcjonalności dopuszczalnej ingerencji w imię ochrony wymienionych wartości, a także odpowiedniego systemu kontroli zachowania tej proporcjonalności w praktyce[5]. W sytuacji, gdy równowaga ta zostaje zachwiana a ograniczenia stają się arbitralne i nieadekwatne do pojawiających się zagrożeń, zagrożone są konstytucyjne prawa i wolności obywatela. Jak podkreślił Trybunał Konstytucyjny „Nie można mówić o osiągnięciu właściwego kompromisu wówczas, gdy poziom ochrony materialno-prawnej będzie wprawdzie wysoki, jednak na poziomie proceduralnym będzie brakowało efektywnych, a więc »dających się uruchomić« przez poszkodowanego, procedur

---

[2] E. Gdulewicz, M. Granat, W. Skrzydło, Zasady naczelne Konstytucji Rzeczypospolitej Polskiej, [w:] Prawo konstytucyjne, red. W. Skrzydło, Lublin 1996, s. 176–177; Zob.: Z. Witkowski, Wybrane zasady prawa konstytucyjnego Rzeczypospolitej Polskiej, [w:] Z. Witkowski, J. Galster, B. Gronowska, W. Szyszkowski, Prawo konstytucyjne, Toruń 1998, s. 63.

[3] Z. Witkowski, *Wybrane zasady prawa…*, s. 63.

[4] Zob.: S. Waltoś, *Problem niektórych wolności osobistych w świetle art. 74 Konstytucji PRL*, „Państwo i Prawo" 1967, nr 8–9, s. 273; A. Lityński, A. Murzynowski, *Niektóre prawa osobiste* oby*wateli w świetle art. 74 Konstytucji PRL oraz ważniejszych ustaw szczególnych*, „Nowe Prawo" 1957, nr 10, s. 53; J. Grochowski, Milicyjne przeszukanie pozaprocesowe a konstytucyjne prawa osobiste w PRL, „Problemy Prawa Karnego" 1989, nr 15, s. 30; L. Garlicki, [w:] Konstytucja Rzeczypospolitej Polskiej. Komentarz, t. III, Warszawa 2003, s. 14; P. Hofmański, Prawo *do poszanowania prywatności, a rozwiązania polskiego prawa karnego materialnego i proces*owego, [w:] *Standardy praw człowieka a polskie prawo karne*, red. J. Skupiński, J. Jakubowska-Hara, Warszawa 1995.

[5] J. Skorupka, *Konstytucyjne i konwencyjne granice przeszukania w postępowaniu karnym* (cz.1), „Palestra" 2007, nr 9–10, s. 93; Por.: L. Garlicki, [w:] Konstytucja Rzeczypospolitej Polskiej. Za*rys wykła*du, Warszawa 1999, s. 95; A. Łabno, *Ograniczenie wolności i praw człowieka na po*dstawie art. 31 Konstytucji III RP, [w:] *Prawa i wolności obywatelskie w Konstyt*ucji RP, red. B. Banaszak, A. Preisner, Warszawa 2002, s. 699.

i środków umożliwiających realizację ochrony zagwarantowanej w przepisach materialno-prawnych, a także – dostępnej dla zainteresowanego – ochrony przed ekscesami i szykanami”[6].

Pomimo tak precyzyjnie określonych w Konstytucji RP priorytetów związanych z zasadami tworzenia prawa i jego stosowaniem, w naszym systemie prawnym nadal istnieją niewłaściwie skonstruowane uregulowania prawne, które dają organom ścigania możliwość pozyskiwania dowodów czynów zabronionych poza procesem i nie dbają o interes jednostki, czym odbiegają od standardów demokratycznego państwa prawnego.

Przedmiotem rozważań w niniejszym artykule jest krytyczna analiza przepisów uprawniających organy Policji do dokonywania kontroli osobistej.

Kontrola osobista – konstrukcja przepisów

Kontrola osobista to samodzielna czynność administracyjno-porządkowa funkcjonariusza Policji, który w razie zaistnienia uzasadnionego podejrzenia popełnienia czynu zabronionego pod groźbą kary, uprawniony jest do jej dokonania. Uprawnienie to znalazło odzwierciedlenie w art. 15 ust. 1 pkt 5 Ustawy z dnia 6 kwietnia 1990 r. o Policji (tekst jednolity: Dz.U. 2016, poz. 1782, z późn. zm.), natomiast sposób przeprowadzenia kontroli osobistej zawarty został w rozporządzeniu Rady Ministrów z dnia 29 września 2015 r. w sprawie postępowania przy wykonywaniu niektórych uprawnień policjantów (Dz.U. 2015, poz. 1565).

Przed przystąpieniem do rozważań na temat przepisów regulujących kontrolę osobistą warto w tym miejscu zwrócić uwagę na sposób konstrukcji samego upoważnienia ustawowego. Otóż ustawodawca, upoważniając Radę Ministrów do wydania niniejszego rozporządzenia, wskazał priorytety przy jego tworzeniu. Pierwszym z nich jest zapewnienie skuteczności podejmowanych przez Policję działań, a dopiero w drugiej kolejności poszanowanie praw osób, wobec których działania te są podejmowane. Przeprowadzona analiza przepisów rozporządzenia niestety potwierdza, iż kierunek ten, zgodnie z wolą ustawodawcy, został zachowany.

Warunkiem niezbędnym do podjęcia działań w ramach kontroli osobistej jest istnienie uzasadnionego podejrzenia popełnienia czynu zabronionego pod groźbą kary. Na podstawie tak określonej przesłanki kontroli osobistej można wnioskować, że w sytuacji, gdy czynność związana będzie z popełnieniem wykroczenia, kontrola osobista nie będzie miała związku z postępowaniem karnym. Natomiast problem pojawia się wówczas, gdy policjant nabierze uzasadnionego podejrzenia popełnienia przestępstwa. Jak w takiej sytuacji powinien postąpić, mając na uwadze, że jest to dokładnie ta sama przesłanka, która obliguje go do podjęcia czynności w kierunku wszczęcia procesu karnego – podejmować czynności w ramach ustawy o Policji i przeprowadzić kontrolę osobistą czy też przystąpić do przeszukania osoby w trybie

[6] Zob.: Wyrok TK z 12 grudnia 2005 r., K 32/04, OTK-A 2005, nr 11, s. 132; B. Gronowska, T. Jasudowicz, M. Balcerzak, M. Lubiszewski, R. Mizerski, *Prawa człowieka i ich ochrona*, Toruń 2005, s. 137–160.

art. 308 k.p.k.?[7] Niestety ustawodawca nie precyzuje, na czym opierać się ma uzasadnione podejrzenie popełnienia czynu zabronionego[8]. Przepisy nie zawierają też jakichkolwiek wskazówek czy wytycznych, które mogłyby pomóc w podjęciu decyzji skutkującej ograniczaniem praw osobistych człowieka.

Oprócz kontrowersyjnej przesłanki warunkującej podjęcie kontroli osobistej, analizie poddano przepisy dotyczące obowiązków i praw obu stron, które, podobnie jak podstawa podjęcia tej czynności, stoją w sprzeczności z konstytucyjnymi zasadami konstruowania aktów wykonawczych.

Według § 14 powyżej wskazanego rozporządzenia policjant po przedstawieniu się i podaniu podstawy prawnej i faktycznej podejmowanej kontroli osobistej przystępuje do następujących czynności:

- sprawdza zawartość odzieży osoby kontrolowanej i przedmioty, które znajdują się na jej ciele, nie odsłaniając przykrytej odzieżą powierzchni ciała;
- sprawdza zawartość podręcznego bagażu oraz innych przedmiotów, które posiada przy sobie osoba kontrolowana;
- odbiera osobie kontrolowanej posiadaną broń lub inne niebezpieczne przedmioty mogące służyć do popełnienia przestępstwa lub wykroczenia albo przedmioty mogące stanowić dowody w postępowaniu lub podlegające przepadkowi;
- a na końcu dopiero legitymuje osobę kontrolowaną.

Zanim jednak przystąpi do czynności kontroli, zobowiązany jest poinformować osobę kontrolowaną o prawie do przybrania sobie osoby do udziału w czynności, chyba że jej obecność może w znaczny sposób utrudnić tę czynność. Jednak to również ocenia policjant. W tym też czasie powinna zostać przekazana informacja, że z czynności kontroli protokół zostanie sporządzony tylko wówczas, gdy osoba kontrolowana tego zażąda. W przypadku braku takiego żądania czynność zostanie udokumentowana w notatniku służbowym lub notatce służbowej bądź w formie elektronicznej. Ponadto policjant musi mieć także na uwadze, że kontrola osobista powinna być przeprowadzona w miejscu niedostępnym dla osób postronnych, przez policjanta tej samej płci, co osoba kontrolowana. Warunki te jednak nie muszą zostać spełnione, jeżeli policjant uzna, że z uwagi na okoliczności mogące stanowić zagrożenie dla życia, zdrowia ludzkiego lub mienia kontrola musi być przeprowadzona niezwłocznie.

Czynności policjanta powinny zakończyć się ustną informacją o prawie złożenia przez osobę kontrolowaną zażalenia do właściwego miejscowo prokuratora na sposób przeprowadzenia tej czynności.

Jak wynika z powyższego, ustawodawca, określając sposób postępowania podczas kontroli osobistej, ograniczył się jedynie do ogólnych zapisów, które nie tylko

[7] Zob.: J. Karaźniewicz, *Przeszukanie i czynności zbliżone do przeszukania w teorii i* praktyce *organów ścigania,* [w:] *Węzłowe problemy procesu karnego. Materiały konferencyjne – Kraków,* 25-28.9.2008, red. P. Hofmański, Warszawa 2010, s. 279; D. Szumiło-Kulczycka, Kontrola osobista, *przeglądanie zawartości bagaży, przeszukanie (przyczynek do kwestii racjonalności leg*islacji), „Państwo i Prawo" 2012, nr 3, s. 36–37.

[8] Zob.: J. Grochowski, *Milicyjne przeszukanie pozaprocesowe…,* s. 26–27; J. Karaźniewicz, Przeszukanie i *czynności*…, s. 280.

nie rozwiązują problemów, z jakimi od lat borykają się strony, ale wciąż je mnożą. Chcąc zatem odpowiedzieć na pytanie, czy tego rodzaju zapisy spełniają niezbędne wymogi i wychodzą naprzeciw zasadzie proporcjonalności, o której mowa w art. 31 ust. 3 Konstytucji RP, warto przyjrzeć się tym przepisom bliżej.

Otóż przepis § 14 niniejszego rozporządzenia zawiera algorytm postępowania policjanta, który podjął decyzję o przeprowadzeniu czynności kontroli osobistej z uwagi na uzasadnione podejrzenie popełnienia czynu zabronionego pod groźbą kary. Wydawałoby się, że takie rozwiązanie, gdzie ustawodawca wyszczególnia po kolei czynności do wykonania, ułatwia zadanie zgodnie z zasadą, że organ państwa może podejmować tylko takie działania, jakie zostały mu dozwolone. Okazuje się jednak, że jedynie pierwsza czynność dotycząca przedstawienia się policjanta i podania podstawy prawnej i faktycznej oraz czynność ostatnia – legitymowanie, nie budzą wątpliwości i pytań. Kolejne czynności składające się na kontrolę osobistą nie są już tak klarowne i pozostawiają różne możliwości ich interpretacji. Otóż zgodnie z treścią § 14 ust. 1 pkt 2 rozporządzenia, policjantowi nakazuje się sprawdzenie zawartości odzieży osoby kontrolowanej i przedmiotów, które znajdują się na jej ciele, bez odsłaniania przykrytej odzieżą powierzchni ciała. Jak zatem skutecznie przeprowadzić sprawdzenie osoby?[9] Trudno wyobrazić sobie, że policjant kontrolując osobę nie podniesie do góry nogawek spodni czy koszuli, tym bardziej w sytuacji, gdy wyczuje pod nimi jakiś przedmiot. Można nawet w tym miejscu postawić tezę, że w praktyce ta część przepisu w ogóle nie jest respektowana. W jakim celu zatem taki warunek został wprowadzony, skoro i tak z uwagi na bezpieczeństwo policjanta nie jest przestrzegany? Można przypuszczać, iż ten zabieg legislacyjny został dokonany z uwagi na liczne skargi[10] związane z przeprowadzaniem kontroli osobistej, która przed lipcem 2005 r. przebiegała dokładnie tak samo jak przeszukanie osoby i z praktycznego punktu widzenia niczym się od niej nie różniła. Prawdopodobnie zapis ten miał wskazać różnice między tymi dwiema instytucjami i tym samym ograniczyć stopień ingerencji w konstytucyjnie chronione prawa. W praktyce jednak niewiele zmienił.

Kolejny punkt algorytmu nakazuje policjantowi sprawdzenie podręcznego bagażu oraz innych przedmiotów, które posiada przy sobie osoba kontrolowana. W tym przypadku również brak jakichkolwiek instrukcji, jak takie sprawdzenie powinno przebiegać i czym to postępowanie powinno się różnić od sprawdzenia bagażu osoby przeszukiwanej. Przepisy nie określają czy z bagażu można wyjąć całą zawartość, czy też sprawdzenie ograniczyć się powinno tylko do jego otwarcia i pobieżnego przyjrzenia zawartości[11].

Następna czynność algorytmu kontroli osobistej dotyczy odebrania posiadanej broni lub innych niebezpiecznych przedmiotów mogących służyć do popełnienia przestępstwa lub wykroczenia albo przedmiotów mogących stanowić dowody w po-

[9] Por.: P. Czyżyk, M. Kaczmarczyk, J. Kosiński, Zatrzymanie rzeczy, przeszukanie, sprawdzenie osoby, kontrola osobista – taktyka realizacji. Zagadnienia wybrane, Szczytno 2013, s. 40–41; A. Sęk, *Czynności zbliżone do przeszukania*, „Policja" 2005, nr 3, s. 65.

[10] A. Kazanowski, Karnoprocesowe aspekty przeszukania osoby w polskiej procedurze karnej, „Wojskowy Przegląd Prawniczy" 2008, nr 3, s. 72.

[11] Zob.: A. Sęk, *Czynności zbliżone do przeszukania*…, s. 65.

stępowaniu lub podlegające przepadkowi. W tym przypadku także brak szczegółowych przepisów, jak to odebranie ma przebiegać. Przepisy milczą także w kwestii ich zabezpieczenia. Jeżeli chodzi o broń czy inne niebezpieczne przedmioty, można przyjąć, że fakt ich znalezienia i w pewnym sensie zabezpieczenia znajdzie odzwierciedlenie w notatce służbowej lub notatniku służbowym, jeżeli osoba kontrolowana nie będzie żądała protokołu. Nadal jednak nie wiadomo, jakie jest dalsze postępowanie z tymi przedmiotami. Co więcej, w przypadku zapisu w notatce lub notatniku czy w formie elektronicznej obywatel nie ma możliwości dostępu do sporządzonej dokumentacji, a tym samym nie ma pewności, że to, co zostało faktycznie odebrane, zostało zapisane w notatniku czy w notatce. Pozostawienie takiej swobody organowi, bez udziału osoby będącej wcześniej posiadaczem czy właścicielem tej rzeczy, również może być źródłem domysłów.

Jednak najwięcej zastrzeżeń budzi kwestia zabezpieczenia przedmiotów, które mogą stanowić dowód w postępowaniu. Uprzednio obowiązujące zarządzenie nr 1426 KGP z dnia 23 grudnia 2004 r. w sprawie metodyki wykonywania czynności dochodzeniowo-śledczych przez służby policyjne wyznaczone do wykrywania przestępstw i ścigania ich sprawców (Dz. Urz. KGP 2005, nr 1, poz. 1), nakazywało przesłuchać policjanta przeprowadzającego kontrolę na okoliczność tego zdarzenia, natomiast ujawnione przedmioty poddać oględzinom. Takie rozwiązanie budziło wiele zastrzeżeń i kontrowersji, dlatego też zostało uchylone. W tym miejscu jednak powstała luka, którą organ ścigania z uwagi na brak jakichkolwiek uregulowań prawnych próbuje sam uzupełnić. Nie ulega wątpliwości, że taki stan prawny skutkuje różną praktyką i uzależniony jest przede wszystkim od tego, czy zostały znalezione przedmioty mogące stanowić dowód w sprawie. Jednak nie można wykluczyć, że nawet w przypadku znalezienia dowodów przestępstwa niektórzy policjanci kontynuują praktykę wypracowaną zapisami nieaktualnego już zarządzenia 1426. Natomiast dla tych, którzy zetknęli się z zagadnieniami procesu karnego priorytetem będzie materiał dowodowy, który należy właściwie zabezpieczyć. Można przypuszczać, że ta grupa funkcjonariuszy podejmie działania w kierunku art. 308 k.p.k. i zamiast kontroli osobistej przeprowadzi przeszukanie osoby.

Powyższa analiza przepisów dotyczących algorytmu czynności kontroli osobistej jednoznacznie wskazuje, że są one pozbawione szczegółowych regulacji i pozostawiają ogromne możliwości interpretacji i swobodę działania organom ścigania, co niewątpliwie pozostaje w sprzeczności z konstytucyjnymi zasadami ograniczania praw i wolności osobistych. „Poza tym, ustawodawca – w świetle art. 2 Konstytucji – ma konstytucyjny obowiązek określić przesłanki ingerencji w sferę prywatności w sposób możliwie precyzyjny, tak, aby ograniczyć zakres swobody decyzyjnej pozostawionej organom stosującym prawo, a jednocześnie ma on obowiązek stworzyć odpowiednie mechanizmy kontroli nad aktami organów władzy publicznej dotykającymi tej sfery. W sytuacji, gdy chodzi o ograniczenie konstytucyjnych wolności i praw człowieka i obywatela, przepisy muszą charakteryzować się należytą precyzją i jasnością. Nakaz ten jest funkcjonalnie związany z zasadami pewności i bezpieczeństwa prawnego oraz ochrony zaufania do państwa i prawa”[12]. W wyroku z 30

[12] Wyrok TK z 20 czerwca 2005 r., sygn. K 4/04, OTK-A 2005, nr 6.

października 2001 r. Trybunał Konstytucyjny stwierdził, że pozostawianie nazbyt szerokich ram dla organów, które w istocie muszą zastępować prawodawcę, pozostawia im nadmierną swobodę przy ustalaniu w praktyce zakresu podmiotowego i przedmiotowego ograniczeń konstytucyjnych wolności i praw jednostki, a tym samym pozostaje w sprzeczności z zasadą określoności ustawowej ingerencji w sferę konstytucyjnych wolności i praw jednostki. Kierując się tą zasadą, Trybunał Konstytucyjny uznał, iż przekroczenie pewnego poziomu niejasności przepisów prawnych stanowić może samoistną przesłankę stwierdzenia ich niezgodności[13].

Kontrola osobista a gwarancje obywatela

We wskazanych powyżej regulacjach prawnych, jak wykazała przedmiotowa analiza, występują liczne nieprawidłowości z uwagi na niewłaściwą konstrukcję przepisów. Taki stan rzeczy niewątpliwie wpływa bezpośrednio na osobą kontrolowaną i ułatwia wkraczanie w jej konstytucyjnie chronione prawa. Obywatel zdany jest na łaskę organu, który w zależności od tego, jak oceni daną sytuację, może korzystać z nadanego mu przez ustawodawcę uprawnienia. Przy tego rodzaju przepisach rolą ustawodawcy powinna być troska o ochronę interesów jednostki przed ewentualnym przekroczeniem granic prawnych przez podmioty je stosujące. Trzeba przecież cały czas pamiętać, że kontrola osobista, podobnie jak przeszukanie osoby, jest swego rodzaju środkiem przymusu, który z natury rzeczy wkracza między innymi w sferę wolności osobistej, nietykalności osobistej oraz czci[14]. Jego stosowanie ma na celu wyegzekwowanie przez organy pożądanego stanu faktycznego, niezbędnego do realizacji celów kontroli osobistej, często wbrew woli określonej osoby, przy ewentualnym użyciu niezbędnej siły dla udaremnienia biernego lub czynnego oporu[15]. Z tego też powodu, mając na uwadze międzynarodowe prawa człowieka[16] oraz konstytucyjne prawa i wolności obywatelskie, powinny obowiązywać podobne, jeśli nie takie same, zasady zapewniające osobie kontrolowanej

[13] Wyrok TK z 30 października 2001 r., sygn. K 33/00, OTK ZU 2001, nr 7, poz. 217; por. wyrok TK z 20 kwietnia 2004 r., sygn. K 45/02, OTK ZU 2004, nr 4/A, poz. 30.

[14] Por.: W. Daszkiewicz, *Proces karny. Część ogólna*, Poznań 1995, s. 303; S. Waltoś, Proces karny, zarys systemu, Warszawa 2009, s. 374; B. Młodziejowski, Taktyka przeszukania terenu, pomieszczeń *i osób*, [w:] J. Kasprzak, B. Młodziejowski, W. Brzęk, J. Moszczyński, Kryminalistyka, Warszawa 2006, s. 268–269.

[15] Zob.: S. Waltoś, P. Hofmański, Proces karny, zarys systemu, Warszawa 2013, s. 407–408; P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego…,* s. 1322; K. Marszał, P*ojęcie środków przymusu i ich system w polskim procesie karnym*, „Problemy Prawa Karnego" 1990, nr 16, s. 113 i n.; tenże, *Przegląd środków przymusu i ich funkc*ji w procesie karnym, [w:] K. Amelung, K. Marszał, *Stosowanie środków przymusu w procesie karnym. Problem karnoprawnych ograniczeń praw obywatelskich*, Katowice 1990, s. 54 i n.; M. Cieślak, *Środki przymusu na tle systemu bodźców prawnych w procesie karnym*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego – Prace Prawnicze" 1960, nr 7.

[16] Zob. Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 listopada 1950 r. (Dz.U. 1993, nr 61, poz. 284, uzup. Dz.U. 1995, nr 36, poz. 175 i 176, zm. Dz.U. 1995, nr 36, poz. 177 oraz Dz.U. 1998, nr 147, poz. 962).

ochronę jej praw. O ile w kodeksie postępowania karnego[17] takie gwarancje istnieją, o tyle w aktach prawnych tzw. branżowych ochrona ta wydaje się iluzoryczna.

Pierwsza kwestia, która z punktu widzenia ochrony konstytucyjnych praw jednostki wymaga rozważenia dotyczy samej decyzji o podjęciu kontroli osobistej i możliwości kontrolowania tej decyzji przez niezależny organ. Z analizy przepisów wynika, iż decyzję o podjęciu czynności kontroli osobistej podejmuje sam policjant na podstawie subiektywnego przekonania, że istnieje uzasadnione podejrzenie popełnienia czynu zabronionego pod groźbą kary. Należy w tym miejscu przypomnieć, że w oparciu o tę przesłankę może również zdecydować o przeprowadzeniu czynności procesowych w trybie art. 308 k.p.k., o czym była mowa wcześniej. Jak już wspomniano, przepis milczy na temat tego, na czym to podejrzenie ma się opierać, pozostawiając tym samym organowi pełną swobodę i, co więcej, zasadność podjęcia tej decyzji nie podlega żadnej kontroli. Zgodnie z treścią art. 15 ust. 7 ustawy o Policji, na sposób prowadzenia kontroli osobistej przysługuje osobie zażalenie do miejscowo właściwego prokuratora, o czym funkcjonariusz zobowiązany jest pouczyć osobę kontrolowaną[18]. Zarówno ustawa o Policji, jak i przedmiotowe rozporządzenie nie przewidziały dla osoby kontrolowanej takiego prawa, jakie zostało zawarte w art. 236 k.p.k., mimo że w art. 15 ust. 6 czytamy, iż „Czynności wymienione w ust. 1 powinny być wykonane w sposób możliwie najmniej naruszający dobra osobiste osoby, wobec której zostają podjęte". Niewątpliwie przepis ten można odnieść do dyrektywy przeprowadzenia przeszukania określonej w art. 227 k.p.k., to jednak forma ochrony praw obywatela w sytuacji, gdy prokurator, którego interesy bardzo często zbiegają się z interesami Policji, rozpatruje zażalenie na sposób postępowania podczas kontroli osobistej, niewiele ma wspólnego z ochroną interesu obywatela, a tym samym ze sprawiedliwością[19]. W wyroku K 38/07, Trybunał Konstytucyjny podkreślił, że „Kontrola zażaleniowa nie tworzy ochrony przed arbitralną ingerencją organów ścigania. Jej celem jest zminimalizowanie jej skutków, ponieważ ma ona charakter następczy. Dokonanie przeszukania i zatrzymanie rzeczy powinno zatem podlegać kontroli niezależnego sądu. W związku z powyższym, ze względu na brak sądowej kontroli postanowienia prokuratora o przeszukaniu i zatrzymaniu rzeczy oraz innych czynności związanych z przeszukaniem i zatrzymaniem rzeczy, regulacja ta narusza prawo do sądu przez to, że zamyka drogę sądową ochrony konstytucyjnych wolności i praw"[20]. Co prawda wyrok ten odnosi się do przeszukania, jednak ma on także zastosowanie do kontroli osobistej, w ramach której osoba kontrolowana, której prawa zostały naruszone została pozbawiona możliwości zaskarżenia tej decyzji do niezależnego sądu[21].

---

[17] Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz.U. 1997, nr 89, poz. 555, z późn. zm.).

[18] Zob.: D. Szumiło-Kulczycka, Kontrola osobista…, s. 38.

[19] Zob.: J. Skorupka, O spr*awiedliwości procesu karnego*, Warszawa 2013.

[20] Wyrok TK z dnia 3 lipca 2008 r., K 38/07, OTK-A 2008, nr 6, poz. 102; P. Starzyński, Skutki uznania niekon*stytucyjności art. 236 par. 2 k.p.k.*, „Przegląd Policyjny" 2010, nr 3, s. 122–131.

[21] S. Waltoś, Problem *niektórych wolności…,* s. 274; J. Grochowski, Przeszukanie w procesie kar*nym, jako instytucja wyznaczająca granice konstytucyjnych praw osobistych*, „Problemy Prawa Karnego" 1991, nr 17, s. 135.

Kolejna wątpliwa regulacja, która osobę kontrolowaną stawia na dalszym planie, dotyczy utrwalania przebiegu czynności kontroli osobistej. Zasadą jest, że z czynności kontroli sporządzany jest zapis w notatniku służbowym lub notatka służbowa bądź zapis w formie elektronicznej. Protokół sporządzany jest tylko wtedy, gdy osoba kontrolowana tego zażąda. Takie rozwiązanie budzi ogromne zastrzeżenia zarówno z punktu widzenia interesu procesu karnego, jak i ochrony interesu jednostki. Należałoby się w tym miejscu zastanowić, w jaki sposób osoba kontrolowana może udowodnić, że rzecz, która została jej odebrana nie została zamieniona czy w inny sposób zniekształcona, skoro nawet nie miała możliwości wglądu w ten dokument. Poza tym dokument, który nie jest protokołem sporządzonym zgodnie z wymogami kodeksu postępowania karnego nie może stanowić dowodu w sprawie[22]. Takie rozwiązanie budzi bardzo poważne zastrzeżenia. Trudno także zgodzić się ze stanowiskiem Dobrosławy Szumiło-Kulczyckiej, która twierdzi, że jest to czynność czasochłonna i bezcelowe jest sporządzanie z niej protokołu, gdy nie przyniosła efektu w postaci pozyskania dowodów mających znaczenie dla procesu karnego[23]. Wydaje się, że używanie tego rodzaju argumentacji przy czynnościach, podczas których organ wkracza w prawa człowieka, nie znajduje najmniejszego uzasadnienia. Oczywiście odpowiednie zabezpieczenie materiału dowodowego to kwestia kluczowa, ale tak samo ważna jest odpowiednia ochrona interesów jednostki. Chodzi przecież także o możliwość skutecznego skontrolowania przez niezależny organ decyzji dotyczącej naruszenia granic praw osobistych jednostki. Oczywistym jest przecież, iż „[…]z punktu widzenia kwestionowania jej legalności jest to najbardziej wiarygodny sposób obrazujący przebieg czynności, pod warunkiem, że jest to protokół sporządzany na postawie przepisów k.p.k. – zobowiązujący do ścisłego zamieszczania wniosków i oświadczeń stron, zezwalający stronie na podniesienie zarzutów, co do jego treści i wymagający autoryzacji strony przez złożenie podpisu”[24]. Obligatoryjna forma protokolarna, chociaż czasochłonna, być może zniechęcałaby organ ścigania w sytuacjach wątpliwych do kontrolowania i zmuszała do większej refleksji, stanowiąc tym samym pewnego rodzaju ochronę przed pochopnym podejmowaniem decyzji o kontroli osobistej.

Podsumowanie

Powyższa analiza wskazała mankamenty w przepisach regulujących kontrolę osobistą, które podważają sens jej istnienia w obecnym kształcie. Nie ulega wątpliwości, iż organy odpowiedzialne za zapewnienie bezpieczeństwa i porządku pu-

[22] Zob.: R. Kmiecik, Prawo dowodowe – *zagadnienia ogólne*, [w:] Prawo dowodowe. Zarys wykładu, red. R. Kmiecik, Warszawa 2008, s. 22; M. Cieślak, *Zagadnienia dowodowe…*, s. 6; W. Ponikowski, Dowody – zagadnienia podstawowe i systemowe, [w:], *Postępowanie karne, część ogólna*, red. Z. Świda, J. Skorupka, R. Ponikowski, W. Posnow, Warszawa 2012, s. 266; T. Grzegorczyk, Dowody w procesie karnym, Warszawa 1998, s. 98–101; D. Szumiło-Kulczycka, Kontrola osobista…, s. 38–41.

[23] D. Szumiło-Kulczycka, Kontrola osobista…, s. 40.

[24] Tamże.

blicznego muszą być wyposażone w odpowiednie kompetencje, aby móc sprostać stawianym przed nimi zadaniom[25]. Jednak ustawodawca, konstruując przepis, który głęboko ingeruje w sferę praw i wolności jednostki, musi uwzględniać zasady przyzwoitej legislacji, opartej między innymi na określoności i konkretności[26], ale także musi mieć na uwadze proporcjonalność zastosowanego środka. „Nie wystarczy, aby stosowane środki sprzyjały zamierzonym celom, ułatwiały ich osiągnięcie albo były wygodne dla władzy, która ma je wykorzystać dla osiągnięcia tych celów. Środki te powinny być godne państwa określanego jako demokratyczne i prawne. Pamiętać przy tym należy, że omawiane środki o tyle mogą zostać uznane za usprawiedliwione, o ile ich celem jest właśnie obrona wartości demokratycznego państwa prawnego"[27].

Ponadto, brak wyznaczenia wyraźnej granicy pomiędzy przeszukaniem osoby a kontrolą osobistą przy różnych zakresach uprawnień stron oraz uzależnienie podjęcia kontroli osobistej od przesłanki i celu, który uruchamia procedurę karną nie tylko wprowadza chaos w praktycznym wykorzystaniu tych instytucji i tym samym nie znajduje normatywnego uzasadnienia, ale nasuwa podejrzenie, że kontrola osobista, która ze względów politycznych została wprowadzona w 1983 r., nadal ma na celu obejście rygorów, jakie stawia regulacja kodeksowa[28].

Dlatego też mając na uwadze fakt, iż uprawnienie do przeprowadzania kontroli osobistej nie zapewnia obywatelowi należnych mu praw a przepisy ją regulujące daleko odbiegają od standardów demokratycznego państwa prawnego, zasadne wydaje się wyeliminowanie tej instytucji z systemu prawnego. Dzięki temu zabiegowi nie tylko zniknęłyby dylematy organów i osób kontrolowanych, ale cały system prawny zyskałby na przejrzystości.

Bibliografia

Cieślak M., Zagadnienia dowodowe w procesie karnym, Warszawa 1955.

Cieślak M., *Środki przymusu na tle systemu bodźców prawnych w procesie karnym*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego – Prace Prawnicze" 1960, nr 7.

Czyżyk P., Kaczmarczyk M., Kosiński J., Zatrzymanie rzeczy, przeszukanie, sprawdzenie osoby, kontrola osobista – taktyka realizacji. Zagadnienia wybrane, Szczytno 2013.

Daszkiewicz W., Taktyka kryminalistyczna a procesowe gwarancje jednostki i prawa obywatelskie, „Państwo i Prawo" 1985, nr 3.

Daszkiewicz W., *Proces karny. Część ogólna*, Poznań 1995.

Garlicki L., [w:] *Konstytucja Rzeczypospolitej Polskiej. Zarys wykładu*, Warszawa 1999.

Garlicki L., [w:] Konstytucja Rzeczypospolitej Polskiej. Komentarz, t. III, Warszawa 2003.

[25] Zob. S. Pieprzny, Policja – organizacja i funkcjonowanie, Kraków 2011.

[26] P. Sarnecki, Prawo konstytucyjne, Warszawa 2004, s. 58.

[27] J. Skorupka, *Konstytucyjne i konwencyjne granice…*, s. 93–94.

[28] D. Szumiło-Kulczycka, Kontrola osobista…, s. 43; Por.: J. Grochowski, Przeszukanie w procesie karnym *jako instytucja wyznaczająca granice konstytucyjnych praw osobistych*, „Problemy Prawa Karnego" 1991, nr 17, s. 126; W. Daszkiewicz, Taktyka kryminalistyczna a procesowe gwarancje jednostki i prawa obywatelskie, „Państwo i Prawo" 1985, nr 3, s. 51.

Gdulewicz E., Granat M., Skrzydło W., Zasady naczelne Konstytucji Rzeczypospolitej Polskiej, [w:] Prawo konstytucyjne, red. W. Skrzydło, Lublin 1996.
Grochowski J., Milicyjne przeszukanie pozaprocesowe a konstytucyjne prawa osobiste w PRL, „Problemy Prawa Karnego" 1989, nr 15.
Grochowski J., *Przeszukanie w procesie karnym jako instytucja wyznaczająca granice* konstytucyjnych praw osobistych, „Problemy Prawa Karnego" 1991, nr 17.
Gronowska B., Jasudowicz T., Balcerzak M., Lubiszewski M., Mizerski R., *Prawa czł*owieka i ich ochrona, Toruń 2005.
Grzegorczyk T., Dowody w procesie karnym, Warszawa 1998.
Hofmański P., *Prawo do poszanowania prywatności a rozwiązania polskiego prawa* karnego materialnego i procesowego, [w:] *Standardy praw człowieka a polskie pr*awo karne, red. J. Skupiński, J. Jakubowska-Hara, Warszawa 1995.
Hofmański P., Sadzik E., Zgryzek K., *Kodeks postępowania karnego. Komentarz do a*rtykułów *1*–296, Warszawa 2011.
Karaźniewicz J., Przeszuka*nie i czynności zbliżone do przeszukania w teorii i praktyce organów śc*igania, [w:] *Węzłowe problemy procesu karnego. Materiały konferencyjne – Kraków, 25–* 28.9.2008, red. P. Hofmański, Warszawa 2010.
Kmiecik R., Prawo dowodowe – *zagadnienia ogólne*, [w:] Prawo dowodowe. Zarys wy*kładu*, red. R. Kmiecik, Warszawa 2008.
Lityński A., Murzynowski A., *Niektóre prawa osobiste obywateli w świetle art. 74 Ko*nstytucji PRL oraz wa*żniejszych ustaw szczególnych*, „Nowe Prawo" 1957, nr 10.
Łabno A., *Ograniczenie wolności i praw człowieka na podstawie art. 31 Konstytucji* III RP, [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, red. B. Banaszak, A. Preisner, Warszawa 2002.
Marszał K., *Pojęcie środków przymusu i ich system w polskim procesie karnym*, „Problemy Prawa Karnego" 1990, nr 16.
Marszał K., *Przegląd środków przymusu i ich funkcji w procesie karnym*, [w:] K. Amelung, K. Marszał, *Stosowanie środków przymusu w procesie karnym. Problem karn*o*prawnych ograniczeń praw obywatelskich*, Katowice 1990.
Młodziejowski B., Takt*yka przeszukania terenu, pomieszczeń i osób*, [w:] J. Kasprzak, B. Młodziejowski, W. Brzęk, J. Moszczyński, Kryminalistyka, Warszawa 2006.
Osiatyński W., *Prawa człowieka i ich granice*, Kraków 2011.
Pieprzny S., Policja – organizacja i funkcjonowanie, Kraków 2011.
Ponikowski R., Dowody – zagadnienia podstawowe i systemowe, [w:] Z. Świda, J. Skorupka, R. Ponikowski, W. Posnow, *Postępowanie karne, część ogólna*, Warszawa 2012.
Sarnecki P., Prawo konstytucyjne, Warszawa 2004.
Sęk A., *Czynności zbliżone do przesz*ukania, „Policja" 2005, nr 3.
Skorupka J., *Konstytucyjne i konwencyjne granice przeszukania w postępowaniu karnym* (cz. 1), „Palestra" 2007, nr 9–10.
Skorupka J., *O sprawiedliwości procesu karnego*, Warszawa 2013.
Starzyński P., Skutki uznania niekonstytucyj*ności art. 236 § 2 k.p.k*., „Przegląd Policyjny" 2010, nr 3.
Szumiło-Kulczycka D., *Kontrola osobista, przeglądanie zawartości bagaży, przeszuk*a*nie (przyczynek do kwestii racjonalności legislacji)*, „Państwo i Prawo" 2012, nr 3.
Waltoś S., *Problem niektórych wolności osobistych w świetle art. 74 Konstytucji PRL*, „Państwo i Prawo" 1967, nr 8–9.

Waltoś S., Proces karny, zarys systemu, Warszawa 2009.
Waltoś S., Hofmański P., Proces karny, zarys systemu, Warszawa 2013.
Witkowski Z., Wybrane zasady prawa konstytucyjnego Rzeczypospolitej Polskiej, [w:] Z. Witkowski, J. Galster, B. Gronowska, W. Szyszkowski, Prawo konstytucyjne, Toruń 1998.

Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, sporządzona w Rzymie dnia 4 listopada 1950 r. (Dz.U. 1993, nr 61, poz. 284, z późn. zm.).
Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz.U. 1997, nr 89, poz. 555, z późn. zm.).
Ustawa z dnia 6 kwietnia 1990 r. o Policji (tekst jednolity: Dz.U. 2016, poz. 1782, z późn. zm.) i Rozporządzenie Rady Ministrów w sprawie postępowania przy wykonywaniu niektórych uprawnień policjantów (Dz.U. 2015, poz. 1565)

Summary

An analysis of legal acts concerning the powers of the police to conduct personal searches clearly indicates that these provisions clearly conflict with the provisions of the Constitution, which exposes the police to accusations of acting against the values of a democratic state ruled by law. This publication is an argument that these acts, which were created in violation of the applicable standards of the rule of law and violate the constitutional rights of the individual, should be removed from the legal system. There still remains the problem of distinguishing, by the different law enforcement agencies, the procedure called personal search and body search.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 57–76 ROK 2017

ISSN 2543–7321

Józef Sadowski

Akademia Pomorska
Słupsk
jozef.sadowski@apsl.edu.pl

CYBERNETYCZNY WYMIAR WSPÓŁCZESNYCH ZAGROŻEŃ

A CYBERNETIC DIMENSION OF THE CONTEMPORARY THREATS

***Zarys treści*:** Rośnie podatność państw na zagrożenia cybernetyczne, w tym typu terrorystycznego. Prezentowane w artykule przykłady z ostatnich lat w Polsce i innych krajach świata wskazują, że tendencja ta będzie się systematycznie zwiększać, bowiem funkcjonowanie nowoczesnych społeczeństw nieodłącznie wiąże się z zapewnieniem stałego i prawidłowego funkcjonowania systemów informatycznych, służących zaspokajaniu podstawowych potrzeb (gromadzeniu i transmisji danych, monitorowaniu, sterowaniu, wspomaganiu zarządzania itp.). Do działań o charakterze agresji czy wręcz terroru cybernetycznego mogą się uciekać władze i służby wrogich państw, koncerny międzynarodowe, przestępcze organizacje o charakterze pozarządowym, nieformalne grupy użytkowników Internetu, a nawet pojedynczy użytkownicy. Celem ataków stają się elementy infrastruktury krytycznej, systemy bankowe, uzbrojenia i kierowania państwem, a nawet końcowi użytkownicy systemów. Ataki te przynoszą straty ekonomiczne liczone już w setkach milionów dolarów rocznie. Przewiduje się, że w niedalekiej przyszłości cyberataki staną się narzędziem szantażu w rękach przestępczości zorganizowanej i mogą stać się zarzewiem cyberkonfliktu a nawet cyberwojny.
***Słowa kluczowe*:** cyberataki, cyberzagrożenia, cyberterroryzm**,** cyberwojna, cyberkonflikt, wojna informacyjna.
Key words: cyber-attacks, cyber threats, cyber-terrorism, cyberwar, cyberconflict, information warfare

Cyberbezpieczeństwo, cyberataki, cyberzagrożenia**,** cyberobrona itp. to pojęcia związane ze współczesnym Internetem. Internet (z ang. *inter-network*, dosłownie „między-sieć") – to ogólnoświatowy system połączeń między komputerami, określany również jako sieć sieci. W znaczeniu informatycznym Internet to przestrzeń

adresów IP przydzielonych hostom i serwerom połączonym za pomocą urządzeń sieciowych, takich jak karty sieciowe, z wykorzystaniem infrastruktury telekomunikacyjnej[1]. Internet w ogólnym znaczeniu to sieć komputerowa, czyli wiele połączonych ze sobą komputerów, zwanych również hostami.

Początki Internetu wiążą się z powstaniem sieci rozległej ARPANET i sięgają końca lat sześćdziesiątych XX w. Powszechnie uważa się, iż potrzeba jego stworzenia była konsekwencją prac amerykańskiej organizacji badawczej RAND Corporation, która prowadziła badania nad możliwościami dowodzenia w warunkach wojny nuklearnej. Na podstawie uzyskanych raportów podjąć miano prace projektowe nad skonstruowaniem sieci komputerowej mogącej funkcjonować mimo jej częściowego zniszczenia. Charles Herzfeld, dyrektor ARPA w czasach powstania ARPANET, obala jednak tak rozumiany mit genezy Internetu zauważając, iż od początku chodziło wyłącznie o zwiększenie potencjału naukowego przez połączenie oddalonych od siebie placówek badawczych wyposażonych w komputery[2].

W latach dziewięćdziesiątych ubiegłego wieku nastąpiła gwałtowna komercjalizacja i rozwój tego środowiska. Powstały nowe usługi: strony internetowe, poczta elektroniczna, wyszukiwarki, komunikatory, strumieniowe przesyłanie multimediów, sieci społecznościowe, fora, blogi i wiele innych. Wraz z rozwojem fizycznej infrastruktury globalnej sieci ciągle rośnie liczba jej użytkowników. W ostatnich latach technologia informatyczna bardzo się rozwinęła. Z administracyjnego narzędzia do wspierania optymizacji pracy biurowej przekształciła się obecnie w narzędzie przemysłu, administracji i wojskowości.

W Polsce pierwsze internetowe łącze analogowe zostało uruchomione 26 września 1990 r. Pierwsza transmisja internetowa miała miejsce w listopadzie 1990 r. Internet w Polsce dostępny jest oficjalnie od 20 grudnia 1991 r.[3] W sierpniu 1993 r. powstał pierwszy polski serwer WWW, pod nazwą „Polska Strona Domowa". W 1992 r. powstała pierwsza polska strona internetowa internet.pl, następnie w 1995 r. powstał polski portal internetowy Wirtualna Polska[4].

W drugiej dekadzie XXI w. społeczeństwa w coraz większym stopniu uzależnione są od informatyki. Do cyberprzestrzeni przenikają kolejne aspekty ludzkiej działalności. Globalny zasięg oraz możliwość natychmiastowego dostępu z dowolnego miejsca na Ziemi, w połączeniu z niewielkimi kosztami użytkowania sprawił, że coraz więcej podmiotów oraz indywidualnych osób decyduje się przenosić różne elementy swojej codziennej działalności do Internetu. Dzisiaj przeciętny Kowalski nie wyobraża sobie życia bez szybkiego dostępu do najświeższych informacji i poczty elektronicznej, bankowości internetowej, zakupów online, elektronicznej rezerwacji biletów czy kontaktu z rodziną i znajomymi przez portale społecznościowe oraz internetowe komunikatory. Komputery kontrolują, gromadzą informacje lub wręcz sterują wieloma dziedzinami życia (dostarczanie energii, komunikacja, transport, finanse, gromadzenie danych medycznych, danych statystycznych itp.).

[1] https://pl.wikipedia.org/wiki/Internet (dostęp: 21.01.2017).
[2] Charles Herzfeld on ARPAnet and Computers, (dostęp: 26.02.2014).
[3] 20 lat polskiego Internetu. di.com.pl. (dostęp: 03.01.2017).
[4] Historia Wirtualnej Polski SA. https://pl.wikipedia.org/wiki/Internet (dostęp: 27.01.2017).

Jednak w czasie, gdy cyberprzestrzeń ułatwia życie, przenikają do niej również negatywne formy ludzkiej działalności. Dając duże poczucie anonimowości, wykorzystywana jest przez organizacje przestępcze, a nawet niektóre państwa, do prowadzenia nielegalnej działalności lub agresji wobec innych państw czy podmiotów. Istnieje przeświadczenie, że współczesny przestępca może dokonać więcej zniszczeń za pomocą komputera niż bomb czy rakiet.

Cyberprzestrzeń jest „zależnym od czasu zbiorem połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcję z tymi systemami”[5]. Nie ma barier kontrolnych. Cele ataków są bardzo szerokie – zagrożone są sieci komputerowe oraz indywidualne komputery, a znalezienie luk w zabezpieczeniach – przede wszystkim z winy użytkowników (nieznajomość/lekceważenie przepisów, łapownictwo, frustracja, ideologia, modyfikacja systemów i danych, błąd organizacyjny lub techniczny, sabotaż, uszkodzenie lub kradzież elementów przesyłowych) – jest bardzo trudne. Zagrożone mogą być instytucje i urzędy państwowe oraz inne jednostki organizacyjne, w tym prywatni użytkownicy.

Cyberprzestrzeń – to przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Ułatwia ona użytkownikowi sieci kontakty w czasie rzeczywistym. Obejmuje wszystkie systemy komunikacji elektronicznej, które przesyłają informacje pochodzące ze źródeł numerycznych. Przestrzeń wirtualna stała się łatwym polem aktywności organizacji terrorystycznych. Rozwój informatyki generuje więc nowy rodzaj zagrożeń związanych z cyberterroryzmem. Ataki cybernetyczne[6] są jednymi z najbardziej skutecznych i jednocześnie uciążliwych (jeśli chodzi o szkody) działań uderzających we współczesne społeczeństwa. Cyberterroryzm staje się coraz bardziej powszechną metodą działania:

- do przeprowadzenia działań związanych z cyberatakiem jedynym potrzebnym narzędziem jest komputer i podłączenie do sieci;
- poprzez tworzenie wirusów, robaków komputerowych, tzw. koni trojańskich i przesyłanie ich docelowo w miejsce ataku, niszczenie serwerów, modyfikację systemów IT oraz fałszowanie stron www.

Istnieje wiele definicji cyberterroryzmu:

1) „neologizm opisujący dokonywanie aktów terroru przy pomocy zdobyczy technologii informacyjnej. Ma na celu wyrządzenie szkody z pobudek politycznych lub ideologicznych, zwłaszcza w odniesieniu do infrastruktury o istotnym znaczeniu dla gospodarki lub obronności atakowanego kraju. Polega na celowym zakłóceniu interaktywnego, zorganizowanego obiegu informacji w cyberprzestrzeni”[7].
2) „[...] groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach pań-

[5] Cyberspace: Definition and Implications, Cooperative Cyber Defence Centre of Excellence, www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf (dostęp: 20.05.2012).

[6] Szerzej na temat cyberterroryzmu, D. Galan, *Cyberterroryzm jako nowe wyzwanie społeczeństwa informacyjnego*, http://academicon.pl/blogi_naukowe/bezpieczenstwo-w-sieci/cyberterroryzm-jako-nowe-wyzwanie-spoleczenstwa-informacyjnego (dostęp: 20.11. 2016).

[7] https://pl.wikipedia.org/wiki/Cyberterroryzm (dostęp: 27.01.2017).

stwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny,

3) […] powinny wywoływać powszechne poczucie strachu"[8].
4) „[...] wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań"[9].
5) „[...] akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie i/lub przerwanie świadczenia usług dla wywołania strachu, poprzez wprowadzanie zamieszania lub niepewności w danej populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonego przez terrorystów programu"[10].
6) „[...] jest to obmyślony, politycznie umotywowany akt przemocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który mając charakter niemilitarny, przeprowadzony jest przez ponadnarodowe lub narodowe grupy terrorystyczne"[11].
7) „[...] jest skrytym, politycznie motywowanym atakiem przeciwko informacji, systemom lub programom komputerowym, bazom danych, których efektem jest przemoc przeciwko celom niewojskowym realizowanym przez grupy ponadnarodowe"[12].

Przedstawione definicje zawierają dwa zasadnicze wyróżniki, aspekty (jednocześnie części składowe cyberterroryzmu):

- celem aktu terrorystycznego jest technologia informatyczna (atakowane są komputery i systemy informatyczne z zamiarem przeprowadzenia sabotażu elektronicznego lub fizycznego) albo
- technologia informatyczna jest jedynie narzędziem (wykorzystywane są narzędzia informatyczne w celu manipulowania, penetracji lub kradzieży danych bądź wymuszenia takiego działania systemu, który jest zgodny z intencją terrorystów).

[8] D. Denning, Cyberterrorism, 2000, www.cs.georgetown.edu~denning/infosec/cyberterror-GD.doc (dostęp: 27.03.2004).
[9] A.J. Lewis, Assessing the risk of cyber terrorism, cyber war and other cyber threats, 2002, Center for Strategic amd International Studies, www.csis.org/tech/0211lewis.pdf (dostęp: 27.03.2004).
[10] L. Garrison, M. Grand, Cyberterrorism, 2001, An evolving concept, NIPC highlights, www.Nopc.gov./publication/highlight/2001/highlight-01-06.htm (dostęp: 04.04.2004).
[11] Tamże.
[12] M.M. Pollitt, Cyberterrorism – Fact or Fancy, http://www.cs.georgetown.edu/~denning/infosechtml/pollitt, (dostęp: 04.04.2004).

Ewolucja zagrożeń cybernetycznych

Rozwój Internetu w XXI w. stał się stymulatorem zagrożeń cybernetycznych. Niegroźne robaki i wirusy przekształciły się ze zwykłych niedogodności w poważne wyzwania bezpieczeństwa oraz idealne narzędzia cyberszpiegostwa. Ataki cybernetyczne (w tym DDoS) stają się coraz powszechniejsze, lepiej zorganizowane. Wyrządzają coraz większe szkody administracji i gospodarce. Walka informacyjna stanowi potencjalnie zagrożenie także dla transportu, sieci dostaw energii oraz elementów infrastruktury krytycznej. W ocenie ekspertów potencjalne ataki cybernetyczne mogą obejmować oprogramowanie przeciwnika (software) lub systemy informacyjne i sprzęt komputerowy (hardware) i osiągnąć poziom, którego przekroczenie może zagrozić światowemu dobrobytowi, bezpieczeństwu i stabilności.

Niżej wybrane przykłady takiej działalności.

W 1986 r. KGB zwerbowało pięciu niemieckich hakerów, którzy włamali się do amerykańskiego Departamentu Obrony i uzyskane informacje przekazywali Rosjanom. Był to pierwszy przypadek szpiegostwa cybernetycznego[13].

Pierwsze przypadki ataków cybernetycznych w NATO miały miejsce podczas kryzysu w Kosowie (1996–1999). Działania ceberprzestępców doprowadziły, między innymi, do zablokowania na kilka dni kont e-mailowych uczestników operacji wojskowych NATO na Bałkanach oraz zakłóceń strony internetowej Sojuszu.

W marcu 2000 r. policja japońska ogłosiła, że w pracach nad oprogramowaniem umożliwiającym śledzenie ponad 150 pojazdów policyjnych, w tym pojazdów nieoznakowanych, uczestniczyli aktywni członkowie sekty Aum Shinryko. Co więcej, przynajmniej 8 japońskich firm prywatnych i aż 10 agencji rządowych przy pracach nad oprogramowaniem zatrudniało, bezpośrednio lub poprzez kooperantów, członków tej sekty. Tym samym istnieje prawdopodobieństwo zainstalowania przez nich „koni trojańskich" w opracowanym oprogramowaniu, które mogą być w przyszłości wykorzystane do przeprowadzenia ataku cyberterrorystycznego[14].

Trzytygodniowa fala zmasowanych ataków cybernetycznych w Estonii latem 2007 r. na infrastrukturę teleinformatyczną doprowadziła do paraliżu państwa, blokując dostęp m.in. do systemu bankowego i sieci komórkowych. Wydarzenia te pokazały wzrastające źródło nowych zagrożeń dla strefy publicznej oraz bezpieczeństwa i stabilności państw (również państw NATO). O przeprowadzenie ataków oskarżono Rosję, jednak nie udało się zebrać dowodów pozwalających stwierdzić, że władze tego kraju były za nie formalnie odpowiedzialne[15].

Poważny atak na amerykański wojskowy system komputerowy przeprowadzono w 2008 r. Z wykorzystaniem pendrive'a wprowadzono do komputera armii amerykańskiej w bazie wojskowej na Bliskim Wschodzie oprogramowanie szpiegowskie. Wirus rozprzestrzenił się szybko i niepostrzeżenie zarówno w tajnych, jak i w jaw-

[13] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe AMW" 2005, XLVI, nr 1 (160), s. 177.

[14] Tamże, s. 184.

[15] Estonia leczy rany po pierwszej cyberwojnie, „Gazeta Wyborcza", z 1 czerwca 2007; Estonia Has no Evidence of Kremlin Involvement in Cyber Attacks, RIA, Novosti, 6 września 2007 r., http://en.rian.ru/world/20070906/76959190.html (dostęp: 24.04.2012).

nych systemach informatycznych. Powstał „informatyczny przyczółek", z którego ściągnięto tysiące plików danych do serwerów będących pod zagraniczną kontrolą. W ten sposób armia amerykańska straciła wiele istotnych, a szczególnie tajnych informacji. Podobne incydenty odnotowano w niemal wszystkich państwach NATO. Od tego czasu cyberataki i cyberszpiegostwo stały się niemal ciągłym zagrożeniem[16].

Do zmasowanych ataków na rządowe strony internetowe i serwery doszło w Gruzji podczas konfliktu gruzińsko-rosyjskiego w 2008 r. Tym razem określenie „wojna cybernetyczna" nabrało bardzo konkretnego, materialnego wymiaru. Działania w cyberprzestrzeni nie doprowadziły do żadnych fizycznych zniszczeń, osłabiły jednak gruziński rząd w krytycznej fazie konfliktu. Wpłynęły również na zdolność komunikowania się ze zszokowaną opinią publiczną w kraju i na świecie[17].

Dnia 7 listopada 2008 r. „Financial Times" doniósł, że chińscy hakerzy zdołali już kilkakrotnie spenetrować sieć komputerową Białego Domu, z Chin zaatakowano też sieci komputerowe kampanii wyborczych ówczesnych kandydatów na prezydenta USA – Baracka Obamy i Johna McCaina.

W czerwcu 2010 r. upubliczniony został fakt wprowadzenia do systemu irańskich sieci informatycznych złośliwego oprogramowania (malware) „Stuxnet". Elektroniczny wirus zaatakował irański program nuklearny[18]. Stuxnet ujawnił kolejny gigantyczny jakościowy skok w destrukcyjnym potencjale cyberwojennym i pokazał potencjalne zagrożenie, jakie niesie ze sobą złośliwe oprogramowanie (malware) atakujące kluczowy system komputerowy zarządzający dostawami energii[19]. Po raz pierwszy udowodniono, że cyberataki mogą powodować rzeczywiste fizyczne zniszczenia i narażać życie ludzi.

O skali, w jakiej cyberprzestrzeń, a szczególnie funkcjonujące w sieci blogi oraz portale społecznościowe, może wywierać wpływ na bezpieczeństwo państw, świadczy przykład „arabskiej wiosny", która rozpoczęła się w 2011 r. Uczestnicy wydarzeń ulicznych i protestów, gdy odcięto ich od informacji w tradycyjnych środkach masowego przekazu, skutecznie organizowali się za pośrednictwem serwisów społecznościowych, takich jak Facebook i Twitter. Tendencja ta z pewnością będzie narastać w przyszłości wraz z coraz szerszym rozprzestrzenianiem się nowoczesnych technologii wśród użytkowników.

Jedną z podstawowych funkcji Internetu jest uzyskiwanie informacji. Dlatego powszechnie stosowaną praktyką jest użycie cyberprzestrzeni do celów wywiadowczych. Jak napisano w raporcie opracowanym przez służby kontrwywiadowcze Stanów Zjednoczonych[20], wybrane państwa (raport wymienia m.in. Chiny i Rosję) na szeroką skalę wykorzystują cyberprzestrzeń do zbierania danych wywiadowczych,

[16] R. Rybicki, Prawo do cyberobrony, „Polska Zbrojna" 2009, nr 35, s. 14.
[17] Cyberwojna na Kaukazie, http://technologie.gazeta.pl/technologie/1,89479,5575376 (dostęp: 22.09.2011).
[18] *Wirus w wirówkach*, „Polska Zbrojna" 2011, nr 5, s. 10.
[19] *Stuxnet, najgroźniejszy wirus świata. Czy to dzieło izraelskiego wywiadu*? – zob. newsweek.pl/stuxnet (dostęp: 23.03.2011).
[20] Foreign Spies Stealing US Economic Secrets in Cyberspace, *październik 2011 r.*, www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (dostęp: 20.05.2012).

szczególnie danych gospodarczych dotyczących nowoczesnych technologii, przemysłu obronnego, farmaceutycznego itp. Jak donosi Onet (22.12.2016 r.) na podstawie ujawnionego raportu CrowdStrike, firmy zajmującej się cyberbezpieczeństwem, rosyjskim hakerom udało się dokonać cyberataku w ukraińskiej armii poprzez zainstalowanie złośliwego oprogramowania na telefonach żołnierzy. Dzięki temu separatyści mieli dokładne dane na temat pozycji ukraińskiej armii i mogli prowadzić skuteczny ostrzał. Oryginalna aplikacja, napisana na system Android przez ukraińskiego oficera artylerii Jarosława Szerstiuka, pozwalała skrócić czas namierzania celu ostrzału dla używanych przez Ukraińców haubic D-30 z kilku minut do mniej niż 15 sekund. Żołnierzy zachęcano do pobierania aplikacji w mediach społecznościowych. Jak przyznawał sam Szerstiuk w wywiadach prasowych, ponad 9 tys. żołnierzy korzystało z aplikacji. Wprowadzali do niej m.in. swoją dokładną pozycję.

Z raportu CrowdStrike wynika, że od końca 2014 r. aż do 2016 r. wirus rozprzestrzeniał się wśród ukraińskich żołnierzy, dostarczając separatystom dokładnych danych dotyczących rozmieszczenia jednostek artyleryjskich przeciwnika. CrowdStrike sugeruje, że mogło to być przyczyną niezwykle wysokich strat poniesionych przez siły ukraińskie. Z ogólnodostępnych danych wynika, że armia Ukrainy straciła ponad 50% broni artyleryjskiej w ciągu dwóch lat trwania konfliktu i ponad 80% haubic D-30. To największy odsetek strat wśród wszystkich rodzajów broni znajdującej się na wyposażeniu ukraińskiej armii. Twórcy raportu uważają, że takie działanie nie może być efektem pracy amatorów, lecz hakerów na usługach GRU, rosyjskiego wywiadu wojskowego. CrowdStrike zidentyfikował autorów wirusa jako grupę posługującą się takimi nazwami, jak „APT 28" czy „Fancy Bear". To ci sami ludzie, którzy według CIA i FBI mieli się włamać do systemów Partii Demokratycznej podczas kampanii prezydenckiej w USA.

Android jest obecnie najczęściej atakowanym mobilnym systemem operacyjnym na świecie. Co gorsza, liczba nowych rodzajów ataków i złośliwego kodu infekującego urządzenia pracujące pod kontrolą Androida dynamicznie wzrasta. Zainteresowanie cyberprzestępców platformą mobilną wynika oczywiście z popularności tego systemu wśród użytkowników smartfonów i tabletów. Zgodnie z raportem Gartnera, ponad 86% użytkowników urządzeń mobilnych korzysta właśnie z Androida, a niecałe 13% korzysta z systemu iOS. Firma F-Secure, jeden z popularnych producentów oprogramowania ochronnego na wszystkie platformy systemowe, podała, że w ostatnim czasie otrzymuje do analizy dziennie ponad 9 tys. zakażonych próbek.

Android jest bezsprzecznie najczęściej atakowaną platformą mobilną. Niezależne niemieckie laboratorium antywirusowe – AV-Test – udostępniło statystyki dotyczące liczebności ataków na urządzenia mobilne pracujące pod kontrolą tego systemu. Od stycznia 2013 r. zanotowano już łącznie ponad 15 mln próbek złośliwego oprogramowania. O dynamice wzrostu liczby ataków świadczy szybko zwiększająca się liczba zagrożeń w ostatnim czasie. Dla porównania, w całym 2015 r. laboratorium odnotowało około 4,5 mln zakażonych plików, natomiast w 2016 r. tylko do sierpnia było ich już ponad 7 mln. Problem coraz intensywniejszych ataków przeprowadzanych przez cyberprzestępców na posiadaczy urządzeń pracujących pod kontrolą systemu Android wynika głównie z braku masowych, regularnych aktualizacji tego

oprogramowania. Mimo że oficjalnie na rynku mamy już Androida 7.1.1., to jeszcze w sierpniu 2016 r. zaledwie 18,7% użytkowników smartfonów i tabletów miało na swoich urządzeniach system Android 6.0 Marshmallow, a olbrzymia większość pozostałych wciąż używa znacznie starszych odmian tego systemu mobilnego. W przypadku systemu iOS ten problem nie istnieje – zaledwie po kilku dniach od udostępnienia nowej wersji oprogramowania systemowego instaluje je ponad połowa użytkowników mobilnego sprzętu Apple[21].

W listopadzie 2014 r. NATO przeprowadziło największe na świecie ćwiczenia dotyczące cyberbezpieczeństwa, w których wzięło udział ponad 670 żołnierzy i cywilów z 80 organizacji i instytucji w 28 krajach. Manewry odbyły się w Tartu, na wschodzie Estonii, zaledwie 50 km od granicy z Rosją. Brytyjska gazeta nazywa ćwiczenia zarówno „imponującymi, jak i potrzebnymi" i dodaje, że „[…] od kiedy kryzys na Ukrainie wywołał impas w stosunkach Sojuszu z Rosją, na jaw wyszła cybernetyczna słabość NATO. […] kluczowe natowskie sieci dziennie narażone są na ponad 200 milionów podejrzanych zdarzeń. Prawie wszystkie to spam mailowy, ale co najmniej 100 wymaga dalszych badań, a ok. 30 okazuje się wysoce wyrafinowanymi próbami cyberszpiegowskimi". „Cyberataki mogą być równie niebezpieczne co ataki konwencjonalne. Mogą wyłączyć ważną infrastrukturę i mogą mieć wielki wpływ na nasze działania" – oświadczył szef NATO Jens Stoltenberg podczas wizyty w Tallinie[22].

Admirał Michael Rogers, który stoi również na czele „wojsk internetowych" Stanów Zjednoczonych, stwierdził, że „nie tylko Chiny, lecz również dwa inne państwa, których nie wymienił z nazwy, są w stanie w każdej chwili spowodować wyłączenie systemu energetycznego USA lub inne fragmenty infrastruktury publicznej o kluczowym znaczeniu. Co więcej, w USA ukazał się raport, którego autorzy przewidują nadchodzący cyberatak na infrastrukturę USA o katastrofalnych konsekwencjach, powodujący utratę życia i zniszczenia mienia na kolosalną skalę: mógłby on nastąpić już w okolicach 2025 roku. Cyberatak na elektrownie czy wodociągi może sparaliżować państwo i gospodarkę"[23].

Przedstawione przykłady obejmują zjawisko nazwane cyberprzestępczością. ***Cyberprzestępczość jest zjawiskiem narastającym, niebezpiecznym i przynoszącym przestępcom dochody większe niż handel bronią czy też handel narkotykami.*** W polskim prawie nie ma oficjalnej definicji cyberprzestępczości. Cyberprzestępstwo dotyczy przestępstw popełnianych w Internecie, za pomocą Internetu oraz przestępstw popełnianych za pomocą komputera.

Cyberprzestępczość według Rady Europy[24] dotyczy:

- fałszerstw komputerowych;
- oszustw komputerowych;

[21] M. Kowalski, Android na celowniku cyberprzes*tępców,* http://softonet.pl/publikacje/aktualnosci/Android.na.celowniku.cyberprzestepcow,1876 (dostęp: 20.12.2016).

[22] http://wiadomosci.onet.pl/swiat/financial-times-nato-przeprowadzilo-wielkie-manewry-cybernetyczne/lr4sk (dostęp: 21.11.2014).

[23] „Gazeta Wyborcza" z 22.11.2014 r., Onet (dostęp: 22.11.2014).

[24] Na podstawie „Konwencji Rady Europy o cyberprzestępczości"**,** sporządzonej w Budapeszcie dnia 23 listopada 2001 r., ogłoszonej w Warszawie 27 maja 2015 r. (Dz.U. 2015, poz. 728).

- przestępstw związanych z charakterem informacji zawartych w systemie informatycznym (np. z treściami pedofilskimi);
- przestępstw związanych z naruszaniem praw autorskich i praw pokrewnych.

Definicja cyberprzestępczości według Unii Europejskiej, przyjęta w 2007 r., zakłada, że cyberprzestępstwa składają się z 4 rodzajów przestępstw[25]:

- wymierzane przeciwko poufności, integralności danych, np. hacking, nielegalny podsłuch, szpiegostwo komputerowe, sabotaż komputerowy;
- przestępstwa „klasyczne" popełniane przy użyciu komputera, np. oszustwa komputerowe, fałszerstwo dokumentów, wyłudzenia towarów lub usług;
- przestępstwa „contentowe" (dotyczące zawartości komputerów, serwerów), np. dziecięca pornografia, dostarczanie instrukcji przestępczych (typu „jak zbudować bombę"), zakazane treści rasistowskie, faszystowskie;
- przestępstwa powiązane z naruszeniem praw autorskich i praw pokrewnych.

Główniejsze wydarzenia związane z działalnością cyberprzestępczą w Polsce w 2015 r.[26]

Styczeń przynosi informacje o błędach w domenie GOV.pl. W sieci pojawia się raport pod tytułem ALERT(666) E-ZINE #1, którego autor informował, że stworzył ów raport, by zwrócić uwagę na problem bezpieczeństwa tej części sieci.

Na początku roku miał miejsce „poważny atak hakerski na prywatną pocztę elektroniczną osób pracujących w Ministerstwie Obrony Narodowej i Sztabie Generalnym Wojska Polskiego". Taką informację opublikował w marcu 2015 r. tygodnik „Wprost" a w listopadzie potwierdził ten atak były doradca Ministra Obrony Narodowej Krzysztof Bondaryk.

W kwietniu zaobserwowaliśmy masową kampanię rozsyłania na skrzynki e-mail fałszywych wiadomości, pochodzących rzekomo od Allegro, informujących o „włamaniu" na konto z prośbą o kliknięcie w zawarty w wiadomości link w celu odblokowania konta. W rzeczywistości strona wyłudzała opłatę. Wiadomość przychodziła z podrobionego adresu security@allegro.pl

Drugi kwartał zaczął się więc z phishingiem i to zjawisko będzie już towarzyszyło polskim internautom do końca roku. Z początkiem maja w skrzynkach polskich internautów, a w szczególności kont przypisanych do kont firmowych, pojawiły się informacje, rzekomo od Poczty Polskiej. Maile z załącznikami ze złośliwym oprogramowaniem typu ransomware, czyli szyfrującym pliki na dysku i wymuszającym wpłaty za ich odszyfrowanie. Jego najbardziej znanym przypadkiem jest Crypto-Locker.

W maju polscy internauci masowo dostają e-maile z zainfekowanymi załącznikami, w których rzekomo była wystawiona faktura.

---

[25] www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298370,Czym-jest-cyberprzestepstwo.html (dostęp: 22.03.2017).

[26] www.cybsecurity.org/wpcontent/uploads/2016/02/RaportFBC_Cyberzagrozenia_2016.pdf (dostęp: 27.12.2016).

W czerwcu cyberprzestępca ukrywający się pod pseudonimem „Polsilver" włamał się do systemu informatycznego Plus Banku i szantażował ten bank, domagając się pieniędzy. Został zatrzymany na początku września. Ten przypadek był tematem wielu dyskusji i w jasny sposób wskazał na realne zagrożenie związane z bezpośrednim atakiem na infrastrukturę banku, a nie, jak bywa w większości przypadków – na komputery klientów bankowości elektronicznej.

Również w czerwcu Polskie Linie Lotnicze LOT poinformowały o awarii systemu teleinformatycznego, w wyniku której uziemiono kilkadziesiąt lotów.

Koniec lipca to StageFright – największa do tej pory dziura, jaką odkryto w Androidzie. Jeden MMS może umożliwić przejęcie kontroli nad większością smartfonów działających pod kontrolą systemu Android. Ofiara nie musi wykonywać żadnej akcji, nawet nie zorientuje się, że została zaatakowana, dlatego że udany atak spowoduje skasowanie śladów włamywacza z telefonu ofiary.

W sierpniu ponownie słyszymy o problemach dotyczących Androidów. Poważna dziura w Androidach podmienia zainstalowane aplikacje na fałszywe. Eksperci szacują, że problem dotyczy około 55% telefonów z Androidem, a za błąd odpowiedzialna jest klasa OpenSSLX509Certificate. Dziura pozwala podnieść uprawnienia aplikacji do poziomu uprawnień systemowych.

Pojawiają się również dane dłużników Getin Banku i Noble Banku. Na Torepublic sprzedawca korzystający z nicka „alialbania" zamieszcza ofertę sprzedaży listy zawierającej dane 18 000 dłużników, ujawniając w celu uwiarygodnienia oferty dane pierwszych 100 osób z listy. Do włamania doszło poprzez przejęcie kontroli nad komputerem pracownika banku.

We wrześniu odnotowano trzy nowe kampanie ataków złośliwego oprogramowania na polskich internautów. Wszystkie dotyczyły informacji rzekomo wysyłanych przez polskie firmy. Kampanie zawierały wezwanie do zapłaty, internauci otrzymywali faktury i dodatkowo np. wezwanie do zapłaty, pojawiła się również kampania mówiąca o protokole odbioru robót.

Listopad to kolejna kampania phishingowa, fałszywe e-maile tym razem podszywające się pod Polskie Koleje Państwowe, próba wyłudzania opłaty za SMS Premium.

Przedstawione przypadki cyberataków sugerują pytania o bezpieczeństwo w cyberprzestrzeni w Polsce. Zdaniem ekspertów, największe szkody w gospodarce spowodowałby atak na systemy energetyczne. Jednak uzależnienie naszego kraju od rozwiązań informatycznych, nadal mniejsze w stosunku do Zachodu, paradoksalnie zwiększa nasze bezpieczeństwo.

Jak wynika z badań polskich ekspertów zestawionych w tabeli 1, zagrożenie klasyczne, czyli akcje phishingowe, nadal dominuje. Podobnie jak w latach 2014–2015, można tylko odnotować przesunięcie się balansu z phishingu WWW na pocztę elektroniczną.

Zagrożenia związane z systemem operacyjnym Android to ponownie druga pozycja wśród liderów najbardziej prawdopodobnych zagrożeń. Powodem wysokiego stopnia zagrożeń jest otwarta architektura dystrybucji aplikacji i niewielka skłonność użytkowników do aktualizacji swoich systemów. Taką samą ocenę zebrało zagrożenie związane z wyciekami danych, co skłania cyberprzestępców do działań

Tabela 1

Największe zagrożenia dla bezpieczeństwa w Internecie w 2016 roku – głos polskich ekspertów

Table 1

Greatest dangers of the year 2016 Internet safety – the voice of polish experts

Rodzaj zagrożeń	P[1]	P[2]
Phishing e-mail and WWW	**4,33**	3,37
Wycieki baz danych (dane osobowe, hasła, nr kart kredytowych itd.)	**4,21**	**4,12**
Zagrożenia dla platformy Android	**4,21**	3,52
APT – ataki ukierunkowane na organizacje, połączone ze spear phishingiem	**4,19**	**4,24**
Akcje cyberszpiegowskie na tle politycznym	3,95	**4,05**
Zagrożenia typu ransomware/scareware	3,88	3,36
Ataki DDoS na podmioty komercyjne	3,86	3,50
Zagrożenia w serwisach społecznościowych	3,81	2,88
Ataki Driver-by Download/Watering Hole	3,71	3,36
Powstawanie botnerów opartych o platformy mobilne	3,69	3,17
Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi	3,67	**4,31**
Ataki DDoS na administrację publiczną	3,61	3,07
Kradzież wirtualnych walut	3,52	2,74
Haktywizm	3,43	2,67
Ataki na system DNS	3,36	3,69
Ataki na system sterowania przemysłowego ICS/SCADA	3,36	**4,55**
Ataki na cloud computing	3,33	3,88
Zagrożenia związane z BYOD	3,33	2,90
Zagrożenia dla platformy iOS	3,29	3,26
Zagrożenia związane z „Internet of Things" (IoT)	3,21	3,15
Zagrożenia dla platformy Windows Phone/Mobile	3,20	3,10
Ataki na platformy hostingowe	3,19	3,37
Wykorzystanie gier sieciowych w atakach	2,90	2,45
Ataki na urządzenia medyczne	2,36	3,95

P[1] – prawdopodobieństwo wystąpienia

P[2] – siła oddziaływania danego zagrożenia; wszystkie wartości oceny odnoszą się do skali 1–5 (1 – najmniejsze prawdopodobieństwo, 5 – największe prawdopodobieństwo)

Źródło: opracowanie własne na podstawie:
www.cybsecurity.org/wpcontent/uploads/2016/02/RaportFBC_Cyberzagrozenia_2016.pdf

wymuszających okup lub chcących skompromitować zaatakowaną organizację. Nie wszystkie zagrożenia wskazywane jako najbardziej prawdopodobne (kolumna P^1 w tabeli) jednocześnie wskazywane były podczas badań jako te, których konsekwencje wystąpienia byłyby najbardziej dokuczliwe i najgroźniejsze (P^2 w tabeli). Od lat eksperci identyfikują te same obszary najbardziej groźnych cyberataków.

W 2016 r. nastąpiło jednak kilka istotnych zmian w stosunku do 2015 r.:

- za jeszcze bardziej niebezpieczne uznane zostały ataki na systemy sterowania przemysłowego (wzrost z **4,33** na **4,55**);
- wzrosła ocena zagrożenia związana z atakami na platformy mobilne, w szczególności na system Android (wzrost z **3,15** na **3,52**), na iOS (z **3,00** na **3,26**) oraz Windows Phone/Mobile (z **2,80** na **3,10**);
- spadła ocena zagrożenia związana z atakami typu DDoS, zarówno na organizacje komercyjne (z **3,58** na **3,50**), jak i na administrację publiczną (z **3,38** na **3,07**).

Eksperci, których wyniki badań zawiera raport[27], oprócz zagrożeń wskazanych w tabeli 1, zaproponowali również własne:

- ataki na systemy płatności internetowych,
- ataki na sieci bezprzewodowe (WiFi, GSM),
- zatruwanie informacji w ogólnodostępnych systemach bezpieczeństwa (np. w serwisach virustotal.com, malwr.com),
- shadow IT / Insider (nieautoryzowane rozwiązania IT wewnątrz organizacji),
- inwigilacja realizowana np. poprzez miejski monitoring,
- kompromitacja urządzeń biometrycznych,
- systemy komputerowe instalowane w środkach komunikacji oraz w gospodarstwach domowych,
- ataki terrorystyczne wspomagane atakami na infrastrukturę,
- ransomware na platformy serwerowe,
- wykorzystanie podatności w aplikacjach webowych.

W cytowanym raporcie przedstawione są również wypowiedzi ekspertów z dziedziny cyberzagrożeń. Oto niektóre z nich:

- Przyszłe zagrożenia[28], które będą dominowały za 3–5 lat będą ściśle powiązane z wdrażaniem nowych technologii, które dotychczas są wykorzystywane w wąskim zakresie i dlatego uważa się je za bezpieczne. Przykładem może być biometryka.
- W 2016 r. zagrożenia dotyczące systemów mobilnych znajdą się już w głównym nurcie problemów bezpieczeństwa. We wszystkich obszarach potrzebny będzie większy nacisk na monitorowanie i szybką reakcję[29].
- 2015 r. pokazał, że nie musimy sami infekować się złośliwym oprogramowaniem, bo robią to za nas producenci naszego sprzętu, m.in. firmy Lenovo (SuperFish) czy Dell (eDellRoot), a z ataków na tzw. Internet of Things dalej

[27] Tamże.
[28] Jakub Bojanowski, Partner Deloitte Polska, Raport FBC…, s. 13.
[29] Arkadiusz Buczek, Specjalista ds. Cyberbezpieczeństwa T-MOBILE POLSKA S. A., tamże, s. 13.

nie wynika żadne realne zagrożenie dla przeciętnego Kowalskiego. Skłaniam się więc do tezy, że dalej borykać będziemy się z:

a) socjotechniką i użytkownikami bezmyślnie klikającymi na linki i załączniki w podrobionych e-mailach,
b) kontami przejmowanymi ze względu na słabe lub domyślne hasło oraz
c) brakiem wyobraźni producentów oprogramowania, prowadzącym do pojawiania się w ich rozwiązaniach znanych od lat błędów[30].

- Olbrzymie zyski cyberprzestępców z szantażowania firm oraz zwykłych użytkowników za pomocą złośliwego oprogramowania typu ransomware, sprawiły, że rok 2016 (i kolejne – dop. autora) będzie obfitował w jeszcze bardziej wyrafinowane sposoby szantażu. Może to być np. ransomware albo szantaż związany z blokowaniem dostępu do popularnych usług. Coraz częściej będziemy mieli do czynienia z sytuacją, w której cyberprzestępcy będą szantażowali firmy, iż opublikują ich wrażliwe dokumenty, jeśli nie zostaną spełnione finansowe oczekiwania. Z uwagi na olbrzymią skuteczność i braki w edukacji związanej ze świadomością zagrożeń, możemy spodziewać się jeszcze większej liczby kampanii wykorzystujących najsłabsze ogniowo, czyli użytkownika[31].
- To co przewidywałem rok temu, czyli wzrost cyberzagrożeń na tle politycznym, niestety się sprawdziło. Nie widzę przyczyny, dla której ten trend miałby się odwrócić. Myślę, że może wręcz narastać, o czym świadczą chociażby ostatnie masowe ataki na sieci i serwisy w Turcji. Ten problem będzie dotyczyć zarówno rozgrywek na poziomie państw, jak i haktywizmu. Dodatkowo sądzę, że jeszcze bardziej może dać się we znaki powszechne atakowanie Internetu Rzeczy. Po serii ataków raczej będących ciekawostkami, możliwe jest wystąpienie ataków o poważnych, niebezpiecznych konsekwencjach[32].

Prognozowane cyberzagrożenia w roku 2017

Oto wybrane przewidywania ekspertów z firmy F-Secure[33] dotyczące cyberzagrożeń:

- Zagrożenia USA przez chińskich cyberszpiegów

W 2016 r. głośno mówiło się o szpiegostwie ze strony Rosjan, a nawet o ich zaangażowaniu w proces wyborów prezydenckich w USA. Jednak prawdziwe zagrożenie, z którym powinna liczyć się nowo wybrana władza w Stanach Zjednoczonych, może nadejść ze strony Chin. W 2015 r. amerykańskie Biuro ds. Zarządzania Personelem (*Office of Personnel Management*) poinformowało o wykryciu naruszenia bezpieczeństwa danych, które mogło dotyczyć nawet 14 mln osób.

---

[30] Piotr Konieczny, Chief Information Security Officer, Niebezpiecznik, tamże.
[31] Borys Łącki, Pentester LogicalTrus, tamże, s. 14.
[32] Mirosław Maj, CEO / CIO Fundacja Bezpieczna Cyberprzestrzeń / ComCERT.PL, tamże.
[33] http://di.com.pl/cyberzagrozenia-w-2017-roku-przewidywania-ekspertow-f-secure-56190 (dostęp: 28.12.2016).

- Złośliwe oprogramowanie przez Wi-Fi – (Sean Sullivan, doradca ds. bezpieczeństwa)

Destrukcyjne możliwości botnetów i ataków DDoS to trend, który utrzyma się w przyszłym roku. Potencjalnie może zostać stworzony pierwszy „robak Wi-Fi", czyli szkodliwe oprogramowanie, które szybko rozprzestrzeniałoby się w obszarach miejskich w wyniku zainfekowania routerów za pomocą sieci bezprzewodowej. Zainfekowane urządzenie zawierałoby kod, który kopiowałby się w routerach za pomocą połączenia z siecią Wi-Fi. Po zainfekowaniu danego routera robak próbowałby replikować się na innych urządzeniach.

- Europejska debata na temat kryptografii – (Erka Koivunen, dyrektor ds. bezpieczeństwa informacji)

Kryptografia stanowi fundament dla bezpieczeństwa cyfrowej informacji. Dzięki zastosowaniu kryptografii informacje przechowywane lub przesyłane w formie elektronicznej są chronione przed szpiegami, przestępcami i nieuczciwymi firmami.

- Więcej ataków DDoS z wykorzystaniem Internetu Rzeczy – (Mika Ståhlberg, dyrektor ds. technicznych)

Atak na firmę Dyn z wykorzystaniem złośliwego oprogramowania Mirai stanowił niemałe zaskoczenie w 2016 r. Ogromne zainteresowanie ze strony mediów to efekt uboczny niezrozumienia przez producentów, jak dużym zagrożeniem jest brak odpowiednich zabezpieczeń ich urządzeń z kategorii Internetu Rzeczy (IoT).

Urządzenia IoT są na wczesnym etapie rozwoju technologicznego i pojawiają się pewne wady, których nie były w stanie ujawnić testy w kontrolowanych warunkach laboratoryjnych. Po ataku z użyciem oprogramowania Mirai pewna firma wycofała z produkcji swoje kamery internetowe, zdając sobie sprawę z tego, że luka w zabezpieczeniach konkretnego modelu może zostać wykorzystana przez hakerów. W 2017 r. urządzenia IoT będą w większym stopniu wykorzystywane do przeprowadzania ataków DDoS. Następnym etapem, który zapewne nastąpi w 2018 r., będzie atakowanie samych użytkowników. Istotne jest, by rządzący, branża cyberbezpieczeństwa oraz producenci wspólnie zadbali o odpowiednią ochronę nowo powstałych inteligentnych środowisk.

- Człowiek i maszyna na straży cyberbezpieczeństwa

Szkodliwe oprogramowanie w klasycznym wydaniu jest coraz mniej skuteczne wobec zabezpieczeń punktów końcowych, które są obecnie dostępne. Hakerzy muszą wykazywać się bardziej innowacyjnym podejściem i większym zaangażowaniem niż kiedyś – ich działalność wymaga stosowania socjotechnik, na przykład z wykorzystaniem wiadomości e-mail do wyłudzenia danych (*phishing*). Innym sposobem może być też znalezienie zapomnianego przez administratora IT serwera i wykorzystanie go do spenetrowania sieci. Do nowych trendów na bieżąco dostosowuje się branża cyberzabezpieczeń. By sprostać nowym wyzwaniom w walce z zagrożeniami, niezbędne będzie połączenie sztucznej inteligencji oraz czynnika ludzkiego. Analiza ryzyka, testy penetracyjne, ocena zagrożeń, reagowanie na incydenty i analiza śledcza to tylko część zadań, które można usprawnić przez odpowiednią współpracę maszyny z człowiekiem. W 2017 r. właśnie ten rodzaj kooperacji będzie cieszył się największym zainteresowaniem podmiotów z branży.

Kolejne przewidywania w obszarze cyberbezpieczeństwa na rok 2017 przedstawiają eksperci firmy Fortinet[34]:

- Zautomatyzowane i naśladujące działania ludzi ataki będą wymagać inteligentniejszej ochrony

Zagrożenia stają się coraz bardziej inteligentne i zdolne do autonomicznego działania. W nadchodzącym roku należy spodziewać się złośliwego oprogramowania z adaptacyjnymi algorytmami uczenia się na podstawie udanych ataków. Malware nowej generacji będzie mieć orientację sytuacyjną, czyli będzie rozumieć swoje otoczenie i samodzielnie decydować o dalszych działaniach. Można powiedzieć, że program zacznie działać podobnie do człowieka prowadzącego atak: będzie rozpoznawać środowisko, identyfikować cele, wybierać odpowiednie metody ataku i inteligentnie unikać wykrycia.

- Producenci urządzeń Internetu Rzeczy (IoT) będą odpowiadać za naruszenia bezpieczeństwa

Ataki na urządzenia IoT mogą powodować ogromne zakłócenia i generować duże zyski. Staną się one coraz bardziej wyrafinowane i ukierunkowane na wykorzystywanie słabych punktów komunikacji IoT i całego łańcucha gromadzenia danych. Przewidujemy m.in., że powstaną gigantyczne Shadownety — botnety urządzeń IoT, których nie da się zobaczyć ani zmierzyć konwencjonalnymi narzędziami. Brak poprawy zabezpieczeń w urządzeniach z kategorii Internetu Rzeczy może mieć fatalny wpływ na cyfrową gospodarkę. Użytkownicy będą się wzbraniać przed ich zakupem w obawie przed cyberatakami. Będziemy świadkami rosnącej presji na dostawców tych urządzeń, mającej doprowadzić do utworzenia i egzekwowania standardów bezpieczeństwa, według których to producenci będą odpowiedzialni za działanie swoich produktów w obliczu cyberzagrożeń.

- 20 miliardów urządzeń Internetu rzeczy najsłabszym ogniwem w atakach na chmurę

Najsłabszym ogniwem bezpieczeństwa chmury nie jest jej architektura, lecz fakt, że dostęp do zasobów chmurowych mają miliony zdalnych urządzeń. W nadchodzącym roku spodziewamy się wykorzystania urządzeń końcowych do włamań i ataków na dostawców chmury. Firmy i instytucje będą coraz częściej wdrażać całościowe strategie ochrony oraz segmentacji, pozwalające na tworzenie, zarządzanie i wzmacnianie spójnych polityk bezpieczeństwa pomiędzy środowiskami fizycznym, wirtualnym i chmurowym.

- Inteligentne miasta znajdą się na celowniku cyberprzestępców

Wraz z coraz większą popularnością systemów automatyzacji i zarządzania wzrośnie liczba cyberataków skierowanych przeciwko nim. Potencjalna przestrzeń ataków na takie środowisko jest gigantyczna – celem mogą być czujniki, oświetlenie, systemy ogrzewania i wentylacji, alarmy pożarowe, systemy kierowania ruchem, windy, systemy awaryjne itd. Skuteczne włamanie do dowolnego ze zintegrowanych systemów mogłoby ogromnie zakłócić życie społeczeństwa. Ostatnio doszło już do wycieku danych z systemów dużej amerykańskiej sieci handlowej w wyniku wyko-

[34] www.conowego.pl/aktualnosci/jakie-cyberzagrozenia-czekaja-nas-w-2017-roku-infografika-20378 (dostęp: 25.11.2016).

rzystania luki w zabezpieczeniach systemu ogrzewania i wentylacji sterowanego z użyciem protokołu IP. Systemy te staną się cennymi celami dla cyberprzestępców i cyberterrorystów.

- Ostatnia fala ransomware to tylko otwarcie bramy

Spodziewamy się bardzo precyzyjnych ataków wymierzanych m.in. w celebrytów, polityków i duże organizacje. Poza samym blokowaniem dostępu do systemów, ataki te będą się też zapewne wiązać z kradzieżą poufnych lub osobistych danych, używanych następnie do wymuszeń i szantażu. Można też oczekiwać, że koszty okupów związanych z takimi atakami będą coraz wyższe. Ataki wymierzone w zwykłych użytkowników i obywateli były dotychczas nieopłacalne dla napastników — okup, jaki przeciętny użytkownik byłby gotów zapłacić za odblokowanie dysku twardego, samochodu lub drzwi wejściowych czy też wyłączenie alarmu pożarowego, jest po prostu za mały. Przewidujemy, że w 2017 r. nastąpi przełamanie tej bariery poprzez wprowadzenie ataków zautomatyzowanych, które pozwolą przestępcom masowo wymuszać niewielkie haracze od wielu ofiar jednocześnie. Szczególnie narażone staną się urządzenia IoT.

- Technologia odpowiedzią na problem braku specjalistów ds. cyberbezpieczeństwa

Współczesny brak wykwalifikowanych specjalistów ds. cyberbezpieczeństwa oznacza, że wiele organizacji i państw uczestniczy w gospodarce cyfrowej, będąc obarczonymi wielkim ryzykiem. Nie mają one doświadczenia i kompetencji koniecznych do stworzenia polityki bezpieczeństwa, ochrony krytycznych zasobów w różnych środowiskach sieciowych czy identyfikowania i odpowiedzi na zaawansowane ataki. Rozsądne firmy będą korzystać z usług doradców ds. bezpieczeństwa, którzy będą ich przewodnikami po zawiłym świecie bezpieczeństwa komputerowego, lub z oferty dostawców zarządzanych usług zabezpieczeń (MSSP), którzy zaproponują gotowe do użytku rozwiązanie zabezpieczające. Inną możliwością będzie przeniesienie większości infrastruktury do środowiska chmurowego, gdzie dodanie zabezpieczeń jest kwestią kilku kliknięć.

Inne prawdopodobne cyberzagrożenia w 2017 r. to:

- Tak zwane ataki pod fałszywą banderą

Ważnym problemem w walce z cyberprzestępcami staje się ustalenie autorstwa cyberataków. Działania w zakresie identyfikowania twórców danej kampanii cyberprzestępczej mogą spowodować ryzyko zastosowania technik kierujących badaczy na fałszywą ścieżkę.

- Wojna informacyjna

Coraz częściej stwierdza się przypadki ujawniania zhakowanych informacji dla agresywnych celów. Istnieje ryzyko, że cyberprzestępcy poprzez manipulowanie informacjami będą próbowali wykorzystać gotowość ludzi do przyjmowania fałszywych danych za prawdziwe.

- Podatność na cybersabotaż

Różnorakie systemy i obiekty infrastruktury krytycznej państwa są połączone z Internetem. przy czym często ich ochrona pozostawia wiele do życzenia lub po prostu nie istnieje, pokusa uszkodzenia lub zakłócenia ich pracy może okazać się łakomym kąskiem dla cyberprzestępców.

- Włamania do systemów płatniczych

Wraz ze wzrostem popularności i rozpowszechnienia systemów płatniczych rośnie zainteresowanie nimi również wśród cyberprzestępców. Możemy także spodziewać się na forach podziemia oferowania na sprzedaż wyspecjalizowanych zasobów lub szkodliwych działań w ramach modelu „atak jako usługa".

- Ransomware

Dalszy wzrost liczby oprogramowania ransomware z jednoczesnym malejącym zaufaniem atakowanych do twierdzenia, że wraz z zapłatą okupu nastąpi zwrot utraconych danych.

Podsumowanie

Cyberzagrożenia stają się coraz liczniejsze, bardziej inteligentne, działają autonomicznie i są coraz trudniejsze do wykrycia. Powracają też stare zagrożenia, ale wzmocnione nowymi technologiami, które przekraczają kolejne granice unikania detekcji i wskazania sprawców. Powodują skutki różnego charakteru: bezpieczeństwa państwa, jego systemów, emocjonalne i finansowe różnych organizacji i obywateli. Cyberprzestępczość dotyka milionów rocznie, ale konsumenci (około 75% wszystkich legalnych stron internetowych) nadal nie podejmują działań w celu własnej ochrony. W 2015 r. 594 mln ludzi na całym świecie padły ofiarą przestępstwa internetowego. Ransomware rozszerzyło swoje działania przestępcze na dowolne urządzenia podłączone do sieci: smartfony, systemy Mac i Linux Symantec a nawet inteligentne zegarki i telewizory.

Straty powstałe w wyniku działalności cyberprzestępców na świecie wyniosły w 2011 r. 388 mld dolarów, w 2013 r. straty te wyniosły już 445 mld dolarów.

W celu ograniczenia tego niebezpiecznego trendu konieczne jest pilne wzięcie odpowiedzialności na wielu poziomach, które obejmują dostawców zabezpieczeń, rządy państw, jak i konsumentów. Bez szybkiego działania istnieje poważne ryzyko zaburzenia rozwoju globalnej, nie tylko cyfrowej gospodarki.

Bibliografia

Estonia leczy rany po pierwszej cyberwojnie, „Gazeta Wyborcza", 1 czerwca 2007.

Rybicki R., Prawo do cyberobrony, „Polska Zbrojna" 2009, nr 35.

Szubrycht T., *Cyberterroryzm, jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe AMW" 2005, XLVI, nr 1 (160).

Wirus w wirówkach, „Polska Zbrojna" 2011, nr 5.

„Konwencja Rady Europy o cyberprzestępczości", sporządzona w Budapeszcie dnia 23 listopada 2001 r., ogłoszona w Warszawie 27 maja 2015 r. (Dz.U. 2015, poz. 728).

Charles Herzfeld on ARPAnet and Computers (dostęp: 26.02.2014).

Cyberspace: Definition and Implications, Cooperative Cyber Defence Centre of Excellence, www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf dostęp: 20.05.2012).
Cyberwojna na Kaukazie, http://technologie.gazeta.pl/technologie/1,89479,5575376.
Denning D., Cyberterrorism, 2000, www.cs.georgetown.edu~denning/infosec/cyberterror-GD.doc, (dostęp: 27.03.2004).
Foreign Spies Stealing US Economic Secrets in Cyberspace, październik 2011 r., www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (dostęp: 20.05.2012).
Galan D., *Cyberterroryzm jako nowe wyzwanie społeczeństwa informacyjnego*, http://academicon.pl/blogi_naukowe/bezpieczenstwo-w-sieci/cyberterroryzm-jako-nowe-wyzwanie-spoleczenstwa-informacyjnego (dostęp: 20.11.2016).
Garrison L., Grand M., Cyberterrorism, 2001, An evolving concept, NIPC highlights, www.Nopc.gov./publication/highlight/2001/highlight-01-06.htm (dostęp: 04.04.2004).
„Gazeta Wyborcza", 22.11.2014 r., Onet (dostęp: 22.11.2014).
Historia Wirtualnej Polski SA. https://pl.wikipedia.org/wiki/Internet (dostęp: 27.01.2017).
Kowalski M., *Android na celowniku cyberprzestępców,* http://softonet.pl/publikacje/aktualnosci/Android.na.celowniku.cyberprzestepcow,1876 (dostęp: 20.12.2016).
Lewis A.J., Assessing the risk of cyber terrorism, cyber war and other cyber threats, 2002, Center for Strategic amd International Studies, www.csis.org/tech/0211lewis.pdf (dostęp: 27.03.2004).
Pollitt M.M., Cyberterrorism – Fact or Fancy, http://www.cs.georgetown.edu/~denning/infosechtml/pollitt, (dostęp: 04.04.2004).
Stuxnet, *najgroźniejszy wirus świata. Czy to dzieło izraelskiego wywiadu*? – zob. newsweek.pl/stuxnet, (dostęp: 23.03.2011).
20 lat polskiego internetu. di.com.pl. (dostęp: 03.01.2017).
https://pl.wikipedia.org/wiki/Cyberterroryzm
www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf (dostęp: 20.05.2012).
http://en.rian.ru/world/20070906/76959190.html (dostęp: 24.04.2012).
http://wiadomosci.onet.pl/swiat/financial-times-nato-przeprowadzilo-wielkie-manewry-cybernetyczne/lr4sk (dostęp: 21.11.2014).
www.cybsecurity.org/wpcontent/uploads/2016/02/RaportFBC_Cyberzagrozenia_2016.pdf (dostęp: 27.12.2016).
http://di.com.pl/cyberzagrozenia-w-2017-roku-przewidywania-ekspertow-f-secure-56190
www.conowego.pl/aktualnosci/jakie-cyberzagrozenia-czekaja-nas-w-2017-roku-infografika-20378 (dostęp: 25.11.2016).
www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298370,Czym-jest-cyberprzestepstwo.html (dostęp: 22.03.2017).
https://us.norton.com/cyber-security-insights (dostęp: 24.01.2017).

Summary

Countries' vulnerability to cybernetic dangers, including cyberterrorism, increases. Recent years examples from Poland and world countires presented in the article below suggest that such tendency will continue to rise, since modern community functioning is inseparably connect with the provision of constant and well-functioning automatic sys-

tems, to match the supply of basic needs services such as (data storage and transmission, monitoring and control processes, management support, etc.). An act of violence or cybernetic terror activity may be employed by the enemy countries government and agencies, international concerns, non-government organized crime groups, network associated groups or even individuals. The objectives of such terrorism may be critical infrastructure elements, banking systems, weapon systems, homeland security systems or even individual Internet users. Cyber-attacks can deal massive economical loss reaching hundreds of millions of dollars annually. Predicting the future, cyber-attacks may be commonly practiced by organized crime groups as extortion or become embers of cyberconflict or even cyberwar.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 77–88 ROK 2017

ISSN 2543–7321

Stanisław Kozdrowski

Akademia Pomorska
Słupsk
kadry@agopol.eu

METODY I ZAKRES GROMADZENIA DANYCH DO STATYSTYKI POLICYJNEJ W II RZECZYPOSPOLITEJ (1919–1934)

METHODS AND SCOPE OF THE DATA COLLECTION TO POLICE STATISTICS IN THE SECOND POLISH REPUBLIC (1919–1934)

***Zarys treści*:** W Polsce międzywojennej główny ciężar walki z przestępczością spoczywał na barkach policji kryminalnej, która stanowiła jeden z pionów służbowych w strukturze Policji Państwowej, wyspecjalizowany do wykrywania i zwalczania przestępstw. Własną statystykę kryminalną w PP zaczęto tworzyć już w 1919 r., a następnie rozwijać w kolejnych koncepcjach. Autor niniejszego artykułu podjął próbę dokonania ogólnej charakterystyki systemów statystyki policyjnej, które funkcjonowały w latach: 1919––1934. Opisuje genezę tworzenia statystyki policyjnej dotyczącej przestępczości, strukturę i dynamikę ujawnionych przestępstw (i wykroczeń) w badanym okresie oraz metody gromadzenia danych statystycznych i zasady działania rozwiniętego systemu z 1922 r., w którym rejestrowano przestępstwa i inne zdarzenia przez 13 lat.

***Słowa kluczowe*:** Policja Państwowa, policja kryminalna, przestępczość, statystyka policyjna, arkusz statystyczny

Keywords: National Police, criminal police, crime, police statistics, the statistical sheet

Wprowadzenie

Jednym z najważniejszych zadań każdego państwa, realizowanych przez jego aparat władzy i administracji, jest zapewnienie ładu i porządku publicznego oraz bezpieczeństwa poszczególnym obywatelom. Podstawową organizacją, stworzoną w celu „utrzymania bezpieczeństwa i porządku publicznego", była w okresie mię-

dzywojennym Policja Państwowa, powołana do życia ustawą sejmową z dnia 24 lipca 1919 r.[1]

Odrębną strukturą, utworzoną w tym samym celu co Policja Państwowa, był korpus Policji Województwa Śląskiego, który funkcjonował w ramach autonomii tego województwa. Podstawą prawną tejże autonomii była Ustawa Konstytucyjna Sejmu RP z dnia 15 lipca 1920 r., która zatwierdziła Statut Organiczny Województwa Śląskiego[2]. Na podstawie art. 4 Ustawy Konstytucyjnej zostało wydane Rozporządzenie Wojewody Śląskiego z dnia 17 czerwca 1922 r. o organizacji korpusu Policji Województwa Śląskiego. W art. 1 tego aktu czytamy, że „Policja Województwa Śląskiego jest organizacją służby bezpieczeństwa, spokoju i porządku publicznego". W dalszych rozważaniach skupimy się na funkcjonowaniu korpusu Policji Państwowej, ponieważ korpus Policji Śląskiej był utworzony i szkolony na wzór PP[3].

Szef resortu spraw wewnętrznych, działając na podstawie art. 5, 7 i 9 Ustawy o PP, wydał przepisy wykonawcze o utworzeniu służby śledczej. Paragraf 2 tych przepisów stanowi, że „Zadania urzędów policyjno-śledczych polegają na zapobieganiu i ujawnianiu przestępstw"[4]. Zatem zwalczaniem przestępczości zajmowała się głównie policja kryminalna, funkcjonująca przy każdej Komendzie Okręgowej Policji Państwowej w formie Urzędu Policyjno-Śledczego. W okręgach policyjnych zorganizowano ekspozytury tego urzędu, odpowiedniej kategorii, zależnej od lokalnych warunków przestępczości. Były to ekspozytury:

- I rzędu, które liczyły nie mniej niż 50 funkcjonariuszy;
- II rzędu, liczące od 25 do 50 funkcjonariuszy;
- III rzędu, składające się z 10 do 25 funkcjonariuszy;
- IV rzędu, które zatrudniały od 3 do 10 funkcjonariuszy (§ 3 zarządzenia). W ciągu 20 lat istnienia II RP *służba śledcza* (nazywana też *policją kryminalną*), ulegała wielokrotnym przekształceniom organizacyjnym[5].

Dążąc do poprawy efektywności walki z przestępczością kryminalną, władze policyjne obciążyły obowiązkiem działania w tym kierunku także tzw. policję mundurową. Była to koncepcja „uśledczania" policji. Programy stałych szkół policyjnych i kursów specjalistycznych zawierały odpowiednie przedmioty traktujące o taktyce i technice wykrywania przestępstw. Na przykład w największej szkole policyjnej, ulokowanej w Mostach Wielkich, realizowano m.in. takie przedmioty, jak: *Służba śledcza, Medycyna kryminalna, Zastosowanie psów w służbie zapobiegawczej w Policji Państwowej, Psy w służbie śledczej, Stowarzyszenia polityczne*[6].

---

[1] „Dziennik Praw Państwa Polskiego" 1919, nr 61, poz. 363 oraz liczne rozporządzenia wykonawcze. Od 1928 r. podstawą prawną działania PP było Rozporządzenie Prezydenta RP z dnia 6 marca 1928 roku o Policji Państwowej (Dz.U. RP 1928, nr 82, poz. 643).

[2] „Dziennik Ustaw Śląskich" 1923, nr 13.

[3] O Policji Województwa Śląskiego, zob.: A. Misiuk, *Przyczynek do dziejów Policji Województwa Śląskiego w latach 1922*–1926, „Zeszyty Naukowe WSO" 1988, nr 3(62).

[4] „Monitor Polski" 1919, nr 235, [w:] *Prawo Policji Państwowej w II Rzeczypospolitej 1915*–1945. *Wybór źródeł*, wybór P.K. Marszałek, Toruń 2009, s. 723.

[5] Szerzej na ten temat zob.: S. Kozdrowski, Wyszkolenie policyjne w II Rzeczypospolitej, Kraków 2006, s. 461–486.

[6] Tamże, s. 630–634.

Proces „uśledczenia" policji rozpoczął się od 1928 r. Od tego czasu zaczęto równorzędnie traktować wszystkie piony Policji Państwowej, a co za tym idzie włączono policję mundurową do wykonywania czynności z zakresu służby śledczej oraz politycznej. Kadra policji kryminalnej bardzo często była delegowana na stanowiska komendantów posterunku i kierowników komisariatów, natomiast policjantów służb mundurowych delegowano na śledcze kursy szkoleniowe[7].

W rozważaniach teoretycznych o tworzeniu statystyki policyjnej w owym czasie napotykamy na wiele poważnych trudności. Przede wszystkim nie ma zbyt wielu opracowań tego tematu. Można tutaj wskazać na kilka publikacji Leona Radzinowicza[8], natomiast ze współczesnych opracowań dotyczących m.in. funkcjonowania PP w II Rzeczypospolitej w aspekcie zwalczania przestępczości oraz statystyki kryminalnej warto wymienić książkę Jacka Dworzeckiego[9].

Zachowały się też źródła archiwalne w postaci *Zbioru Zarządzeń Ministerstwa* Spraw W*ewnętrznych z lat 1918*–1930, wydanego nakładem „Gazety Administracji i Policji Państwowej" (Warszawa 1930), a w Archiwum Akt Nowych w Warszawie Zbiór rozkazów Komendanta Głównego Policji Państwowej II Rzeczypospolitej (z lat: 1922–1939, t. I–V). Ponadto dostępne są tomy „Małych Roczników Statystycznych GUS" z lat: 1930, 1931, 1933, 1935, 1937, 1938 i 1939. Można dodać, że istnieją także w zbiorach archiwalnych Arkusze statystyczne Komendy Głównej Policji Państwowej z oryginalnymi zestawieniami liczbowymi o przestępstwach i wykroczeniach z lat: 1921, 1922, 1924, 1925, 1926, 1927, 1928, 1929, 1930, 1931, 1932, 1933, 1934, 1935, 1936, 1937, 1938 oraz miesięczne zestawienie za okres od stycznia do lipca 1939 r. Na szczególną uwagę zasługują Arkusze statystyczne PP z 1919 r. oraz dane policyjne za okres od 1 stycznia do 1 lutego 1920 r. Wskazane źródła archiwalne wykorzystał Zbigniew Piotrowski w swojej pracy magisterskiej[10].

Należy przyjąć, że głównym czynnikiem kryminogennym w pierwszych latach istnienia II Rzeczypospolitej były skutki materialne i moralne I wojny światowej. Zaliczyć tutaj można: wycofanie przed nadejściem frontu milionów osób do Rosji, ogromne zniszczenia i grabieże dóbr materialnych dokonywane głównie przez wojska zaborczych armii; degradację rolnictwa i gwałtowny spadek produkcji przemysłowej. Z tych względów czynniki materialne w sposób bezpośredni bardzo silnie wpłynęły na wzrost przestępczości, zwłaszcza kradzieży i bandytyzmu. Ponadto odrodzona Polska musiała przetrwać silny wstrząs związany z wybuchem wojny sowiecko-polskiej w 1920 r.

---

[7] K. Halicki, *Policja polityczna w województwie pomorskim w latach 1920*–1939, Łódź 2015, s. 32.

[8] L. Radzinowicz, *Przestępczość w Polsce w latach 1924*-1933. Na podstawie policyjnej statystyki kryminalnej, Warszawa 1935; tenże, *Przestępczość w 1934 r.*, „Głos Sądownictwa" 1935, nr 7–8; tenże, *Wpływ warunków ekonomicznych na przestępczość w Polsce w latach 1928*–1934, „Czasopismo Prawno-Historyczne" 1969, t. XXI, z. 2.

[9] J. Dworzecki, Policja w Polsce. Wybrane zagadnienia, Kraków 2011, s. 34–61.

[10] Z. Piotrowski wnikliwie badał policyjne statystyki przestępczości z okresu istnienia II Rzeczypospolitej. Sprawozdanie z tych badań zamieścił w niepublikowanej pracy magisterskiej pt.: *Przestępczość w II Rzeczypospolitej w świetle statystyki poli*cyjnej, obronionej w Akademii Spraw Wewnętrznych w Warszawie w 1986 r.

Warto zwrócić uwagę na fakt, że dopiero pod koniec lat dwudziestych i w latach trzydziestych Polska osiągnęła ogólny poziom produkcji materialnej z 1913 r. Jak pisali Zbigniew Landau i Jerzy Tomaszewski, w całym okresie istnienia II Rzeczypospolitej 8 lat przypadało na kryzysy (1924–1925 i 1930–1935). Przez pozostałe 13 lat koniunktura gospodarcza była w zasadzie dobra. Z tego jednak należy jeszcze odliczyć lata 1918–1920, które stanowiły nie tylko okres początków odbudowy kraju, ale i nowych poważnych zniszczeń spowodowanych działaniami wojennymi[11]. W sumie więc dokładnie połowa okresu międzywojennego przypadła na lata istotnych trudności gospodarczych.

To wszystko przekładało się negatywnie nie tylko na wzrost przestępczości w kraju, ale także na kondycję sił policyjnych w latach 1919–1934 i późniejszych. Czynnikiem kryminogennym były również manifestacje uliczne i masowe strajki chłopskie i robotnicze (1936–1937).

Źródła wskazują, że korpus policyjny od samego początku był nieźle zorganizowany do walki z przestępczością – już w 1919 r. przygotowywano się do opracowania własnej statystyki kryminalnej[12]. Celem niniejszego szkicu jest próba przedstawienia wybranych elementów policyjnego systemu statystyki kryminalnej, który funkcjonował w latach 1919–1934. Ten okres przyjęto za cezurę czasową z tego względu, że szczupłe ramy zaplanowanej publikacji nie pozwalają na opis systemu statystyki policyjnej w latach 1935–1939.

Geneza systemu

W zasobach archiwalnych zachowały się wykazy statystyczne przestępczości z sześciu okręgów (z m.st. Warszawy oraz okręgów: warszawskiego, łódzkiego, kieleckiego, lubelskiego i białostockiego). Wykazy obejmowały rok 1919 oraz tylko styczeń 1920 r. Nie zdołano ustalić, kto zainicjował prowadzenie takich statystyk.

Wykazy statystyczne z tego okresu obejmowały 108 kolumn. W kolumnach od 1 do 72 zamieszczano zbiorcze dane o tzw. przestępstwach właściwych, wykroczeniach i niektórych innych zdarzeniach (np. samobójstwach, zaginięciach osób) z wymienionych wyżej okręgów. W pozostałych kolumnach omawianych wykazów zamieszczono informacje o stanie uzbrojenia policji, liczbie osób aresztowanych, dane ilościowe o niektórych formach pracy PP (np. o inwigilacjach osób czy o przepływie korespondencji biurowej)[13].

Podstawą sporządzenia zbiorczego wykazu statystycznego były jednostkowe raporty pisemne przygotowane przez funkcjonariuszy urzędów śledczych i komisariatów. Przykładowo arkusz statystyczny m.st. Warszawy obejmował dane Urzędu Śledczego i 26 komisariatów, a okręgu warszawskiego zawierał dane z dwóch urzę-

[11] Z. Landau, J. Tomaszewski, *Trudna niepodległość. Rozważania o gospodarce Polski 1918–1939*, Warszawa 1978, s. 61.

[12] W październiku 1919 r. wydrukowano 1000 arkuszy statystycznych, na których w styczniu 1920 r. zarejestrowano pierwsze dane liczbowe o przestępczości, zob.: Z. Piotrowski, *Przestępczość w II Rzeczypospolitej…*, s. 44.

[13] Tamże, Aneks nr 1, s. 173–178.

dów śledczych (UŚ Komendy PP okręgu warszawskiego i UŚ KM PP we Włocławku[14]) oraz z 24 jednostek powiatowych[15].

Z. Piotrowski opracował treść tabeli 1 na podstawie zsumowania pozycji od 1 do 71 arkuszy statystycznych ze stycznia 1920 r., które zachowały się w Archiwum Akt Nowych w Warszawie. Nie rozgraniczał przestępstw od wykroczeń, bo nie było jednoznacznych kryteriów. Nie widział też potrzeby takiego rozgraniczenia, zakładając, że informacje z tego zestawienia „do porównań z przestępczością w innych okresach nie nadają się"[16].

Tabela 1

Statystyka PP za styczeń 1920 r. (z 6 okręgów)

Table 1

PP statistics for January 1920 (from 6 districts)

Okręgi	Przestępstwa i wykroczenia	Różne	Razem	Samobójstwo, zagrożenie osób	Ogółem
I – m. st. Warszawy	3803	728	4531	36	4567
II – warszawski	1731	670	2401	7	2408
III – łódzki	2982	1723	4705	16	4721
IV – kielecki	1300	377	1677	10	1687
V – lubelski	1580	322	1902	7	1909
VI – białostocki	709	288	997	3	1000
Razem:	12 105	4 108	16 213	79	16 292

Źródło: Z. Piotrowski, *Przestępczość w II Rzeczpospolitej…*, s. 47.

Można przyjąć, że rejestry tego rodzaju miał dwa cele, a raczej dwa różne aspekty tego samego problemu. Z jednej strony wyraźnie dążono do zapewnienia dopływu pełnych danych o liczbie, strukturze i dynamice przestępstw oraz wykroczeń, realizując w ten sposób kryminologiczny aspekt statystyki policyjnej. Z drugiej strony zaś kierowano się celami kryminalistycznymi, zamierzając uzyskać dane, które charakteryzowały przestępczość z punktu widzenia miejsca dokonania czynu i równocześnie żądano od jednostek policji informacji o sposobie popełnienia przestępstwa, czyli określenia modus operandi sprawcy[17]. Miało to istotne znaczenie praktyczne dla trafnego typowania sprawcy przestępstwa w sytuacjach istnienia tzw. przestępców zawodowych, którzy kształtowali swoje umiejętności przestępcze w jednym kierunku, co wyrażało się w powtarzalności sposobu popełniania czynów.

[14] KM PP we Włocławku do 1938 r. znajdowała się w strukturze VI Okręgu – warszawskiego, a od tego roku ulokowano ją w strukturach XII Okręgu – pomorskiego.
[15] Z. Piotrowski, *Przestępczość w II Rzeczpospolitej…*, s. 45.
[16] Tamże.
[17] Modus operandi (z łac.) – sposób działania, w tym przypadku sposób popełnienia przestępstwa. Zob.: B.M. Szawer i A.J. Winberg, Kryminalistyka, Warszawa 1949, s. 32.

Jednostki wykonawcze były obowiązane zamieszczać takie informacje w codziennych raportach. Obowiązek ten zniesiono na mocy Rozkazu nr 150 Komendanta Głównego PP z dnia 24.01.1922 r., w którym m.in. napisano, że „Przedkładanie codziennych raportów zwyczajnych pisanych znosi się”[18].

Rejestry tego rodzaju w jakiś sposób przybliżały wiedzę o doświadczeniach i nawykach przestępców, ale to było możliwe jedynie pod warunkiem, że w modus operandi odnotowuje się trwałe, indywidualne i powtarzalne cechy postępowania przestępcy, który „dopracował się” własnej techniki i taktyki dokonywania czynów, swoistej specjalizacji (np. taką mieli tzw. kasiarze, doliniarze, kieszonkowcy, oszuści)[19]. W 1921 r. nastąpił dalszy rozwój metod sporządzania danych o przestępczości dla potrzeb policyjnej statystyki. W tymże roku przygotowywano już zestawy miesięczne ze wszystkich 16 okręgów policyjnych. Na ich podstawie Komenda Główna PP zestawiała arkusze zbiorcze o przestępczości na terenie całej Rzeczypospolitej, jednakże zakres rejestrowanych wówczas danych uległ znacznemu zawężeniu. Zrezygnowano mianowicie z umieszczania w wykazach statystycznych informacji ilościowej o pracy PP, o stanie jej uzbrojenia, wyposażenia w przybory daktyloskopijne, aparaty fotograficzne itp.; zaniechano umieszczania danych o liczbie spraw przekazanych do postępowania sądowego. Nie zaszły większe zmiany dotyczące systemu rejestrowanych zdarzeń przestępczych w układzie wewnętrznym kolumn arkusza statystycznego.

W tabeli 2 ukazano zestawienie liczby przestępstw w Polsce w 1921 r. opracowane na podstawie zmodyfikowanych arkuszy policyjnej statystyki.

Tabela 2

Statystyka PP o przestępczości w Polsce w 1921 r.

Table 2

PP statistics about crime in Poland in 1921

Kwartał 1921 r.	Przestępstwa i wykroczenia	Zaginięcia	Samobójstwa	Ogółem
I	59 709	109	238	60 056
II	74 641	279	398	75 318
III	90 016	278	411	90 705
IV	94 961	253	346	95 560
Razem:	319 327	919	1393	321 639

Źródło: Z. Piotrowski, *Przestępczość w II Rzeczpospolitej…*, s. 53.

Po 1921 r. Policja Państwowa zrezygnowała ze stosowania omawianego arkusza, w którym nie rozdzielono przestępstw od wykroczeń. Szacunkowo w podanej liczbie mieści się ponad 200 tys. przestępstw i ponad 100 tys. wykroczeń. Są to stosun-

[18] Archiwum Akt Nowych w Warszawie (dalej: AAN), Zespół MSW, Zbiór rozkazów KG PP, t. 1, poz. 150.

[19] L. Radzinowicz, *Przestępczość w Polsce w latach 1924–1933…*, s. 70.

kowo niskie wskaźniki liczby ujawnionych przestępstw i wykroczeń, bo w następnym roku odnotowano już ok. 320 tys. przestępstw i prawie 540 tys. wykroczeń, a kolejnym roku liczby te wzrosły do poziomu ok. 437 tys. przestępstw i ok. 1097 tys. wykroczeń[20].

W 1922 r. przystąpiono do wprowadzania bardziej rozwiniętego systemu policyjnej statystyki przestępczości.

Statystyka kryminalna Policji Państwowej w latach 1922–1934

W dniu 24 stycznia 1922 r. Komendant Główny Policji Państwowej wydał wspomniany wyżej Rozkaz nr 150, którym (w punkcie V) został uregulowany nowy system statystyczny wg nowych arkuszy sprawozdawczych dotyczących stanu przestępczości.

Analiza tego rozkazu w kontekście doboru i układu nazw kolumn statystycznych oraz danych liczbowych z lat 1922–1934 uzasadnia podjęcie próby dokonania ogólnej charakterystyki istotnych cech omawianego systemu. Wyniki analizy pozwalają na streszczenie wniosków w następujących punktach:

- **Po pierwsze** – można uznać za dominującą zaletę nowego systemu jego **kompleksowość**. Kolumnami arkusza objęto wszystkie typy przestępstw i wykroczeń. Taka teza wynika z tego, że każdą grupę przestępstw uzupełniała kolumna o nazwie „inne", a przedmiotowo nazwane wykroczenia zamykała kolumna o nazwie „różne"[21]. Ponadto w arkuszach rejestrowano trzy rodzaje zdarzeń kryminalnopodobnych. Były to: pożary przypadkowe, samobójstwa i nieszczęśliwe wypadki. Oczywiście praktyczne korzyści dla organów ścigania zależały już od stopnia wykrywalności rejestrowanych zdarzeń i ich wiarygodności.
- **Po drugie** – zagadnieniu **wiarygodności** rejestrowanych zdarzeń poświęcono wiele uwagi. Takie traktowanie problemu ścisłości zbioru danych jest kolejną zaletą nowego systemu statystycznego. Od samego początku obowiązywała zasada, zgodnie z którą zameldowane (czyli wykryte) zdarzenie rejestrują tylko te jednostki wykonawcze, które uzyskały informacje pierwotne na ten temat. Chodziło tu o posterunki PP, komisariaty, urzędy śledcze i ich ekspozytury, przy czym rejestracji podlegały tylko informacje sprawdzone. W ten sposób zapobiegano ich dublowaniu przez powtórne rejestrowanie (niejako „na swoje konto"). Z tych powodów Komendant Główny w Rozkazie nr 150 kategorycznie nakazał, że dane dostarczane przez „[...] posterunki, komisariaty, ekspozytury śledcze i ewentualnie urzędy śledcze [...] muszą być stwierdzone dochodzeniem policyjnym".

W tym samym kierunku szły dalsze zalecenia Komendanta Głównego PP, skoro w Rozkazie nr 742 z dnia 28.02.1938 r. napisał: „Aby unikać na przyszłość pewnego odsetka danych nieprawdziwych w statystyce polecam: [...] 1) po stwierdzeniu, że

[20] Z. Piotrowski, *Przestępczość w II Rzeczpospolitej...,* s. 54.
[21] L. Radzinowicz, *Przestępczość w Polsce w latach 1924*–1934..., s. 14.

przestępstwo nie miało miejsca, natychmiast wysłać sprostowanie; 2) po upływie roku wraz z wykazem przestępczości za dany rok, wszystkie jednostki policyjne przesyłają jednostkom wyższej instancji wykaz sprostowań dokonanych w ciągu ubiegłego roku. Na podstawie tego wykazu poprawia się roczny wykaz przestępczości z danego terenu"[22].

Z tego widać, że w praktyce tworzenia zbiorów statystycznych stwierdzono jednak „pewien odsetek danych nieprawdziwych". Stąd decyzja Komendanta Głównego Policji Państwowej, aby temu zapobiec na przyszłość. Na podkreślenie zasługuje tu jeszcze stanowisko autorów zbiorów statystycznych Głównego Urzędu Statystycznego, którzy w dwóch kolejnych rocznikach napisali, że publikowane zestawy policyjne o przestępczości zawierają „czyny przestępcze będące przedmiotem dochodzeń policyjnych"[23]. Jest to wyraz zaufania GUS-u do wiarygodności policyjnej statystyki przestępczości.

- **Po trzecie** – kolejną ważną zaletą omawianej na tym miejscu statystyki była stosunkowo duża jej **szczegółowość**. Przestępstwa, wykroczenia i inne zdarzenia początkowo grupowano w 59 odrębnych kolumnach, po czym rozszerzono je na 65 rubryk. Na rejestrację przestępstw właściwych przeznaczono 52 kolumny, na wykroczenia – 10, a na inne zdarzenia – 3[24]. Znaczne uszczegółowienie zbioru statystycznego pozwala na łatwiejszą analizę wielu odrębnych typów przestępstw i innych rejestrowanych zdarzeń. Ale trudności pozostały, bo zatarta była granica podziału między niektórymi typami przestępstw, szczególnie w grupie przestępstw skierowanych przeciwko państwu, porządkowi publicznemu i przestępstw tzw. natury politycznej.
- **Po czwarte** – statystyka kryminalna z lat 1922–1934 została **dostosowana do poziomu wykształcenia policjantów** z najniższych ogniw Policji Państwowej. To ważny walor, ponieważ trudności wynikające z niskiego wykształcenia posterunkowych były w praktyce potęgowane różnorodnością przepisów prawnych. Równocześnie funkcjonowały trzy kodeksy karne byłych zaborców (austriacki, pruski i rosyjski). Ponadto wprowadzono wiele szczegółowych aktów materialno-normatywnych i proceduralnych, w postaci zarządzeń, okólników, instrukcji itp. W omawianym okresie wszedł w życie Kodeks karny i wykroczeń z 1932 r. (autorstwa J. Makarewicza), co dodatkowo utrudniało opanowanie nowej problematyki prawnej.

Z tych wszystkich powodów władze policyjne utrzymały przedmiotowe określenie zdarzeń podlegających rejestracji, co pozwoliło na wprowadzenie i utrzymanie ciągłości statystyki przez 13 lat, tj. do czasu wdrożenia nowego ustawodawstwa. Wprowadzono w tym czasie tylko jedną drobną zmianę, która polegała na wyłączeniu z arkuszy statystycznych (w 1929 r.) pojęć: zameldowano policji i wykryty (chodzi o sprawców) i wprowadzeniu na to miejsce określeń: wiadomo policji i nie wykryto (także sprawców)[25].

---

[22] AAN, Zespół MSW, Zbiór rozkazów KG PP, t. 3, poz. 742.
[23] „Mały Rocznik Statystyczny GUS" 1938, s. 350; tenże za rok 1939, s. 362.
[24] L. Radzinowicz, *Przestępczość w Polsce w latach 1924*–1934..., s. 20–23.
[25] AAN, Zespół MSW, Zbiór rozkazów KG PP, t. 3, poz. 413, akapit IX, Rozkaz KG PP nr 413 z dnia 8 X 1928 r.

- **Po piąte** – istotną zaletą nowego systemu policyjnej statystyki przestępczości była dość duża liczba przekazywanych **informacji**. Dlatego duża, bo poza danymi o ujawnionych zdarzeniach, w wielu rubrykach notowano w tym systemie także informacje o wykrywalności sprawców czynów karalnych. Umieszczano również częściowe dane o miejscu zdarzenia (pole, las, mieszkanie, kasa) i rodzajach popełnianych przestępstw (fałszerstwa, oszustwa, kradzieże z włamaniem i bez włamania, rozboje, wymuszenia itd.). Wszystko to istotnie przybliżało ustalenie poziomu realnej przestępczości w danym roku i na określonym obszarze.

W tabeli 3 ukazano zbiorczą liczbę przestępstw i wykroczeń w Polsce (w latach 1922–1934) przedstawioną przez L. Radzinowicza.

Tabela 3

Przestępstwa i wykroczenia w Polsce w latach 1924–1934 (i ich wskaźniki)

Table 3

Crimes and misdemeanors in Poland in the years 1924–1934 (and pointers)

Rok	Suma w liczbach bezwzględnych	Wskaźniki dynamiki – 1924 r. = 100%
1924	1 948 586	100,00
1925	1 822 912	93,55
1926	1 755 052	91,09
1927	2 455 680	126,02
1928	2 232 774	114,58
1929	2 358 397	121,03
1930	2 023,192	103,82
1931	1 869 135	95,92
1932	1 945 248	99,82
1933	1 945 248	99,82
1934	2 040 123	104,69

Źródło: L. Radzinowicz, *Przestępczość w Polsce w latach 1924–1934…,* s. 25–26.

Dane zawarte w tabeli 3 jednoznacznie wskazują, że w porównaniu z rokiem 1924 najwyższą dynamikę przestępstw i wykroczeń odnotowano w roku 1927. Procentowy wskaźnik tego wzrostu wyniósł 126,02. Nieco niższy wskaźnik dynamiki był w roku następnym (114,58). Najniższy wskaźnik omawianej tendencji odnotowano w roku 1926 (91,09).

Przedstawione informacje o zbiorczym zestawieniu liczby przestępstw i wykroczeń w Polsce (w latach 1922–1934) zweryfikował Z. Piotrowski, który przeliczył wszystkie wskaźniki na podstawie zachowanych w archiwach kompletnych i oryginalnych arkuszy statystycznych PP z omawianego okresu. Wyniki tej weryfikacji (w uproszczeniu) wyglądają następująco[26]:

- wg uzupełnionych przez niego danych za rok 1922 i 1923, liczba przestępstw i wykroczeń w roku 1922 została ustalona na poziomie 858 228, a wskaźnik dynamiki wyniósł 44,06, natomiast w roku następnym, odpowiednio, 1 533 310 i 78,72;
- w 1924 r. przestępstw i wykroczeń było mniej o 925;
- w 1925 r. w wyliczeniu Radzinowicza zaniżono liczbę przestępstw i wykroczeń o 1315;
- w 1927 r. zaniżono liczbę przestępstw i wykroczeń o 8996, a wskaźnik dynamiki o 0,52%;
- w następnym roku zaniżenie to wyniosło 9013, a wskaźnik dynamiki 1,48%.

Ponadto Z. Piotrowski ustalił w ten sposób jeszcze kilka innych rozbieżności, np. w 1929 r. przestępstw i wykroczeń było mniej o 7175, a wskaźnik dynamiki był niższy o 0,31%.

Nie można przy tym wykluczyć pomyłki Z. Piotrowskiego, który wykonał bardzo żmudną i pracochłonną analizę porównawczą przedstawionych danych liczbowych i procentowych. Rozbieżności wystąpiły w liczbach bezwzględnych, natomiast różnice we wskaźnikach dynamiki mieściły się w granicach 1% /+/-1.

Można jeszcze zaprezentować dane statystyczne dotyczące stanu przestępczości opublikowane w innej książce L. Radzinowicza.

Liczby zawarte w tym zestawieniu zbiorczym dają przybliżony obraz zadań Policji Państwowej na odcinku zwalczania przestępczości. Najmniej przestępstw zarejestrowano w 1925 r. (331 742), a najwięcej w 1934 r. (657 892).

Tabela 4

Zbiorcze zestawienie statystyczne o przestępczości w Polsce w latach 1924–1934

Table 4

Summary statistics on crime in Poland in the years 1924–1934

Rok	Ogólna liczba przestępstw	Rok	Dane ze statystyki policyjnej
1924	364 033	1930	479 017
1925	331 742	1931	531 373
1926	404 654	1932	619 748
1927	450 956	1933	643 720
1928	470 194	1934	657 892
1929	485 937		

Źródło: L. Radzinowicz, *Struktura przestępczości w Polsce*, Warszawa 1937, s. 25.

[26] Z. Piotrowski, *Przestępczość w II Rzeczpospolitej...*, s. 63.

Po odjęciu liczby zarejestrowanych w danym roku przestępstw od ogólnej liczby przestępstw i wykroczeń stwierdzonych w danym roku, pozostaje liczba zarejestrowanych wykroczeń. Wykroczenia dominowały w policyjnych statystykach, np. w 1927 r. stwierdzono największą zbiorczą liczbę przestępstw i wykroczeń, która wyniosła 2 455 680, w tym zarejestrowano 450 956 przestępstw (wg wyliczeń L. Radzinowicza, tab. 4). Po odjęciu liczby przestępstw różnica wynosi 2 004 724, co stanowi sumę wykroczeń zarejestrowanych w policyjnych statystykach w 1927 r.

Podsumowanie

Nasuwające się refleksje i wnioski da się streścić w kilku następujących punktach:

1. Mimo licznych mankamentów w organizacji i działaniach Policji Państwowej w Polsce przedwrześniowej zdołano zorganizować sprawny aparat policyjny, który zapewniał społeczeństwu poczucie bezpieczeństwa i efektywnie zwalczał przestępczość.
2. Główny ciężar zadań dotyczących wykrywania i ścigania przestępstw natury kryminalnej spoczywał na barkach służby śledczej, którą powołano jako pion specjalistyczny do walki z przestępstwami.
3. Pierwsze próby opracowania i wcielenia w życie policyjnej statystyki kryminalnej miały miejsce w latach 1919–1920. Podstawę zbiorów stanowiły codzienne raporty policjantów z poszczególnych jednostek wykonawczych, początkowo z sześciu okręgów (1919 r.). Następnie udoskonalono wykazy statystyczne i gromadzono dane ze wszystkich okręgów. Przełom w organizacji statystyki nastąpił w 1922 r. Wówczas odstąpiono od codziennych r*aportów*, w to miejsce wprowadzono do użytku kolejny szczegółowy arkusz statystyczny, który prawie bez zmian funkcjonował 13 lat – do 1934 r. Kolejne zmiany nastąpiły w 1935 r.; ich charakterystyka może być przedmiotem rozważań w odrębnej publikacji.

Bibliografia

Archiwum Akt Nowych w Warszawie, Zespół MSW, Zbiór rozkazów KGPP, t. 1 i 3.

Dworzecki J., Policja w Polsce. Wybrane zagadnienia, Kraków 2011.

Halicki K., *Policja Polityczna w województwie pomorskim w latach 1920*–1939, Łódź 2015.

Hanausek T., *Kryminalistyka. Zarys wykładu*, Zakamycze 1997.

Kozdrowski S., Wyszkolenie policyjne w II Rzeczypospolitej, Kraków 2006.

Landau Z., Tomaszewski J., *Trudna niepodległość. Rozważania o gospodarce Polski* 1918–1939, Warszawa 1978.

Misiuk A., *Przyczynek do dziejów Policji Województwa Śląskiego w latach 1922*–1926, „Zeszyty Naukowe WSO" 1988, nr 3 (62).

Piotrowski Z., *Przestępczość* w II Rzeczypospolitej, wg statystyki policyjnej, 1986 – praca magisterska niepublikowana.
Radzinowicz L., *Przestępczość w Polsce w latach 1924*–1933. Na podstawie policyjnej statystyki kryminalnej, Warszawa 1935.
Radzinowicz L., *Przestępczość w Polsce w 19*34 r., „Głos Sądownictwa" 1935, nr 7–8.
Radzinowicz L., *Struktura przestępczości w Polsce*, Warszawa 1937.
Radzinowicz L., *Wpływ warunków ekonomicznych na przestępczość w Polsce w latach* 1928–1934, „Czasopismo Prawno-Historyczne" 1969, t. XXI, nr 2.
Służba śledcza. Podręcznik dla funkcjonariuszów Policji Państwowej, oprac.: podinspektor Józef Piątkiewicz, nadkomisarz dr Gabryel Lax i komisarz Józef Jakubiec – wykładowcy I kursu instruktorskiego Głównej Szkoły Policji w Warszawie, Warszawa 1928.
Szawer B.M., Winberg A.J., Kryminalistyka, Warszawa 1949.

Summary

Despite the many flaws in the organization and activities of the national police, this does not change the fact that interwar Poland managed to organize an efficient police apparatus, which gave the public a sense of security and effectively combated social crime. The main burden of tasks relating to the detection and prosecution of criminal offences rested on the shoulders of the investigative services, which was established as a specialized division to fight crime. The first attempts to develop and implement police force crime statistics took place in 1919-1920. The basic sets were the daily reports of police officers from different units, initially with six districts (1919). Then statistical lists were improved and data was collected from all districts. A breakthrough in the organization of statistics came in 1922, which departed from "daily reports". Instead a detailed statistical sheet was used that did not change much for 13 years – to 1934, and subsequent changes occurred in 1935.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 89–100 ROK 2017

ISSN 2543–7321

Mateusz Ziętarski

Akademia Pomorska
Słupsk
mateusz.zietarski@gmail.com

STRATEGIA *MODUS VIVENDI* JAKO ELEMENT WZMACNIAJĄCY BEZPIECZEŃSTWO W STOSUNKACH POLSKO-UKRAIŃSKICH

MODUS VIVENDI STRATEGY AS STRENGHTEN ELEMENT SECURITY IN THE POLISH-UKRAINIAN RELATIONS

***Zarys treści*:** Przedmiotem badań autora są bilateralne relacje Polski i Ukrainy oraz ich wpływ na bezpieczeństwo w regionie Europy Środkowo-Wschodniej. W artykule zderzone zostały dwa podejścia: popierające zbliżenie Polski z Ukrainą oraz krytykujące percepcję polskich elit, które nie dostrzegają zagrożenia w ukraińskim nacjonalizmie. Autor jako remedium na pojawiające się bariery w relacjach między państwami podaje strategię modus vivendi.

***Słowa kluczowe*:** bezpieczeństwo narodowe, bezpieczeństwo regionalne, bezpieczeństwo społeczne, strategia modus vivendi, polityka bezpieczeństwa, nacjonalizm.

Key words: national security, regional security, social security, modus vivendi strategy, security policy, nationalism.

Wstęp

Przyczynkiem do powstania niniejszego artykułu stały się niebezpieczne zdarzenia, które należy określić jako zjawisko aberracji nacjonalistycznej. Wydarzenia, które mogą wyzwolić i utrwalić niebezpieczny trend, jakim jest wzrost nastrojów nacjonalistycznych, należy uporządkować i poddać klasyfikacji. Ich źródłem i źle pojmowaną inspiracją są trudne i bolesne sploty wydarzeń w dziejach Polski i Ukrainy. Brak umiejętności antycypowania doprowadzi do anomii bilateralnych stosunków. Obecnie oba narody weszły w fazę atrofii, której egzemplifikacją jest zjawisko aberracji nacjonalistycznej przejawiające się we wzajemnych oskarżeniach. Należy przyjrzeć się tym incydentom oraz przedstawić przyczyny ich powstawania. Dia-

gnoza rzeczywistości w obecnych relacjach polsko-ukraińskich stanowić będzie punkt wyjścia do poszukiwania remedium, określonego przez autora jako element umacniający więzi.

Niebezpieczne incydenty

Pierwsze dwa wydarzenia, których ranga i wydźwięk mają charakter międzynarodowy to dewastacje pomników w Bykowni i Hucie Pieniackiej. W Bykowni znajduje się wspólny polsko-ukraiński cmentarz upamiętniający ofiary totalitaryzmu. Dewastacja pomników, które zostały pomalowane czerwoną farbą, stanowi wyraz zaniku człowieczeństwa sprawców. Niszczenie i dewastowanie miejsc ważnych dla historii kraju, a przede wszystkim miejsca pochówku osób zabitych przez NKWD w trakcie II wojny światowej oraz ofiar Wielkiego Terroru z lat 1937–1938 jest przejawem barbarzyństwa[1]. Dyrektor nekropolii w Bykowni Bohdan Bilasziwski podkreśla, że napisy pojawiły się na pomniku polskim i ukraińskim. Polska część pomnika została sprofanowana napisem gloryfikującym ugrupowanie „SS Galizien", natomiast na ukraińskiej części pojawił się napis, który w wulgarny sposób charakteryzował ugrupowania Organizacji Ukraińskich Nacjonalistów oraz Ukraińskiej Powstańczej Armii[2]. Polska premier Beata Szydło w dzień po zajściu na cmentarzu w Bykownie odniosła się do sprawy i poleciła jej wyjaśnienie na szczeblu ministerstw spraw zagranicznych. W odpowiedzi na pytania szefa polskiej dyplomacji Witolda Waszczykowskiego minister spraw zagranicznych Ukrainy Pawło Klimkin potępił opisaną wcześniej dewastację oraz ocenił ją jako akt prowokacji, której celem jest osłabienie więzi polsko-ukraińskich[3]. Podobny wydźwięk międzynarodowy miała dewastacja polskiego pomnika we wsi Huta Pieniacka, który upamiętnia akt ludobójstwa popełniony przez ukraińskich nacjonalistów na polskich obywatelach w 1944 r. Reakcja na to zdarzenie polskich władz spotkała się z szybkim odzewem i działaniami władz ukraińskich. Powołany został zespół dochodzeniowy, który zbada sprawę dewastacji dwóch polskich pomników, na których pojawił się napis „SS" i namalowana była flaga banderowska. Przedmiotem badań zespołu będzie także sprawa wysadzenia krzyża znajdującego się przy pomnikach[4]. Ambasador Ukrainy w Polsce Andrij Deshchytsia stanowczo potępił te zdarzenia i zaapelował, aby oba narody nie dały się sprowokować, gdyż o to chodzi sprawcom. W tym samym tonie wypowiadał się szef Instytutu Pamięci Narodowej na Ukrainie Wołodymyr Wiatrowycz, który wydarzenia z Huty Pieniackiej określił jako „[…] prowokację i akt wandalizmu. Prowokację, za którą stoją trzecie siły zainteresowane dalszym za-

[1] www.rp.pl/Historia/170129334-Ukraina-o-zniszczeniu-cmentarza-w-Bykowni-Prowokacja.html#ap-1 (dostęp: 25.01.2017).
[2] www.tvn24.pl/wiadomosci-ze-swiata,2/ukraina-wandale-pomazali-farba-polski-cmentarz-w-bykowni,710018.html (dostęp: 25.01.2017).
[3] http://wiadomosci.onet.pl/swiat/szef-msz-ukrainy-potepil-wandalizm-na-polskim-cmentarzu-w-bykowni/1px309b (dostęp: 25.01.2017).
[4] www.tvp.info/28547288/zdewastowano-pomnik-polakow-na-ukrainie-film-ze-zniszczeniami-trafil-do-sieci (dostęp: 25.01.2017).

ostrzeniem relacji polsko-ukraińskich”[5]. Nadzieje ambasadora Ukrainy w Polsce należy zakwalifikować jako wyraz myślenia życzeniowego, które w krajach anglosaskich znane jest jako wishful thinking, czego najbardziej wymowną egzemplifikacją jest teza premiera Wielkiej Brytanii Nevilla Chamberlaina jakoby układ monachijski stanowił gwarancję pokoju i ładu na świecie. Konsekwencją aktów wandalizmu w Bykownie i Hucie Pieniackiej, wbrew myśleniu życzeniowemu ambasadora, było pobicie studentów z Ukrainy, do którego doszło w Rzeszowie. Agresja wobec studentów zza wschodniej granicy miała pobudki nacjonalistyczne i ksenofobiczne, bowiem napastnicy zadawali pytania o przynależność Lwowa. Odpowiedź, iż obecnie jest to miasto ukraińskie wyzwoliła wrogość. Grupę ukraińskich studentów zaczęto obrażać, a następnie ciężko pobito[6]. Zdarzenie to wpisuje się w szerszy kontekst, jakim jest problem relacji polsko-ukraińskich wśród młodzieży, w tym studentów.

W Polsce najliczniejszą mniejszością podejmującą studia są właśnie obywatele Ukrainy, którzy stanowią 42% wszystkich zagranicznych studentów w Polsce[7]. Groźby, zastraszanie, wyzwiska oraz bicie są niedopuszczalne, a w środowisku akademickim winny być rugowane i eliminowane. Skonfundowanie wywołuje informacja, że najbardziej niechętni wobec obywateli Ukrainy są ludzie młodzi. Występujące antyukraińskie nastroje muszą wywołać alarm i spotkać się z merytoryczną i racjonalną krytyką. Mateusz Rojewski w swoim artykule krytykuje proces rekrutacji na polskie uczelnie, który według autora jest niesprawiedliwy i krzywdzący, bowiem promuje kandydatów z Ukrainy, otrzymujących swoisty niewidzialny bonus. Pomimo krytycznego stanowiska, w konkluzji autor przestrzega jednak przed dyskryminacją i wykluczeniem oraz apeluje o okazanie solidarności i życzliwości przybyszom z Ukrainy. Jednocześnie postuluje stworzenie przejrzystego i rzetelnego algorytmu, który jako priorytet ustanowiłby wyniki egzaminów maturalnych kandydatów[8]. Zasygnalizowanie pewnych problemów, merytoryczna argumentacja i chęć rozmowy oparte na wzajemnym poszanowaniu i wypracowaniu konsensusu to właściwe podejście. Niestety w przestrzeni publicznej nie brakuje emocjonalnych głosów, które wpisują się w ton rewanżyzmu i rewizjonizmu, przy wykorzystywaniu historii i bolesnego niekiedy splotu losów polsko-ukraińskich. Głosy te płyną często ze strony młodych, zbuntowanych obywateli Polski i Ukrainy. Skuteczna edukacja dla bezpieczeństwa, której adresatem powinna zostać młodzież zagrożona postawami nacjonalistycznymi i ksenofobicznymi, jest wielkim wyzwaniem dla obu państw.

Opisane incydenty dowodzą, że stan relacji polsko-ukraińskich wymaga poprawy. Należy pamiętać, że przypadki dewastacji polskich pomników stanowić mogą część szerzej zakrojonego planu, którego głównym założeniem jest ochłodzenie stosunków Polski z Ukrainą i przedstawienie naszego wschodniego sąsiada jako kraju,

[5] www.tvp.info/28557967/ukraincy-wyjasniaja-zniszczenie-pomnika-prowokacja-i-akt-wandalizmu (dostęp: 25.01.2017).
[6] http://rzeszow-news.pl/rasistowski-atak-rzeszowie-ukrainskich-studentow/ (dostęp: 25.01.2017).
[7] www.newsweek.pl/polska/ukrainscy-studenci-w-polsce-pogrozki-pobicia-ksenofobia,artykuly,355932,1.html (dostęp: 25.01.2017).
[8] http://krknews.pl/uczelnie-zalane-ukraincami-dyskryminacja-polakow/ (dostęp: 25.01.2017).

który nie dojrzał do niepodległości i który na tę niepodległość nie zasługuje[9]. Potrzebne jest rzetelne wyjaśnienie sprawy, do czego niezbędne jest wyzbycie się negatywnych emocji. Należy także przestrzec przed zakładaniem a priori, że to ukraińscy nacjonaliści są winni dewastacji. Dochodzenie do prawdy i proces ustaleń w tej sprawie musi odbyć się bez z góry założonej tezy. Należy wziąć pod uwagę krytykę tych zdarzeń przez władze Ukrainy i ich determinację w transparentnym i rzetelnym wyjaśnieniu sprawy stronie polskiej. Trzeba też pamiętać, że nastroje nacjonalistyczne wśród młodzieży i akty agresji stanowią zaledwie odsetek zachowań właściwych dla stosunków polsko-ukraińskich, czemu należy przeciwstawić wspólne marsze studentów z Polski i Ukrainy kwestionujących aneksję Krymu przez Federację Rosyjską. Poprawę relacji można osiągnąć dzięki zmierzeniu się z trudnymi problemami, niebezpiecznymi incydentami i równie niebezpiecznymi nastrojami nacjonalistycznymi występującymi w poszczególnych grupach. Należy zanegować deprecjonowanie, marginalizowanie i ignorowanie przedstawionych zjawisk, które mogą przeobrazić się w bariery na ścieżce porozumienia i dialogu między państwami.

W prezentowanym artykule zostanie dokonana analiza przyczyn występowania powyższych zjawisk i postawiona diagnoza. Jednak najistotniejsze jest przedstawienie strategii modus vivendi, która według autora stanowi model dla rozwiązania negatywnych aspektów relacji pomiędzy Polską i Ukrainą.

Historyczny imposybilizm relacji polsko-ukraińskich

Symbolem rozbieżności i sporów, często przeradzających się w antagonizmy, stało się ludobójstwo na Wołyniu, Organizacja Ukraińskich Nacjonalistów i Ukraińska Powstańcza Armia oraz postacie Stepana Bandery, Romana Szuchewycza, Mychajło Kołodzińskyja, Ołeksandra Hasyna.

Stepan Bandera od wczesnego dzieciństwa wykazywał bezkompromisowość. Jego świadomość i życiowe wybory zostały również ukształtowane w czasach młodzieńczych, kiedy podczas nauki w szkole średniej zaangażował się w działalność młodzieżowych organizacji nacjonalistycznych. Kolejnym krokiem w kształtowaniu jego postawy była przynależność do organizacji nacjonalistycznych w trakcie studiów na Politechnice Lwowskiej. Działalność w szeregach Organizacji Ukraińskich Nacjonalistów stała się początkiem dalszych działań, m.in. stworzenia frakcji OUN-B odpowiedzialnej za ludobójstwo Polaków zamieszkujących teren Galicji oraz Małopolski Wschodniej[10]. Bandera, przewodząc zbrodniczej działalności, dążył do powstania narodowego państwa ukraińskiego, którego warunkiem istnienia według niego była eliminacja i eksterminacja ludności nieukraińskiej. Inspiracją dla Bandery było dzieło Dmytro Dyncowa Nacjonalizm[11]. Była to wykładnia wiedzy i swoista

[9] B. Wildstein, *Demokracja limitowana czyli Dlaczego nie lubię III RP*, Poznań 2013, s. 191.
[10] G. Motyka, *Wołyń 43. Ludobójcza czystka – fakty, analogie, polityka historyczna*, Kraków 2016, s. 24.
[11] A. Drogoń, *Rzeź wołyńska – tego ludobójstwa już po prostu zakłamać się nie da*, Katowice 2016, s. 6.

instrukcja dla kadry kierowniczej OUN-B, a nie dla ludności Ukrainy. Główne hasła, które rozkręciły spiralę nienawiści i wrogości wobec innych, brzmiały: „Ukraina tylko dla Ukraińców", „Trzeba krwi – damy morze krwi"[12].

Roman Szuchewycz to druga po Banderze postać w hierarchii Organizacji Ukraińskich Nacjonalistów, a jego historia rozpoczyna się analogicznie do losów lidera ukraińskich nacjonalistów, bowiem w dzieciństwie był członkiem młodzieżowych organizacji nacjonalistycznych, w późniejszym wieku łącząc to z służbą w Ukraińskiej Organizacji Wojskowej. Szuchewycz podczas służby musiał wykonać egzekucję, wykazując tym swoje oddanie sprawie, co stało się przepustką do pełnienia wyższych funkcji – R. Szuchewycz został oddelegowany do pionu walki bieżącej Organizacji Ukraińskich Nacjonalistów, co de facto oznaczało koordynowanie działań terrorystycznych[13].

Losy Romana Szuchewycza i Mychajło Kołodzińskyja wiąże Ukraińska Organizacja Wojskowa. Kołodzińskyj, który odegrał znaczącą rolę w ludobójstwie Polaków na Wołyniu jako przewodniczący referatu wojskowego Organizacji Ukraińskich Nacjonalistów, swoją pozycję zawdzięcza pozytywnej ocenie jego służby dla Ukraińskiej Organizacji Wojskowej. W tamtym okresie był odpowiedzialny za przygotowanie powstania nacjonalistycznego, budowania podglebia rewanżyzmu, którego spiritus movens stanowić miały nastroje nacjonalistyczne. Ponadto do zadań M. Kołodzińskyja należało przygotowanie kadry wojskowej pod kątem szkoleniowym[14].

Ołeksandr Hasyn to postać, która odcisnęła piętno na warstwie ideologicznej. Zanim stał się odpowiedzialny za kształtowanie umysłów członków Organizacji Ukraińskich Nacjonalistów, zdobył wykształcenie na terenie Polski, podobnie jak S. Bandera i R. Szuchewycz. Po ukończeniu studiów na Politechnice Lwowskiej zdecydował się na działalność w organizacji harcerskiej „Płast", która była swoistym inkubatorem nacjonalistów, a jej najbardziej znanym członkiem był S. Bandera. Kolejnym etapem w życiu O. Hasyna było wstąpienie do Ukraińskiej Organizacji Wojskowej i Organizacji Ukraińskich Nacjonalistów. Działalność w tych ugrupowaniach, kontakt z najważniejszymi osobami w hierarchii ukraińskich nacjonalistów pozwoliły Hasynowi usystematyzować i uporządkować wiedzę oraz zdobyć doświadczenie, czego efektem stał się *Podręcznik wojskowy*, napisany przez Hasyna we współpracy z Jewhenem Konowalcem. Książka stała się wykładnią i źródłem wiedzy dla osób reprezentujących Organizację Ukraińskich Nacjonalistów i Ukraińską Powstańczą Armię. Bohdan Piętka, który zajmuje się badaniem ukraińskiego nacjonalizmu, uważa *Podręcznik wojskowy* O. Hasyna i Nacjonalizm D. Dyncowa za dwie najważniejsze dla ukraińskich nacjonalistów książki. Hasyn stał się później siewcą ideologii nacjonalizmu, wykładając na kursach oficerskich w radykalnym ramieniu Organizacji Ukraińskich Nacjonalistów, jakim było OUN-B. Ponadto po sformowaniu samozwańczego rządu Jarosława Stećki został mianowany wiceministrem spraw wojskowych[15].

---

[12] W. Filar, *Wydarzenia wołyńskie 1939–1944. W poszukiwaniu odpowiedzi na trudne pytania*, Toruń 2008, s. 382.
[13] G. Motyka, *Wołyń 43…*, s. 25.
[14] Tamże, s. 26–27.
[15] B. Piętka, *Nacjonalizm ukraiński. Od Bandery do Majdanu*, Warszawa 2015, s. 201–203.

Współczesne stosunki polsko-ukraińskie z historią w tle

Historia O. Hasyna została zamieszczona w niniejszym artykule nie bez przyczyny, bowiem postać pułkownika Ukraińskiej Powstańczej Armii, działacza Organizacji Ukraińskich Nacjonalistów oraz kreatora i inżyniera umysłów członków tych organizacji jest podstawą sporu, który wybuchł w maju 2013 r. Wówczas większością głosów Lwowska Rada Miejska, którą zdominowali członkowie ugrupowania „Swoboda", gloryfikującego i legitymizującego działalność Ukraińskiej Powstańczej Armii oraz Organizacji Ukraińskich Nacjonalistów, zdecydowała się nazwać jeden z placów w centrum Lwowa imieniem Ołeksandra Hasyna. W dniu tego wydarzenia we Lwowie przebywał wicemarszałek sejmu Rzeczpospolitej Polskiej Cezary Grabarczyk. Brak reakcji ze strony ważnego polskiego polityka, reprezentanta polskiego parlamentu i polskiego społeczeństwa, zirytował część opinii publicznej w Polsce[16].

Prawdziwą burzę wywołało jednak wydarzenie, które miało miejsce blisko dwa lata później. W kwietniu 2015 r. z wizytą na Ukrainie przebywał prezydent Polski Bronisław Komorowski. Rozmowy dotyczyły degradującego kraj konfliktu we wschodniej części Ukrainy, postawy Rosji oraz polskiego wsparcia dla narodu ukraińskiego. W dniu wizyty polskiego prezydenta Rada Najwyższa Ukrainy przyjęła ustawę podnoszącą członków Ukraińskiej Powstańczej Armii do rangi bohaterów narodowych[17]. Dyskurs ukraińskich polityków już wcześniej ukierunkowany został na próbę gloryfikowania członków Ukraińskiej Powstańczej Armii oraz Organizacji Ukraińskich Nacjonalistów, a egzemplifikacją takiej polityki było przyznanie Banderze tytułu „Bohatera Ukrainy" przez prezydenta Ukrainy Wiktora Juszczenkę[18]. Trudno jednak uznać prezydenta Juszczenkę za osobę zamkniętą na dialog, skupioną na ukraińskim nacjonalizmie. Świadczy o tym fakt ocieplenia relacji polsko-ukraińskich podczas „pomarańczowej rewolucji" na kijowskim Majdanie, zaprzestanie kłótni i otwarcie cmentarza Orląt Lwowskich oraz wspólne uroczystości upamiętniające wydarzenia na Wołyniu. Punktem spornym jest sposób komunikacji i retoryka, jaką przyjęli przedstawiciele polskich władz. Zachowawczość polityków, ich lęk przed sprowokowaniem i eskalowaniem drażliwych kwestii jest argumentem osób, które dopominają się o wskazanie sprawców zbrodni wołyńskiej i określenie jej mianem ludobójstwa[19].

Trudne losy Polski i Ukrainy stały się przedmiotem wielu debat i konferencji. Uczestnicy konferencji poświęconej polsko-ukraińskiemu sąsiedztwu mówili o funkcjonowaniu niebezpiecznych stereotypów. Jako przykład podano fakt, że „[…] wszystkie akty antypolskie na Ukrainie, nawet te najdrobniejsze, utożsamia się z tradycją metod działań ekstremistów z OUN czy UPA"[20]. Powszechne, według uczestników

[16] B. Piętka, *Nacjonalizm ukraiński...*, s. 200.
[17] G. Motyka, *Wołyń 43…*, s. 243.
[18] B. Mendyk, *Nacjonalizm ukraiński jako czynnik destabilizujący bezpieczeństwo publiczne*, „Securitologia" 2014, nr 1, s. 70.
[19] G. Motyka, *Wołyń 43….*, s. 221–222.
[20] M. Śliwa, *Stosunki polsko-ukraińskie w powojennej publicystyce i historiografii emigracyjnej*, [w:] *Polska i Ukraina po II wojnie światowej*, red. W. Bonusiak, Rzeszów 1998, s. 275.

konferencji, było funkcjonowanie stereotypu Ukraińca-banderowca. Natomiast badania przeprowadzone przez Romana Czmełyka i Lecha Mroza, których wyniki zostały zaprezentowane w monografii Na pograniczu nowej Europy. Polsko-*ukraińskie sąsiedztwo*, ukazują różnice pomiędzy owym stereotypem a rzeczywistym sposobem zachowania się mieszkańców Ukrainy. Osoby poddane badaniom wypowiadały się w sposób powściągliwy na tematy drażliwe dla obu narodów – okres drugiej wojny światowej, zbrodnicza działalność OUN, UPA. Wyniki przeprowadzonych badań dowodzą dużej wrażliwości społecznej oraz świadomości, że niezbędna jest ona w stosunkach polsko-ukraińskich[21]. Mieszkańcy Ukrainy doceniają polskie wsparcie i liczą na umacnianie tego procesu. Niechlubne fakty z przeszłości starają się wypełnić kartą pozytywnych stosunków pomiędzy Polską i Ukrainą. Potwierdzeniem tej tezy są wywiady przeprowadzone z niektórymi mieszkańcami Ukrainy. Jedna z ukraińskich studentek wspomina okres „pomarańczowej rewolucji", który według niej stanowił cezurę i stał się fundamentem nowego otwarcia w relacjach polsko-ukraińskich. Polska bowiem podtrzymała na duchu naród ukraiński, okazała wielowymiarowe wsparcie. Zdaniem ukraińskiej studentki te wydarzenia pozwoliły obu krajom wyzwolić sąsiedzką przyjaźń[22].

Trafną diagnozę tamtych i obecnych stosunków sformułował Grzegorz Motyka, który podkreśla, że kult ugrupowań nacjonalistycznych jest elementem kodu kulturowego i narodowotwórczego mieszkańców Ukrainy. Autor stoi na stanowisku, iż ultymatywne żądanie całościowego potępienia i stygmatyzowania Ukraińskiej Powstańczej Armii i Organizacji Ukraińskich Nacjonalistów doprowadzi do eskalacji nieporozumień polsko-ukraińskich. Jednocześnie badacz ten podkreśla, że nie wolno pozwolić na marginalizowanie, deprecjonowanie, a wreszcie przemilczenie zbrodni, co więcej, według niego należy forsować termin adekwatny do tamtych zdarzeń, jakim jest ludobójstwo[23]. B. Wildstein uważa, iż stawianie ultimatum Ukrainie jest działaniem krótkowzrocznym. Kwestia uznania przez Ukrainę zbrodniczych działań Ukraińskiej Powstańczej Armii oraz Organizacji Ukraińskich Nacjonalistów, uznania czynów na Wołyniu za ludobójstwo oraz, co najważniejsze, przeproszenie za tamten ponury okres winny stanowić priorytet w polityce zagranicznej skierowanej na Ukrainę. Należy jednak pamiętać o osiąganiu tego dzięki polityce dialogu[24]. Wagę więzi polsko-ukraińskich należy rozpatrywać na dwóch płaszczyznach.

Pierwszą jest wspólnota losów i uwarunkowania geopolityczne, które determinują współpracę przeciwko imperialnej polityce Federacji Rosyjskiej[25]. Nie da się problematyki poruszonej w tym artykule analizować abstrahując od nielegalnej aneksji Krymu, rosyjskiej agresji na Ukrainę i permanentnego wspierania prorosyjskich separatystów. Zagrożenie rosyjskim imperializmem funkcjonuje w percepcji społeczeństw państw Europy Środkowo-Wschodniej, dlatego Polska stała się de facto re-

[21] R. Czmełyk, L. Mróz, *Pamięć przedzielona rzeką*, [w:] *Na pograniczu „nowej Europy". Polsko-ukraińskie sąsiedztwo*, red. M. Zowczak, Warszawa 2010, s. 66–67.
[22] A. Pruszyński, *Obcy pośród nas. Radiowe reportaże o Ukraińcach w Polsce po 2005 roku,* [w:] *Polska-Ukraina. Dziedzictwo i współczesność*, red. R. Drozd, T. Sucharski, Słupsk 2012, s. 306.
[23] G. Motyka, *Wołyń 43…*, s. 245–246.
[24] B. Wildstein, *Demokracja limitowana…*, s. 191.
[25] Tamże, s. 190.

prezentantem i lobbystą sprawy ukraińskiej. Zbigniew Brzeziński przekonuje, że „[…] utrwalenie niepodległości Ukrainy ma takie samo znaczenie jak wejście Polski do NATO, eliminuje bowiem zagrożenie od Wschodu i zamyka 250-letni okres, w którym Polska, zagrożona z obu stron, była krajem niezależnym jedynie przez dwadzieścia lat”[26]. Polska jest jednym z krajów mających pełną świadomość znaczenia powyższych słów, okazuje zrozumienie i wsparcie wobec ukraińskich działań zmierzających do umocnienia niepodległości i suwerenności oraz wzmacnia marsz Ukrainy ku zachodnim strukturom. Polska poprzez kreowanie pozytywnego wizerunku Ukrainy, stając się de facto jej ambasadorem w strukturach unijnych, wypracowała sobie miano państwa-stabilizatora w regionie Europy Środkowo-Wschodniej[27].

Drugą płaszczyzną jest optyka narodu ukraińskiego, który nie w pełni popiera nacjonalistyczne nastroje i nie w pełni utożsamia się z ideologią nacjonalistyczną. Punktem wyjścia do dyskusji i uświadamiania historycznego powinien być sondaż przeprowadzony na Ukrainie, w którym 53% ankietowanych opowiedziało się za odebraniem tytułu „Bohatera Ukrainy” Banderze. Należy pamiętać, że społeczeństwo ukraińskie jest bardzo zróżnicowane i podzielone. Losy obu państw w okresie pozimnowojennym również są zróżnicowane i przypominają sinusoidę. Pierwszy okres związany jest ze strategicznym partnerstwem, które wyzwoliło wielopłaszczyznową współpracę zahamowaną w drugim okresie, który w literaturze przedmiotu nazywany jest okresem rozczarowania. Następnie pojawił się okres renesansu współpracy politycznej, który trwa do dziś[28]. Przykładem jest wielkie wsparcie dla Ukrainy podczas dwóch wielkich zrywów narodowych: pomarańczowej rewolucji i protestu na Euromajdanie.

Piotr Sztompka w pracy zatytułowanej Socjologia wymienia symptomy traumy. Wśród nich znajduje się syndrom braku zaufania, syndrom apatii i syndrom nostalgii. Trzy powyższe elementy stanowią fundament diagnozy, która dotyczy barier w relacjach polsko-ukraińskich. Przezwyciężenie tych syndromów pozwoli uniknąć uwiądu, a w dalszym stadium anomii więzi pomiędzy sąsiednimi państwami[29]. Jej podstawą powinny stać się pozytywne momenty współpracy obu państw, tożsame geopolityczne cele oraz pozytywne symptomy prawidłowego odbioru Ukraińców.

Strategia modus vivendi jako remedium na anomię relacji polsko-ukraińskich

Strategia modus vivendi jest modelowym sposobem prowadzenia rozmów, rozwijania stosunków bilateralnych i multilateralnych pomimo istniejących rozbieżnych kwestii. Modus vivendi jest to środek, który obiera państwo w celu ułożenia stosunków na arenie międzynarodowej. Możliwość osiągnięcia takich relacji wymaga pominięcia najbardziej rozbieżnych i zapalnych kwestii, co powoduje wypracowanie porozumienia i późniejszego konsensusu. Modus vivendi zakłada jednak uregulowa-

[26] Z. Brzeziński, *Wielka szachownica*, Warszawa 1999, s. 41.
[27] D. Gibas-Krzak, *Ukraina – między Rosją a Polską*, Toruń 2004, s. 102–103.
[28] Tamże, s. 68–69.
[29] P. Sztompka, *Socjologia*, Kraków 2009, s. 465.

nie spraw różniących obie strony. Niebezpieczeństwo, jakie niesie ze sobą ten sposób prowadzenia polityki międzynarodowej związane jest z percepcją problemów przez zainteresowane strony. Jeżeli rozbieżne kwestie są bagatelizowane przez jedną ze stron, wówczas trudno o dialog i osiągnięcie konsensusu. Skuteczność strategii modus vivendi uzależniona jest zatem od właściwego podejścia, którym jest określenie przez strony wagi problemu i jego chwilowe odsunięcie, tak by nie przysłaniał punktów wspólnych. Wówczas stanowić one będą fundament do stworzenia recepty pozwalającej przezwyciężyć dzielące kwestie. Po ustaleniu skutecznego rozwiązania strony zobowiązane są do podjęcia rozmów na temat punktów spornych i kwestii zapalnych[30].

Historia związków polsko-ukraińskich jest często naznaczona krwią i okrucieństwem. Poza ekstremum, jakim było ludobójstwo na Wołyniu były również inne wydarzenia dzielące Polaków i Ukraińców, m.in. wojna z lat 1918–1919, powstanie Chmielnickiego czy koliszczyzna. Słusznie jednak przedstawia się determinanty, które powinny stanowić przyczynek do umacniania współpracy bilateralnej i regionalnej. Przez wielu autorów Ukraina przedstawiana jest jako kraj ważny dla Polski ze względu na zagrożenie imperialną polityką Federacji Rosyjskiej, wspólne dla Polski i Ukrainy[31].

W nurt budowania, a wręcz odbudowywania wzajemnych więzi z wykorzystaniem strategii modus vivendi wpisuje się m.in. G. Motyka, który w swojej książce *Wołyń 43* przytacza wypowiedź Tetiany Czornowoł, będącej symbolem ukraińskiej rewolucji na Euromajdanie, która stwierdza, że „[…] trzeba mieć odwagę nazywać rzeczy po imieniu. Zabijanie wielkiej liczby ludzi z jakichkolwiek narodowych czy rasowych powodów jest ludobójstwem. I jeśli Ukraińcy dopuścili się go na Wołyniu, to ja za to przepraszam. A z drugiej strony UPA to dla mnie bohaterowie”[32]. G. Motyka uważa, iż takie sformułowania powinny stanowić fundament uzdrowienia relacji polsko-ukraińskich. Strategia modus vivendi przewiduje pominięcie najbardziej rozbieżnych kwestii, w tym przypadku będzie to ocena działalności Ukraińskiej Powstańczej Armii, Organizacji Ukraińskich Nacjonalistów, diametralnie różna w Polsce i na Ukrainie. Skupiając się na pozytywnych aspektach wypowiedzi T. Czornowoł, czyli przyznaniu, że rzeź wołyńska była ludobójstwem i, co ważniejsze, na przeprosinach i żalu za tamte wydarzenia, możemy budować wspólną narrację. Potępienie ludobójstwa na Wołyniu jest bowiem celem priorytetowym. Budując dialog i wspólnie dokonując analizy historii związków polsko-ukraińskich, możemy przedkładać argumentację, która pozwoli na zaprzestanie dokonywania aktów deifikacji względem Ukraińskiej Powstańczej Armii i Organizacji Ukraińskich Nacjonalistów. Będzie to powrót do nierozwiązanych jeszcze kwestii w myśl strategii modus vivendi.

Autor niniejszego artykułu przeprowadził badania na temat wykorzystania powyższej strategii przez Federację Rosyjską w wojnie rosyjsko-ukraińskiej. Wykorzystując strategię modus vivendi, Rosja odwróciła uwagę światowej opinii publicz-

[30] M. Ziętarski, *Russian* modus vivendi *strategy in Ukraine,* [w:] *Security in the conditions of bifurcation of the international system. Challenges for policy and education*, red. M. Brodnicki, G. Cimek, D. Bień, Kijów 2016, s. 113.
[31] B. Wildstein, *Demokracja limitowana...*, s. 190–191.
[32] G. Motyka, *Wołyń 43...*, s. 246–247.

nej od agresji skierowanej na państwo ukraińskie, rewizji jej granic wskutek aneksji Krymu i przeprowadzenia tam nielegalnego referendum. W politycznym, medialnym i publicznym dyskursie nie pojawiał się ten problem. Zastąpiona przez inne wydarzenia tematyka aneksji Krymu, a szerzej, rosyjskiej agresji na Ukrainę i pogwałcenia prawa międzynarodowego zostały całkowicie zmarginalizowane[33]. Przykład ten dowodzi, że prezentując strategię modus vivendi jako swoiste remedium na pojawiające się bariery w relacjach polsko-ukraińskich, należy przestrzec przed jej częściowym zastosowaniem oraz cynicznym wykorzystaniem. Strategia ta bowiem nie może stanowić planu ucieczki przed trudnymi rozmowami o tragedii polskich mieszkańców Wołynia i Galicji Wschodniej. Należy o tym pamiętać, przypominać i uświadamiać – zwłaszcza elity ukraińskie i całe społeczeństwo ukraińskie w myśl zasady papieża Grzegorza I, który twierdził, że „[…] nawet jeśli prawda może powodować zgorszenie, lepiej dopuścić do zgorszenia niż wyrzec się prawdy". Strategia modus vivendi jest sposobem na przytaczanie prawdy, uświadamianie o faktach bez uczucia zgorszenia. Wielka wrażliwość, która potrzebna jest w kontaktach między Polską a Ukrainą powinna widnieć jako punkt agendy rozmów między państwami, natomiast z agendy tej powinna zniknąć historia jako narzędzie polityczne. W jej miejscu powinna widnieć historia jako nauka, która wiedzie do poznania prawdy.

Zakończenie

Pozytywny i niezaprzeczalny dla wzbogacenia nauki i kultury aspekt współpracy polsko-ukraińskiej przedstawia Łarysa Masenko. Autorka przypomina więź łączącą Jurija Szewelowa i Jerzego Giedroycia, której pokłosiem stało się opracowanie i wydanie dzieła Rozstrzelane Odrodzenie. Jest to niezmiernie ważna pozycja w literaturze, przypominająca bowiem zapomniane, a w latach dwudziestych XX w. zakazane przez władze Związku Radzieckiego zbiory literatury ukraińskiej. Doceniając inicjatywę i wytężoną pracę na rzecz literatury ukraińskiej J. Giedroycia, Ł. Masenko uważa, że „[…] tradycje kontaktów polsko-ukraińskich, wspólnej działalności w sferze nauki i kultury wymagają kontynuacji i rozwoju również obecnie, gdy Polska weszła już do kręgu wolnych narodów Europy"[34]. O wpływie polskiej kultury świadczy fakt określenia zrywu z roku 2004 mianem pomarańczowej rewolucji. Do tego momentu w ukraińskim zbiorze leksykalnym nie funkcjonował rzeczownik pomarańcza i pochodny od niego przymiotnik pomarańczowy. Nazwanie wielkiego protestu pomarańczową rewolucją świadczy o wpływie języka polskiego[35]. Pomarańczowa rewolucja pokazała empatię i wsparcie ze strony polskich władz, polskich elit i polskiego społeczeństwa. Taka postawa spotkała się z wdzięcznością Ukraińców, a w badaniach sondażowych dotyczących sympatii dla innych krajów ukraiń-

[33] M. Ziętarski, *Russian* modus vivendi…, s. 113–114.
[34] Ł. Masenko, *Język, przemiany społeczno-polityczne i współpraca międzynarodowa*, [w:] *Ukraińska humanistyka i słowiańskie paralele*, red. M. Bracka, A. Bracki, M. Żmudzka-Brodnicka, M. Brodnicki, Gdańsk-Kijów 2014, s. 89–90.
[35] Tamże, s. 91–92.

scy respondenci na pierwszym miejscu wskazali Polskę[36]. W bibliografii pomarańczowej rewolucji, opracowanej przez Instytut Geopolityki, Robert Potocki i Agnieszka Stec prezentują całą listę osób wyróżnionych za wsparcie ukraińskich dążeń ku Europie[37].

Przedstawione przykłady pokazują więź, jaka splata oba narody pomimo trudnej i bolesnej historii. Ponadto, co najważniejsze, mogą wraz ze szczerymi wypowiedziami, w których widoczny jest żal i przeprosiny za wyrządzone krzywdy, stanowić fundament odbudowy relacji polsko-ukraińskich. Opisane w tym artykule incydenty, wydarzenia o charakterze nacjonalistycznym i ksenofobicznym oraz wykorzystywanie historii prowadzą do atrofii, a ostatecznie do anomii więzi obu narodów. Eksperci Fundacji Batorego projektowali zmiany w strukturach Unii Europejskiej w stosunku do Ukrainy. W nawiązaniu do relacji polsko-ukraińskich głosili tezę, iż „[…] w sprawach dotyczących zaszłości historycznych w sposób szczególny należy rekomendować spokój oraz systematyczną konsekwentną pracę”[38]. Powyższa teza jest swoistą klamrą spinającą zapisy strategii modus vivendi. Zastosowanie tej strategii do naprawy, a w późniejszym okresie także umocnienia wspólnych więzi jest propozycją autora. Ze względu na znaczenie relacji polsko-ukraińskich dla bezpieczeństwa w wymiarze międzynarodowym, narodowym, regionalnym i społecznym strategia modus vivendi, jako środek redukujący zagrożenia, jest potrzebna w optyce obu narodów oraz elit, które projektują i zarządzają bezpieczeństwem.

Bibliografia

Berdychowska B., Stosunki polsko-*ukraińskie po pomarańczowej rewolucji. Propozycj*e dla polskiej polityki zagranicznej, [w:] *Więcej niż sąsiedztwo. Rozszerzona Unia E*uropejska i Ukraina. Nowe relacje, Fundacja im. Stefana Batorego, Warszawa 2005.

Brzeziński Z., Wielka szachownica, Warszawa 1999.

Czmełyk R., Mróz L., *Pamięć przedzielona rzeką*, [w:] Na pograniczu nowej Europy. Polsko-*ukraińskie sąsiedz*two, red. M. Zowczak, Warszawa 2010.

Drogoń A., *Rzeź wołyńska – tego ludobójstwa już po prostu zakłamać się nie da*, Katowice 2016.

Filar W., *Wydarzenia wołyńskie 1939*–1944. W poszukiwaniu odpowiedzi na trudne pytania, Toruń 2008.

Gibas-Krzak D., Ukraina – *między Rosją a Polską*, Toruń 2004.

Kowalski M., Malicki J., *Błękit pomarańczy, czyli raport o podzielonym narodzie*, [w:] *Ukraina na zakręcie. Drogi i bezdroża pomarańczowej rewolucji*, aut. J.M. Nowakowski i in., Warszawa 2005.

[36] M. Kowalski, J. Malicki, *Błękit pomarańczy, czyli raport o podzielonym narodzie*, [w:] *Ukraina na zakręcie. Drogi i bezdroża pomarańczowej rewolucji*, aut. J.M. Nowakowski i in., Warszawa 2005, s. 70.

[37] R. Potocki, A. Stec, *Polska bibliografia pomarańczowej rewolucji*, t. 1, Częstochowa 2008, s. 175–178.

[38] B. Berdychowska*, Stosunki polsko-ukraińskie po pomarańczowej rewolucji. Propozycje dla polskiej polityki zagranicznej*, [w:] *Więcej niż sąsiedztwo. Rozszerzona Unia Europejska i Ukraina. Nowe relacje*, Fundacja im. Stefana Batorego, Warszawa 2005, s. 10.

Masenko Ł., *Język, przemiany społeczno-polityczne i współpraca międzynarodowa*, [w:] *Ukraińska humanistyka i słowiańskie paralele*, red. M. Bracka, A. Bracki, M. Żmudzka-Brodnicka, M. Brodnicki, Gdańsk-Kijów 2014.
Motyka G., *Wołyń 43. Ludobójcza czystka* – fakty, analogie, polityka historyczna, Kraków 2016.
Mendyk B., *Nacjonalizm ukraiński jako czynnik destabilizujący bezpieczeństwo publiczne*, „Securitologia" 2014, nr 1.
Piętka B., *Nacjonalizm ukraiński. Od Bandery do Maj*danu, Warszawa 2015.
Potocki R., Stec A., *Polska bibliografia pomarańczowej rewolucji*, t. I, Częstochowa 2008.
Pruszyński A., *Obcy pośród nas. Radiowe reportaże o Ukraińcach w Polsce po 2005 r*oku, [w:] Polska – *Ukraina. Dziedzictwo i współczesność*, red. R. Drozd, T. Sucharski, Słupsk 2012.
Sztompka P., Socjologia, Kraków 2009.
Śliwa M., Stosunki polsko-*ukraińskie w powojennej publicystyce i historiografii emigr*acyjnej, [w:] *Polska i Ukraina po II wojnie światowej*, Rzeszów 1998.
Wildstein B., Demokracja lim*itowana czyli Dlaczego nie lubię III RP*, Poznań 2013.
Ziętarski M., Russian modus vivendi strategy in Ukraine, [w:] Security in the conditions of bifurcation of the international system. Challenges for policy and education, red. M. Brodnicki, G. Cimek, D. Bień, Kijów 2016.

http://krknews.pl/uczelnie-zalane-ukraincami-dyskryminacja-polakow/ (dostęp: 25.01.2017).
www.rp.pl/Historia/170129334-Ukraina-o-zniszczeniu-cmentarza-w-Bykowni-Prowokacja.html#ap-1 (dostęp: 25.01.2017).
www.newsweek.pl/polska/ukrainscy-studenci-w-polsce-pogrozki-pobicia-ksenofobia,artykuly,355932,1.html (dostęp: 25.01.2017).
http://rzeszow-news.pl/rasistowski-atak-rzeszowie-ukrainskich-studentow/ (dostęp: 25.01.2017).
www.tvn24.pl/wiadomosci-ze-swiata,2/ukraina-wandale-pomazali-farba-polski-cmentarz-w-bykowni,710018.html (dostęp: 25.01.2017).
http://wiadomosci.onet.pl/swiat/szef-msz-ukrainy-potepil-wandalizm-na-polskim-cmentarzu-w-bykowni/1px309b (dostęp: 25.01.2017).
www.tvp.info/28547288/zdewastowano-pomnik-polakow-na-ukrainie-film-ze-zniszczeniami-trafil-do-sieci (dostęp: 25.01.2017).
www.tvp.info/28557967/ukraincy-wyjasniaja-zniszczenie-pomnika-prowokacja-i-akt-wandalizmu (dostęp: 25.01.2017).

Summary

The inspiration for the author of this article are incidents that threaten Polish-Ukrainian relations. Revived nationalism contributes to the reasons for undertaking research on the condition Polish-Ukrainian relations. After-effects of the manipulation of history will be imcompatible with dialogue between both countries. The solution is the development and strengthening of Polish-Ukrainian relations, while conducting difficult conversations about the complexity of our common history. The instrument that will strengthen relations is a modus vivendi strategy.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 101–118 ROK 2017

ISSN 2543–7321

Ireneusz Bieniecki

Akademia Pomorska
Słupsk
bieniecki.ireneusz@vp.pl

SZKOŁA CHORĄŻYCH WOJSK OCHRONY POGRANICZA W KĘTRZYNIE I JEJ ROLA W PRZYGOTOWANIU KADR DLA OBRONNOŚCI KRAJU W LATACH 1969–1991

THE MILITARY SCHOOL OF TROOP BORDER PROTECTION IN KĘTRZYN AND ITS ROLE IN PREPARING STAFF FOR NATIONAL DEFENCE IN THE YEARS 1969–1991

***Zarys treści*:** W artykule przedstawiono powstanie i rozwój organizacyjny Szkoły Chorążych Wojsk Ochrony Pogranicza w Kętrzynie w latach 1969–1991 oraz jej znaczenie w przygotowaniu kadry dla tej formacji. Omówiono m.in. takie zagadnienia, jak: rozwój organizacyjny tej placówki, organizację i przebieg procesu nauczania kadetów, nauczane przedmioty oraz osiągane wyniki w nauce.

***Słowa kluczowe*: s**zkolnictwo Wojsk Ochrony Pogranicza, Szkoła Chorążych Wojsk Ochrony Pogranicza w Kętrzynie, szkolenie kadry dla potrzeb ochrony granicy PRL

Key words: Education of Border Troops, Warrant Officer School of Border Troops in Kętrzyn, Staff training for border protection needs in Polish People's Republic

Wstęp

Wojska Ochrony Pogranicza (WOP), które utworzono 13 września 1945 r., funkcjonowały do 15 maja 1991 r. W tym czasie formacja ta wielokrotnie zmieniała swoje struktury organizacyjne, dostosowując je do potrzeb istniejącego w tych latach systemu ochrony granicy państwowej[1]. Przez ponad 45 lat pełniła w niej służbę znaczna grupa żołnierzy zawodowych i służby zasadniczej. Przygotowaniem perso-

[1] Zob.: J. Prochwicz, Wojska Ochrony Pogranicza 1945–1965. Wybrane problemy, Piotrków Trybunalski 2001; H. Łach, *System ochrony polskiej granicy państwowej w latach 1989*–2004, Olsztyn 2013.

nelu dla potrzeb tej formacji zajmowało się wiele ośrodków podlegających Ministerstwu Spraw Wewnętrznych (MSW), jak i Ministerstwu Obrony Narodowej (MON). Szkoliły one zarówno kadrę, jak i podoficerów oraz specjalistów z grupy żołnierzy zasadniczej służby wojskowej (zsw).

W zakresie przygotowania personelu zawodowego na uwagę zasługują szkoły działające w Kętrzynie: Oficerska Szkoła WOP (OfS WOP), Szkoła Chorążych WOP (SCh WOP) i Podoficerska Szkoła Zawodowa WOP (PSZ WOP). Po rozwiązaniu w roku 1968 OfS WOP formacja ta była w szerszym niż dotychczas zakresie zasilana absolwentami Wyższych Szkół Oficerskich (WSO), Szkół Chorążych (SCh) i Podoficerskich Szkół Zawodowych (PSZ) Ministerstwa Obrony Narodowej. Od lat siedemdziesiątych XX w. SCh WOP w Kętrzynie stała się jedyną placówką tej formacji przygotowującą do ochrony granicy średni personel zawodowy w różnych specjalnościach.

Do roku 1991 potrzeby dotyczące przygotowania korpusu chorążych do ochrony granicy państwowej PRL były zróżnicowane w poszczególnych okresach – zarówno pod względem liczby chorążych, jak i posiadanych przez nich specjalności. Przed powołaniem SCh WOP – w połowie roku 1969 – zapotrzebowanie na personel w korpusie chorążych dla tej formacji szacowano na 30–40 żołnierzy przygotowywanych w dwuletnim cyklu szkoleniowym[2].

Dlatego też w roku 1970 na bazie Oficerskiej Szkoły Wojsk Ochrony Pogranicza sformowano Centralny Ośrodek Kształcenia Wojsk Wewnętrznych (COK WW – zarządzenie Szefa Sztabu Wojsk Obrony Wewnętrznej z 15 lipca 1970 r.) Ośrodek ten funkcjonował w Kętrzynie przy ul. Gen. Sikorskiego 102 i podlegał Głównemu Inspektoratowi Obrony Terytorialnej (GIOT) w Warszawie. W jego strukturze organizacyjnej oprócz Podoficerskiej Szkoły Zawodowej WOP funkcjonowała też SCh WOP. W tym czasie w placówce tej pobierało naukę 33 kadetów, których wcielono do służby 25 września 1969 r.[3] Do 15 września 1971 r. komendantem Centralnego Ośrodka Kształcenia Wojsk Wewnętrznych był płk Zbigniew Furgała a następnie płk dypl. Józef Sawczuk.

Na przełomie lat sześćdziesiątych i siedemdziesiątych XX w. potrzeby kadrowe WOP w znacznym zakresie zaspokajali też absolwenci szkół wojskowych MON. Na przykład jesienią 1971 r. na uzupełnienie jednostek Wojsk Wewnętrznych (WOP i WOW – Wojsk Obrony Wewnętrznej) przyjęto grupę absolwentów WSO, SCh i Szkół Podoficerskich MON. Tylko do jednostek WOP (Brygad – BWOP i Oddziałów – OWOP) trafiło ogółem 93 (100%) absolwentów tych szkół, w tym najwięcej z: Wyższych Szkół Oficerskich – 54 (58,1%), Szkół Chorążych – 37 (39,8%) i Podoficerskiej Szkoły Zawodowej im. Rodziny Nalazków w Elblągu – 2 (2,1%). Najwięcej absolwentów WSO otrzymało przydział do 8. BWOP (18,5%) a absolwentów SCh do 3. BWOP (29,7%)[4].

---

[2] Archiwum Straży Granicznej (dalej ASG) w Szczecinie, Akta DWOP, sygn. nr 1839, t. 2, Notatka służbowa w sprawie centralnego ośrodka szkolenia i doskonalenia kadr Wojsk Ochrony Pogranicza nr 01838 z 24 kwietnia 1969 r., s. 3 oraz załącznik nr 1.

[3] ASG w Szczecinie, Akta CSWOP, sygn. nr 1759, t. 8, Rozkaz komendanta Ośrodka Szkolenia WOP płka dypl. Józefa Sawczuka nr pf 161 z 22.09.1969 r., s. 1.

[4] ASG w Szczecinie, Akta DWOP, sygn. nr 1841, t. 2, Zestawienie liczbowe absolwentów Wyż-

Tabela 1
Przydział absolwentów szkół wojskowych jesienią 1971 r. do jednostek WOP
Table 1
The military school graduates in autumn 1971 of The Troop Border Protection units

Lp.	Nazwa jednostki	Absolwenci			Razem absolwentów
		WSO	SCh	PSZ	
1.	3. BWOP	2	**11**	1	**14**
2.	4. BWOP	5	2	-	**7**
3.	5. BWOP	1	5	-	**6**
4.	8. BWOP	**10**	-	-	**10**
5.	9. BWOP	8	1	-	**9**
6.	12. BWOP	5	3	-	**8**
7.	15. BWOP	6	-	-	**6**
8.	16. BWOP	7	-	1	**8**
9.	MBOP	8	3	-	**11**
10.	19. OWOP	1	1	-	**2**
11.	22. OWOP	-	4	-	**4**
12.	23. OWOP	1	3	-	**4**
13.	26. OWOP	-	3	-	**3**
14.	Ośrodek Szkolenia WW (w Kętrzynie)	-	1	-	**1**
Ogółem		**54**	**37**	**2**	**93**
Odsetek ogółu		**58,1**	**39,8**	**2,1**	**100**

MBOP – Morska Brygada Okrętów Pogranicza

Źródło: ASG w Szczecinie, Akta DWOP, sygn. nr 1841, t. 2, Zestawienie liczbowe absolwentów Wyższych Szkół Oficerskich, Szkół Chorążych i Podoficerskiej Szkoły Zawodowej im. Rodziny Nalazków, które przybyły na uzupełnienie Wojsk Wewnętrznych 15.09.1971 r. nr pf 809 z 15.09.1971 r., s. 1.

W roku 1972 w programie szkolenia SCh WOP w sposób następujący określono cel kształcenia słuchaczy: „Zasadniczym celem szkolenia kadetów jest wykształcenie i wychowanie pełnowartościowego chorążego zwiadu WOP – szczerze oddanego swemu narodowi, Polskiej Zjednoczonej Partii Robotniczej, Rządowi Polskiej Rzeczypospolitej Ludowej, ofiarnego obrońcy i gorącego szermierza idei budownictwa socjalistycznego, związanego braterstwem broni z sojuszniczymi armiami państw socjalistycznych, a w szczególności z Armią Radziecką; o wysokich walo-

szych Szkół Oficerskich, Szkół Chorążych i Podoficerskiej Szkoły Zawodowej im. Rodziny Nalazków, którzy przybyli na uzupełnienie Wojsk Wewnętrznych 15.09.1971 r. nr pf 809 z 15.09.1971 r., s. 1.

rach moralnych i etycznych oraz odpowiednio przygotowanego do pełnienia funkcji pomocników dowódców placówki i kontrolera ruchu granicznego”[5].

Z treści powyższego cytatu wynika, że przełożeni widzieli przyszłego chorążego zwiadu (służby operacyjno-rozpoznawczej) tej formacji jako żołnierza zawodowego o uniwersalnych cechach, który byłby jednocześnie człowiekiem zaangażowanym politycznie (po stronie PZPR – Polskiej Zjednoczonej Partii Robotniczej) i żołnierzem dobrze przygotowanym do realizacji zadań w ochronie granicy.

Już w tym czasie kadeci SCh WOP szkolili się przez okres roku, który rozpoczynał się 1 października a kończył 31 sierpnia. Ze względu na krótki czas nauki, szkolenie kadetów można uznać za bardzo intensywne.

Na szkolenie społeczno-polityczne, ogólnowojskowe i specjalistyczne przeznaczano ogółem 219 dni. Długość dnia szkoleniowego była zróżnicowana, w zależności od tego czy był to dzień powszedni, czy przedświąteczny. W dniach powszednich, których było 170, szkolenie trwało 7 godzin, natomiast w dni przedświąteczne (49) czas szkolenia był krótszy i wynosił 6 godz. Godzina lekcyjna trwała 45 min.

W obowiązującym programie szkolenia dla obu plutonów SCh WOP (operacyjno-kontrolerskiego i operacyjnego) najwięcej czasu przeznaczano na: szkolenie specjalne (46,6%), szkolenie społeczno-polityczne – 9,1%, szkolenie techniczne (samochodowe – 8,1%), naukę języków obcych (7,1%) i szkolenie graniczne (6,1%)[6]. Od dwóch do trzech dni w miesiącu przeznaczano na samokształcenie. W porządku dnia, oprócz zajęć programowych, przewidywano:

- po dwie godziny w tygodniu na ćwiczenia sprawnościowe z wychowania fizycznego,
- godzinę w tygodniu na informację polityczną w czasie pozaprogramowym.

Ponadto w porządku dnia przewidywano 2–3 godz. na naukę własną, w tym także czas przeznaczony na inne przedsięwzięcia związane ze szkoleniem, pracą kulturalno-oświatową, konserwacją broni, sprzętu itp.

W pierwszych dwóch miesiącach nauki organizowano szkolenie pod kątem przygotowania kadetów do złożenia przysięgi wojskowej i pełnienia służby wartowniczej. W ramach doskonalenia znajomości regulaminów byli oni wyznaczani do pełnienia służby wartowniczej i garnizonowej w dniach dyspozycyjnych, gospodarczych i świątecznych.

Obowiązkową naukę własną organizowano dla kadetów w wymiarze określonym w porządku dnia – w każdym dniu tygodnia w godzinach popołudniowych, z wyjątkiem sobót i dni świątecznych.

Podczas trwania szkolenia przeprowadzano egzaminy i kolokwia zgodnie z programem. Egzamin dyplomowy organizowano i prowadzono w oparciu o obowiązujące w tym zakresie przepisy. Natomiast egzaminy z zakresu szkolenia samochodowego prowadziła uprawniona do tego komisja Wydziału Komunikacji Powiatowej Rady Narodowej.

---

[5] ASG w Szczecinie, Akta CS WOP, sygn. nr 1862, t. 106, Tymczasowy program szkolenia rocznej Szkoły Chorążych WOP (plutony operacyjno-kontrolerskie i plutony operacyjne), Kętrzyn 1972, s. 2.

[6] Tamże, s. 9.

Za wszystkie czynności dotyczące programowania i planowania szkolenia odpowiadał wydział szkolenia Ośrodka Szkolenia WOP (OS WOP) w Kętrzynie, a cykl zwiadu opracowywał dokumenty w zakresie planowania tematyki zwiadowczej, uwzględniając roczny i miesięczne plany przygotowane przez wydział szkolenia oraz potrzeby wypływające z *Programu Tematycznego Szkolenia Specjalistycznego Kadetów SCh WOP*[7].

Każdorazowo przed rozpoczęciem roku szkoleniowego komendant OS WOP przeprowadzał odprawę szkoleniową z kadrą szkoły, podczas której podsumowywał przebieg szkolenia za rok ubiegły i stawiał zadania na nowy rok szkolny.

Z powyższego wynika, że życie i kształcenie kadetów szkoły było podporządkowane realizacji zadań wychowawczych i szkoleniowych, a wszystkie zajęcia organizowano i prowadzono w taki sposób, aby stanowiły one jednocześnie poglądową lekcję wzorowego przygotowania i prowadzenia ćwiczeń. Cały materiał szkoleniowy działu ogólnowojskowego był podporządkowany taktyce działu szkolenia specjalnego (szkoleniu zwiadowczo-granicznemu). Jako podstawową metodę szkolenia kadetów stosowano zajęcia praktyczne (ćwiczenia laboratoryjne). Zajęcia praktyczne poprzedzano niezbędnymi wykładami i ćwiczeniami pokazowymi, a podczas wykładów omawiano zasadnicze problemy, wytyczano kierunki samodzielnej pracy i wskazywano literaturę fachową.

W procesie szkolenia kadetów zakładano, że materiał pamięciowy, który nie wymagał specjalnych wyjaśnień, zostanie przez nich opanowany w trakcie pracy samokształceniowej. W celu doskonalenia umiejętności instruktorskich wyznaczano też kadetów kolejno do prowadzenia zajęć oraz na instruktorów[8].

W roku 1972 na bazie Centralnego Ośrodka Kształcenia Wojsk Wewnętrznych sformowano Ośrodek Szkolenia WOP (OS WOP – zarządzenie Szefa Sztabu Generalnego WP nr 055/Org. z 9 czerwca 1972 r.). Podlegał on Dowództwu WOP (DWOP) w Warszawie, a w jego strukturze organizacyjnej nadal funkcjonowała SCh WOP. Komendantami Ośrodka byli płk mgr Stanisław Majcher (do 26 września 1978 r.) i płk dypl. Ryszard Bartoszewicz[9].

Na podstawie zarządzenia MSW nr 95/72 z 12 września 1972 r. w sprawie organizacji szkół i kursów WOP z dniem 1 marca 1973 r. komendant OS WOP płk mgr Stanisław Majcher rozwiązał Radę Wychowawczą w SCh WOP, a w jej miejsce powołał kilkunastoosobową Radę Pedagogiczną, której przewodniczącym został zastępca komendanta OS WOP ds. zwiadu[10].

Każdorazowo etap nauki kadetów w SCh WOP kończył się egzaminami komisyjnymi, np. zgodnie z rocznym planem zamierzeń i zarządzeniem dowódcy WOP (nr pf 67 z 2 sierpnia 1972 r.) od 20 do 24 sierpnia 1973 r. przeprowadzono egzaminy dyplomowe z kadetami SCh WOP w Kętrzynie z ośmiu przedmiotów:

---

[7] Tamże, s. 2–5.

[8] Tamże, s. 6–7.

[9] Z. Jackiewicz, Wojska Ochrony Pogranicza 1945–*1991. Krótki informator historyczny,* Kętrzyn 1988, s. 161.

[10] ASG w Szczecinie, Akta OSWOP, sygn. nr 2048, t. 9, Rozkaz komendanta OS WOP płka mgra Stanisława Majchera nr 27 z 13.02.1973 r. w sprawie Rady Ośrodka, Rad Pedagogicznych SCh WOP i PSZ WOP, s. 1–3.

- szkolenie społeczno-polityczne,
- szkolenie operacyjne,
- szkolenie graniczne,
- szkolenie operacyjno-kontrolerskie,
- szkolenie z zakresu kryminalistyki dochodzenia i wybranych zagadnień prawnych,
- szkolenie graniczno-taktyczne,
- szkolenie ogniowe,
- szkolenie z zakresu regulaminów[11].

Do SCh WOP w Kętrzynie 25 września 1973 r. wcielono 96 słuchaczy i z początkiem października zostali oni zaliczeni do stanu zmiennego kadetów na rok szkolny 1973/1974[12].

Do dalszej rozbudowy SCh WOP w Kętrzynie, zarówno pod względem liczby przyjmowanych kadetów, jak i liczby tworzonych plutonów szkolnych w poszczególnych specjalnościach, doszło w latach siedemdziesiątych XX w. O ile w roku szkolnym 1974/1975 utworzono 5 plutonów (3 w pierwszej kompani i 2 w drugiej), to już w roku 1979/1980 było ich 7, liczących łącznie 209 kadetów[13]. W roku szkolnym 1974/1975 w pierwszej kompanii (dowódca kpt. Marian Tomasik, szef sierż. Radziejewski) funkcjonowały 3 plutony operacyjno-kontrolerskie, natomiast w drugiej kompanii (dowódca por. Tadeusz Ekstowicz, szef plut. Leszek Lewandowski) funkcjonowały dwa plutony – pluton polityczny (dowódca ppor. Konrad Kubasiak) oraz pluton operacyjny (dowódca ppor. Marek Kazuła). Komendantem szkoły w tym czasie był ppłk mgr Zdzisław Samul, natomiast jego zastępcą ds. politycznych mjr mgr Ryszard Małkowski[14].

Do końca lat siedemdziesiątych XX w. liczba kandydatów do tej szkoły systematycznie wzrastała. Pierwotnie grupa kandydatów do SCh WOP w roku 1979 wg stanu z 25 października tego roku liczyła 416 osób, w tym 350 (84,1%) było wcielonych przez WKU, a 66 (15,9%) z jednostek wojskowych. Jednak do egzaminów przystąpiła nieco mniejsza liczba osób – 363, w tym 297 wcielonych przez WKU i 66 z jednostek wojskowych. Egzaminy zdało i zostało przyjętych ogółem 192 (100%) kandydatów, w tym 132 (68,8%) pochodzących z cywila i 60 (31,2%) z jednostek wojskowych. Ponadto przyjęto do SCh WOP z Wojskowych Komend Uzupełnień (WKU) 8 osób z nadwyżek innych szkół wojskowych i 9 osób z dodatkowego naboru (7 z WKU i 2 z jednostek WOP).

Ostatecznie do SCh WOP przyjęto łącznie 209 słuchaczy, w tym 147 (70,3%) wcielonych przez WKU i 62 (29,7%) z jednostek wojskowych. Jednak od 25 wrze-

[11] ASG w Szczecinie, Akta OS WOP, Rozkaz komendanta OS WOP płka Stanisława Majchera nr pf 136 z 11.08.1973 r. w sprawie egzaminów dyplomowych kadetów SCh WOP, s. 1–3.

[12] ASG, Akta OS WOP, sygn. nr 2048, t. 9, Rozkaz personalny komendanta OS WOP płka mgra Stanisława Majchera nr 0170 z 2.10.1973 r. w sprawie zaliczenia kandydatów w poczet kadetów SCh WOP, s. 1–4.

[13] Materiały własne autora.

[14] ASG w Szczecinie, Akta OS WOP, sygn. nr 2049, t. 9, Rozkaz komendanta OS WOP płka mgra Stanisława Majchera nr pf 293 z 11.10.1974 r., s. 2; oraz materiały własne autora.

śnia 1979 r. do 25 października 1979 r. wykruszyło się 20 (21,5%) słuchaczy, w tym 2 wcielonych przez WKU i 18 z jednostek wojskowych.

Do pierwszego etapu egzaminów w SCh WOP w Kętrzynie w roku 1979 (sprawdzian psychotechniczny) przystąpiło 363 kandydatów. Egzaminy zdało 215 osób a przyjętych zostało 200 (100%) kandydatów, z tego 60 (30%) żołnierzy zsw z jednostek wojskowych. Ponadto 15 kandydatów zdało egzamin z wynikiem pomyślnym, jednak ze względu na brak miejsc nie zostali przyjęci do SCh WOP. Powołano ich do Szkoły Podoficerskiej w Sudeckiej Brygadzie WOP (Kłodzko), a po jej ukończeniu i odbyciu półrocznej praktyki w jednostkach w roku szkolnym 1980/1981 mieli być przyjęci bez egzaminów do SCh WOP w Kętrzynie.

W tym czasie ze względu na duży napływ kandydatów do SCh WOP nie prowadzono w ośrodkach szkoleniowych MON specjalnej akcji werbunkowej, która miała na celu pozyskanie dodatkowych chętnych kandydatów do placówki. Jedynie w 8 przypadkach przejęto z ośrodków szkoleniowych MON wartościowych kandydatów do SCh WOP.

Ponadto, w wyniku dodatkowego naboru oraz uwzględnienia odwołań, na podstawie decyzji dowódcy WOP przyjęto 9 kandydatów, w tym 2 z wojska. Łącznie w tym roku przyjęto do SCh WOP 209 kandydatów, w tym:

- z Wojskowych Komend Uzupełnień (WKU) – 147 kandydatów (70,3%),
- z jednostek wojskowych MON – 38 (18,2%),
- z jednostek WOP – 24 (11,5%).

209 kadetów rozpoczęło naukę, jednak do 25 października 1979 r. zrezygnowało z niej 20, a dalszych 2 po złożeniu rezygnacji oczekiwało w tej sprawie na decyzję dowódcy WOP.

W roku szkolnym 1979/1980 w SCh WOP zorganizowano 7 profili szkolenia, w tym 3 zwiadowcze.

Tabela 2

Profile szkolenia i liczba kadetów w SCh WOP w roku szkolnym 1979/1980

Table 2

Training profiles and the number of cadets in Troop Border Protection Warrant Officers school for the school year 1979/1980

Lp.	Profil nauki	Liczba plutonów	Liczba kadetów		Łączna liczba kadetów	Odsetek ogółu kadetów
			z WKU	z wojska		
1.	Zwiadowczy	3	86	16	**102**	**48,8**
2.	Ogólnowojskowy	1	-	30	**30**	**14,4**
3.	Polityczny	1	19	5	**24**	**11,5**
4.	Samochodowy	1	23	4	**27**	**12,9**
5.	Łączności	1	19	7	**26**	**12,4**
Ogółem		**7**	**147**	**62**	**209**	**100**

Źródło: ASG w Szczecinie, Akta DWOP, sygn. nr 2526, t. 96, Notatka szefa Oddz. Org.-Mob. i Uzup. Sztabu WOP płka Tadeusza Góry w sprawie naboru kandydatów i rozpoczęcia nauki w SCh WOP w roku szkolnym 1979/1980, s. 2.

Ocena poziomu intelektualnego przyjętych kandydatów do SCh WOP przeprowadzona przez przełożonych wykazała ich wysoką wartość (podobnie jak w roku ubiegłym). Z ogólnej liczby kadetów przyjętych do szkoły 51% miało świadectwa szkolne z przeciętną ocen bardzo dobrą i dobrą, a 65% ogółu przyjętych uzyskało na egzaminach wstępnych średnie oceny bardzo dobrą i dobrą. Gorzej prezentowała się ich sprawność fizyczna, gdyż aż 63% ogółu przyjętych uzyskało z WF tylko oceny dostateczne.

Przekrój społeczny przyjętych kadetów wg deklarowanego pochodzenia był następujący:

- robotnicze – 113 (54,1%).
- inteligenckie – 56 (26,8%),
- chłopskie – 40 (19,1%).

W grupie tej spory odsetek stanowiły też osoby wywodzące się z rodzin związanych zawodowo ze służbami mundurowymi – 41 osób (19,6%), z czego 21 miało ojców pełniących służbę w wojsku, a 10 rodziców było funkcjonariuszami MSW.

W grupie przyjętych kandydatów bardzo wiele było osób deklarujących przynależność do różnych organizacji politycznych i społecznych, w tym najwięcej do:

- Związku Socjalistycznej Młodzieży Polskiej – 89 (42,6%),
- Polskiej Zjednoczonej Partii Robotniczej – 42 (20,1%),
- Ligi Obrony Kraju – 19 (9,1%),
- Związku Harcerstwa Polskiego – 58 (20,8%),
- Stronnictwa Demokratycznego – 1 (0,5%).

Spośród nich 26 miało pisemne rekomendacje z tych organizacji, a 42 opinie polecające.

W tym czasie najwięcej kandydatów przyjętych do SCh WOP pochodziło z następujących województw:

- olsztyńskiego – 18 (8,6%),
- gorzowskiego i katowickiego – po 11 (5,3%),
- suwalskiego – 10 (4,8%),
- zielonogórskiego – 9 (4,3%).

W roku tym nie stwierdzono też rażących nieprawidłowości dotyczących przygotowania i terminowego przesyłania dokumentów oraz kierowania kandydatów na egzaminy kwalifikacyjne. Pewne uchybienia wystąpiły jednak w zakresie stosowanej procedury związanej z naborem, a dotyczyły one przesłania niekompletnych dokumentów oraz typowania kandydatów nieposiadających średniego wykształcenia. Ponadto przesłano 19 teczek akt personalnych kandydatów mających negatywną opinię organów Wojskowej Służby Wewnętrznej (WSW)[15].

Podobnie jak w roku ubiegłym, nabór do SCh WOP w roku 1979 charakteryzował się stosunkowo dużym napływem kandydatów. Przy uwzględnieniu nakazanego limitu przyjęć (ok. 200 miejsc) SCh WOP miała w tym czasie do 2 kandydatów na 1 miejsce, chociaż w roku tym nie zabiegano o przejęcie nadwyżek kandydatów na studia z ośrodków szkoleniowych MON. Według oceny przełożonych poziom intelektualny, przekrój społeczny, stopień upartyjnienia kadetów rozpoczynających

[15] Tamże, s. 3.

w tym roku naukę nadal się poprawiał. Zmniejszył się natomiast znacznie napływ kandydatów będących synami żołnierzy zawodowych i funkcjonariuszy Milicji Obywatelskiej (MO w 1978 r. – 51, w 1979 r. – 31).

Należy podkreślić, że w tym czasie formacja WOP (wg stanu na 5 maja 1979 r.) miała znaczną liczbę wakatów na stanowiskach żołnierzy zawodowych – 1128 (100%), w tym najwięcej – 499 (44,2%) na stanowiskach oficerskich, 221 (19,6%) na stanowiskach chorążych i 408 (36,2%) na stanowiskach podoficerów zawodowych.

W roku 1979 dla potrzeb formacji wypromowano 66 oficerów specjalności WOP w WSO Wojsk Zmechanizowanych (we Wrocławiu) i 209 chorążych z SCh WOP oraz pozyskano do służby zawodowej 54 żołnierzy wcielonych w październiku 1977 r., co jednak nie rozwiązywało problemów kadrowych. Dzięki tym przyjęciom tylko w korpusie chorążych nastąpiło nasycenie kadrą, jednak, jak oceniano, sytuacja była tylko pozornie dobra, bowiem w jednostkach WOP wielu chorążych zajmowało wakujące stanowiska oficerskie. W tej sytuacji, przy uwzględnieniu wielkości wykruszeń w korpusie chorążych, przewidywano utrzymanie w kolejnych latach limitu kandydatów przyjmowanych do SCh WOP na poziomie 200 osób.

Ponadto zwracano uwagę, że w roku 1979 masowo wykruszali się kadeci SCh WOP, co było motywowane sytuacją osobistą (na własną prośbę). Tylko w pierwszych trzech tygodniach nauki ubyło ze szkoły 20 kadetów, w tym 18 skierowanych z jednostek wojskowych. Z ogólnej liczby skreślonych kadetów 12 (60%) szkolono w profilu ogólnowojskowym. Ponadto kolejnych 2 oczekiwało na decyzję w sprawie zwolnienia[16].

W roku 1980 doszło do kolejnej reorganizacji ośrodka szkolenia w Kętrzynie. Na bazie dotychczasowego Ośrodka Szkolenia WOP sformowano bowiem Centrum Szkolenia WOP (CS WOP – zarządzenie org. MSW nr 054/WW z 12 września 1980 r.). Centrum to podlegało Dowództwu WOP w Warszawie, a w jego składzie organizacyjnym funkcjonowała nadal SCh WOP. Komendantami Centrum byli: płk dypl. Ryszard Bartoszewicz (do 31 sierpnia 1985 r., płk mgr Bogdan Mazurek (do 18 sierpnia 1990 r.) i płk Marek Śmiałkowski.

Jesienią 1980 r. mianowano kolejną grupę kadetów SCh WOP – 141 osób (100%) na stopień młodszego chorążego. Najliczniejsza ich grupa została awansowana w korpusie osobowym chorążych, w następujących specjalnościach:

- WSW – 84 (59,6%),
- łączności w grupie dowódczo-sztabowej – 18 (12,8%),
- samochodowych w grupie samochodowej – 15 (10,6%),
- politycznych – 13 (9,2%),
- piechoty w grupie ogólnowojskowej – 11 (7,8%)[17].

Latem 1981 r. ukazał się rozkaz dowódcy WOP nakazujący przeprowadzenie od 9 do 12 lipca 1981 r. kolejnego naboru do SCh WOP na lata nauki 1981–1983, w celu skompletowania obsady personalnej. Powołana w tym celu komisja miała zakwa-

[16] Tamże, s. 4.

[17] ASG w Szczecinie, Akta CS WOP, sygn. nr 2253, t. 18, Rozkaz personalny ministra Spraw Wewnętrznych Stanisława Kowalczyka nr 03768 z 18.09.1980 r., s. 1–4.

lifikować najbardziej wartościowych 150 kandydatów do nauki w dwóch profilach szkolenia:

- łączności, o rocznym cyklu nauczania, dla 30 kandydatów (jeden pluton) z wojska oraz pozyskanych z WKU,
- zwiadowczym, o dwuletnim cyklu nauczania, dla 120 kandydatów (cztery plutony po 30 kandydatów) z wojska oraz pozyskanych z WKU.

Szkolenie kadetów przyjętych do SCh na lata 1981–1983 realizowano wg programu przesłanego do Kętrzyna przez Dowództwo WOP. Jednocześnie dowódca WOP zabronił przenoszenia kadetów w ramach SCh pomiędzy poszczególnymi profilami szkolenia[18].

Podobną liczbę kadetów wcielano do SCh WOP w Kętrzynie po wprowadzeniu w Polsce stanu wojennego (13 grudnia 1981 r.). Np. od 9 do 15 lipca 1983 r. przeprowadzono badania psychologiczne i próbę sprawności fizycznej dla kolejnej grupy kandydatów do SCh WOP. W tym samym czasie dokonano naboru na pierwszy rok nauki spośród kandydatów skierowanych z WKU i jednostek wojskowych. Ogółem do 6 plutonów, w czterech specjalnościach, powołana komisja zakwalifikowała 159 najbardziej wartościowych kandydatów.

W roku szkolnym 1983/1984 utworzono następujące profile szkolenia w SCh WOP:

- zwiadowczy (o dwuletnim cyklu nauczania dla 90 kandydatów – 3 plutony po 30 kadetów),
- łączności (o dwuletnim cyklu nauczania dla 24 kandydatów),
- zakwaterowania i budownictwa (o rocznym cyklu nauczania dla 24 kandydatów – wyłącznie mających wykształcenie technika budowlanego i technika instalacji sanitarnych),
- służby granicznej (tresura psów o rocznym cyklu nauczania dla 21 kandydatów – wyłącznie mających wykształcenie technika hodowcy zwierząt, technika weterynarii, zootechnika)[19].

W połowie dekady lat osiemdziesiątych XX w. w CS WOP w Kętrzynie organizowano również kursy przeszkoleniowe dla chorążych tej formacji, np. od 17 do 19 stycznia 1984 r. powołana komisja przeprowadziła egzaminy końcowe na kursie przeszkolenia chorążych WOP z 6 przedmiotów, ze szkolenia: społeczno-politycznego, operacyjnego, operacyjno-kontrolerskiego, prawno-kryminalistycznego, graniczno-taktycznego i z zakresu znajomości regulaminów[20].

W roku 1986 przyjęto na profil zwiadowczy WOP do SCh WOP 132 kandydatów. Po egzaminach przejściowych na drugi rok nauki na profil zwiadowczy zakwalifikowano 112 kadetów, a 20 z różnych powodów się wykruszyło. Powody wykruszenia kadetów z profilu zwiadowczego w tym czasie były związane z:

[18] ASG w Szczecinie, Akta CS WOP, sygn. nr 2264, t. 37, Rozkaz dowódcy WOP gen. dyw. Czesława Stopińskiego nr pf. 1074 z 8.07 1981 r., s. 1–2.

[19] ASG w Szczecinie, Akta DWOP, sygn. nr 2519, t. 80, Zarządzenie dowódcy WOP gen. bryg. Feliksa Stramika nr 034/Sztab. z 21.06.1983 r. w sprawie ukompletowania SCh WOP na I rok nauki, s. 1–4.

[20] ASG w Szczecinie, Akta CS WOP, sygn. nr 2429, t. 20, Sprawozdanie przewodniczącego komisji płka Antoniego Kacprzyka z przeprowadzonego egzaminu końcowego kursu przeszkolenia chorążych WOP nr pf 176 z 8.01.1984 r., s. 1–4.

- rezygnacją z nauki na własną prośbę – 11,
- niezadowalającym stanem zdrowia – 7,
- dyscypliną kadetów – 2[21].

Natomiast podczas drugiego roku z nauki na profilu zwiadowczym SCh WOP zrezygnowało już tylko 4 kadetów (w tym 2 ze względu na niezadowalający stan zdrowia i 2 na własną prośbę).

Ostatecznie do egzaminów końcowych w SCh WOP dopuszczono 108 (100%) kadetów o profilu zwiadowczym, z których 92 (85,2%) uzyskało ocenę dobrą, 13 (12%) ocenę dostateczną i 3 (2,8%) ocenę bardzo dobrą. Nie było oceny niedostatecznej.

Oceniając stan moralno-polityczny i dyscyplinę egzaminowanych kadetów, przewodniczący komisji płk mgr Jerzy Wolski zwrócił uwagę, że w roku szkolnym 1986/1987 i 1986/1987 kształtował się on na poziomie dobrym, a stosunek kadetów do ówczesnej polityki partii (PZPR) i rządu oraz aktualnej sytuacji społeczno-politycznej i gospodarczej uznano za prawidłowy.

W ocenianym okresie tytuł i brązową odznakę „Wzorowego Kadeta" uzyskało 11 słuchaczy. Według stanu z 6 maja 1988 r. do PZPR należało 48 kadetów, co stanowiło znaczny odsetek (44,4%) stanu osobowego. Natomiast do ZSMP deklarowało przynależność 98 kadetów, co stanowiło 90,7% kadetów zdających egzaminy końcowe[22].

Również w drugiej połowie lat osiemdziesiątych XX w. weryfikację efektów kształcenia kadetów SCh WOP przeprowadzano podobnie jak w latach wcześniejszych, np. od 30 kwietnia do 5 maja 1988 r. komisja powołana rozkazem komendanta CS WOP w Kętrzynie przeprowadziła egzaminy końcowe.

W tym samym roku kończył się też jednoroczny kurs w SCh WOP o profilu budowlanym. Do przeprowadzenia egzaminów końcowych od 10 do 17 sierpnia 1988 r. rozkazem komendanta CS WOP powołano komisję pod przewodnictwem płka dypl. Marka Śmiałkowskiego. Efektywność szkolenia w tej specjalności była również stosunkowo wysoka, bowiem naukę w roku 1987 rozpoczęło 12 kadetów, natomiast do egzaminów końcowych dopuszczono 10 z nich. 2 kadetów zrezygnowało z nauki – 1 ze względu na niezadowalający stan zdrowia i 1 na własną prośbę. Z egzaminowanych 10 kadetów tego profilu 9 uzyskało ocenę dobrą, a 1 ocenę bardzo dobrą (bez ocen dostatecznych i niedostatecznych)[23].

Należy jednak podkreślić, że w końcu lat osiemdziesiątych XX w. skompletowanie kadry SCh WOP było nadal niepełne, a przydatność części z członków tej kadry była wątpliwa, np. niekompletna była obsada etatowa w I i II kompanii tej placówki. W I kompani brakowało 2 dowódców plutonów (szkolnych), a funkcję tę pełnili kadeci. Jednak, jak stwierdzono, duże zaangażowanie całej kadry SCh WOP pozwoliło na uzyskanie dobrych wyników ze wszystkich egzaminowanych przedmiotów. Generalnie uznano, że kadra szkoły miała dobre przygotowanie do wykonywania za-

[21] ASG w Szczecinie, Akta CS WOP, sygn. nr 2474, t. 42, Protokół z przebiegu egzaminów końcowych SCh WOP w 1988 r. nr pf. 608 z 5.05.1989 r., s. 1.
[22] Tamże, s. 1–4.
[23] ASG w Szczecinie, Akta CS WOP, sygn. nr 2474, t. 42, Protokół z przebiegu egzaminów końcowych SCh WOP w 1988 r. nr pf. 1586 z 18.08.1988 r., s. 1–3.

wodu. Personel zawodowy miał ukończone studia I°, a ponadto 1 oficer kontynuował studia II°, 1 ukończył kurs oficerski, a szefowie pododdziałów mieli ukończone szkoły średnie[24].

Do końca lat osiemdziesiątych XX w. w SCh WOP kształcono kadetów w podobnych profilach, np. w roku 1988 do tej placówki szkoleniowej przyjęto łącznie 150 kandydatów w dwóch specjalnościach – zwiadowczej – 116 i ogólnowojskowej – 34, a w roku następnym przyjęto ponadto 23 kadetów na profil łączności. Po pierwszym roku z nauki zrezygnowało łącznie 22 kadetów (14,7%), w tym 12 z profilu zwiadowczego (8%) i 10 z profilu ogólnowojskowego (6,7%). Najczęściej kadeci zwalniali się na własną prośbę – 14 (9,3%) oraz ze względu na zły stan zdrowia – 6 (4,0%)[25].

Tabela 3

Powody rezygnacji kadetów SCh WOP z kontynuowania nauki po pierwszym roku szkolenia w 1989 r.

Table 3

Reasons for the resignation of cadets in the Troop Border Protection warrant officers school after the first year of study in 1989

Lp.	Powody zwolnienia	Profile nauki:		Razem	Odsetek ogółu
		zwiadowczy	ogólno-wojskowy		
1.	Na własną prośbę	7	7	**14**	**63,6**
2.	Ze względu na stan zdrowia	4	2	6	**27,3**
3.	Ze względu na negatywną opinię kadeta	1	1	**2**	**9,1**
4.	Ze względu na słabe postępy w nauce	-	-	-	-
Ogółem		**12**	**10**	**22**	**100**
Odsetek ogółu		**54,5**	**45,5**	**100**	

Źródło: ASG w Szczecinie, Akta CS WOP, sygn. nr 2484, t. 35, Protokół z przebiegu egzaminów końcowych SCh WOP w 1990 r. nr pf. 854 z 23.07.1990 r., s. 1.

Natomiast na drugi rok nauki w SCh WOP dopuszczono 128 kadetów, w tym na kierunku zwiadowczym 104 (81,2%), a ogólnowojskowym 24 (18,8%).

Podczas szkolenia w drugim roku nauki zwolniono z różnych powodów łącznie 33 kadetów (100%), z tego 28 (84,8%) na własną prośbę.

[24] ASG w Szczecinie, Akta CS WOP, sygn. nr 2474, t. 42, Protokół z przebiegu egzaminów końcowych SCh WOP w 1988 r. nr pf. 608 z 5.05.1989 r., s. 1–4.

[25] ASG w Szczecinie, Akta CS WOP, sygn. nr 2484, t. 35, Protokół z przebiegu egzaminów końcowych SCh WOP w 1990 r. nr pf. 854 z 23.07.1990 r., s. 1.

Tabela 4

Przyczyny rezygnacji kadetów SCh WOP z kontynuowania nauki po drugim roku szkolenia w 1989 r.

Table 4

Reasons for the resignation of cadets in Troop Border Protection warrant officers school after the second year of study in 1989

Lp.	Powody zwolnienia	Profile nauki			Razem	Odsetek ogółu
		zwiadowczy	ogólno-wojskowy	łączności		
1.	Na własną prośbę	18	4	6	**28**	**85**
2.	Ze względu na stan zdrowia	-	1	-	**1**	**3**
3.	Ze względu na negatywną opinię kadeta	1	-	-	**1**	**3**
4.	Ze względu na słabe postępy w nauce	2	-	-	2	**6**
5.	Na skutek wypadków	1	-	-	1	**3**
Ogółem		**22**	**5**	**6**	**33**	**100**
Odsetek ogółu		**66,7**	**15,1**	**18,2**	**100**	

Źródło: ASG w Szczecinie, Akta CS WOP, sygn. nr 2484, t. 35, Protokół z przebiegu egzaminów końcowych SCh WOP w 1990 r. nr pf. 854 z 23.07.1990 r., s. 1.

Do egzaminów końcowych w roku 1990 w SCh WOP dopuszczono 82 kadetów na kierunku zwiadowczym, 19 na kierunku ogólnowojskowym i 17 na kierunku łączności z II kompanii oraz 1 podoficera zawodowego (plutonowy) z CS WOP.

Podczas nauki 2 kadetów otrzymało tytuł i srebrną odznakę „Wzorowego Kadeta", a 15 tytuł i brązową odznakę „Wzorowego Kadeta".

Również w roku 1990 w protokole egzaminacyjnym SCh WOP w Kętrzynie przewodniczący komisji egzaminacyjnej płk mgr Franciszek Nowak stwierdził, że obsada tej placówki była niekompletna, bowiem brakowało 2 dowódców plutonów, a funkcje te w zastępstwie pełnili kadeci. Jednak i w tym okresie znaczne zaangażowanie całej kadry pozwoliło uzyskać dobre wyniki ze wszystkich egzaminowanych przedmiotów. Oceniono też, że kadra SCh WOP miała dobre przygotowanie do zawodu. 1 oficer miał ukończone studia II°, pozostali studia I°, a 1 oficer ukończył kurs oficerski. Ponadto szefowie kompanii szkolnych mieli ukończone szkoły średnie. Bieżące szkolenie kadry w tym czasie realizowano zgodnie z wytycznymi[26].

Ostatecznie z dniem 15 maja 1991 r. Centrum Szkolenia WOP zakończyło działalność i zostało rozformowane, a w dniu następnym przekształcono je w Centrum Szkolenia Straży Granicznej RP w Kętrzynie.

[26] Tamże, s. 2–4.

Podsumowanie

Podsumowując ponad dwudziestoletni okres działalności SCh WOP w Kętrzynie, należy stwierdzić, że w tym czasie placówka ta wykształciła kilkutysięczną grupę żołnierzy zawodowych w korpusie chorążych, którzy w większości zasilili szeregi kadry pełniącej bezpośrednio służbę w ochronie polskich granic. Otrzymali oni przygotowanie fachowe w różnych specjalnościach i w olbrzymiej większości dobrze realizowali postawione przed nimi zadania na granicy. Najwięcej przedstawicieli korpusu chorążych kształciło się w tej placówce w profilach: operacyjno-kontrolerskim, kontrolerskim i operacyjnym, a mniej w innych kierunkach, co było podyktowane potrzebami ochrony granicy. Ze względu na występujące braki w korpusie oficerskim wielu z nich dalszą służbę pełniło również na stanowiskach oficerskich. Od lat osiemdziesiątych XX w. zakwalifikowani przez przełożonych z jednostek WOP przedstawiciele korpusu chorążych mieli też możliwość podwyższania swoich kwalifikacji i awansowania na jednorocznych kursach oficerskich organizowanych w Kętrzynie bądź w innych ośrodkach szkoleniowych. Należy również wspomnieć o tym, że liczna grupa chorążych w drugiej połowie XX w. ukończyła studia w cywilnych uczelniach wyższych, po których byli też awansowani na kolejne stopnie oficerskie.

Ze względu na krótki, trwający tylko rok, okres nauki SCh WOP w Kętrzynie cieszyła się w latach siedemdziesiątych i osiemdziesiątych XX w. sporym zainteresowaniem ze strony tych kandydatów, którzy zamierzali docelowo wybrać zawód żołnierza zawodowego. Dlatego stosunkowo często zdarzały się sytuacje, że kandydaci i podchorążowie z Wyższych Szkół Oficerskich rezygnowali z wybranych wcześniej wojskowych uczelni wyższych i decydowali się na kontynuowanie nauki w SCh WOP w Kętrzynie.

Z chwilą rozwiązania WOP i powstania Straży Granicznej olbrzymia większość chorążych przygotowanych w SCh WOP w Kętrzynie do służby w ochronie granicy państwowej kontynuowała ją po 1991 r. w nowej formacji.

Bibliografia

Archiwum Straży Granicznej (ASG) w Szczecinie

Akta CS WOP, sygn. nr 1862, t. 106, Tymczasowy program szkolenia rocznej szkoły chorążych WOP (plutony operacyjno-kontrolerskie i plutony operacyjne), Kętrzyn 1972

Akta CS WOP, sygn. nr 2484, t. 35, Protokół z przebiegu egzaminów końcowych SCh WOP w 1990 r. nr pf. 854 z 23.07.1990 r.

Akta CS WOP, sygn. nr 2474, t. 42, Protokół z przebiegu egzaminów końcowych SCh WOP w 1988 r. nr pf. 1586 z 18.08.1988 r.

Akta CS WOP, sygn. nr 2474, t. 42, Protokół z przebiegu egzaminów końcowych SCh WOP w 1988 r. nr pf. 608 z 5.05.1989 r.

Akta CS WOP, sygn. nr 2429, t. 20, Sprawozdanie przewodniczącego komisji płka Antoniego Kacprzyka z przeprowadzonego egzaminu końcowego kursu przeszkolenia chorążych WOP nr pf 176 z 8.01.1984 r.

Akta CS WOP, sygn. nr 2474, t. 42, Protokół z przebiegu egzaminów końcowych SCh WOP w 1988 r. nr pf. 608 z 5.05.1989.
Akta CS WOP, sygn. nr 2253, t. 18, Rozkaz personalny ministra Spraw Wewnętrznych Stanisława Kowalczyka nr 03768 z 18.09.1980 r.
Akta CS WOP, sygn. nr 2264, t. 37, Rozkaz dowódcy WOP gen. dyw. Czesława Stopińskiego nr pf. 1074 z 8.07 1981 r.
Akta CS WOP, sygn. nr 1862, t. 106, Tymczasowy program szkolenia rocznej Szkoły Chorążych WOP (plutony operacyjno-kontrolerskie i plutony operacyjne), Kętrzyn 1972.
Akta CS WOP, sygn. nr 1759, t. 8, Rozkaz komendanta Ośrodka Szkolenia WOP płka dypl. Józefa Sawczuka nr pf 161 z 22.09.1969 r.
Akta DWOP, sygn. nr 1841, t. 2, Zestawienie liczbowe absolwentów Wyższych Szkół Oficerskich, Szkół Chorążych i Podoficerskiej Szkoły Zawodowej im. Rodziny Nalazków, którzy przybyli na uzupełnienie Wojsk Wewnętrznych 15.09.1971 r. nr pf 809 z 15.09.1971 r.
Akta DWOP, sygn. nr 1839, t. 2, Notatka służbowa w sprawie centralnego ośrodka szkolenia i doskonalenia kadr Wojsk Ochrony Pogranicza nr 01838 z 24 kwietnia 1969 r., s. 3 oraz załącznik nr 1.
Akta DWOP, sygn. nr 2526, t. 96, Notatka szefa Oddz. Org.-Mob. i Uzup. Sztabu WOP płka Tadeusza Góry w sprawie naboru kandydatów i rozpoczęcia nauki w SCh WOP w roku szkolnym 1979/1980.
Akta DWOP, sygn. nr 2519, t. 80, Zarządzenie dowódcy WOP gen. bryg. Feliksa Stramika nr 034/Sztab. z 21.06.1983 r. w sprawie ukompletowania SCh WOP na I rok nauki.
Akta OS WOP, sygn. nr 2048, t. 9, Rozkaz personalny komendanta OS WOP płka mgra Stanisława Majchera nr 0170 z 2.10.1973 r. w sprawie zaliczenia kandydatów w poczet kadetów SCh WOP.
Akta OS WOP, sygn. nr 2049, t. 9, Rozkaz komendanta OS WOP płka mgra Stanisława Majchera nr pf 293 z 11.10.1974 r.
Akta OS WOP, sygn. nr 2048, t. 9, Rozkaz komendanta OSWOP płka mgra Stanisława Majchera nr 27 z 13.02.1973 r. w sprawie Rady Ośrodka, Rad Pedagogicznych SCh WOP i PSZ WOP.
Akta OS WOP, Rozkaz komendanta OS WOP płka Stanisława Majchera nr pf 136 z 11.08.1973 r. w sprawie egzaminów dyplomowych kadetów SCh WOP.

Jackiewicz Z., Wojska Ochrony Pogranicza 1945–*1991. Krótki informator historyczny*, Kętrzyn 1988.
Łach H., *System ochrony polskiej granicy państwowej w latach 1989*–2004, Olsztyn 2013.
Prochwicz J., Wojska Ochrony Pogranicza 1945–1965. Wybrane problemy, Piotrków Trybunalski 2001.

Summary

The Warrant Officers School of Border Troops in Kętrzyn was one of the three institutions to prepare professional staff for this formation, but the only one that prepared staff for various roles such as specialist or managerial positions. The article presents the

origin and organizational development of the Warrant Officers School of Border Troops in Kętrzyn. At this school, in the years 1970-1991, a few thousand professional soldiers for the protection of the Polish People's Republic state border were trained. The role of this institution was to train Warrant Officers. The organization's development of this institution, the process of teaching cadets, subjects taught and the results achieved in science will be discussed. The groups of candidates who wanted to join this school have been profiled.

Załącznik 1

Podział godzin w SCh WOP w roku 1972

Lp.	Wyszczególnienie	Liczba dni i godz. szkoleniowych
1.	**Dni kalendarzowe**	**335 (od 1 października 1972 r. do 31 sierpnia 1973 r.**
2.	**Z tego:**	
	– dni świątecznych	49
	– przygotowanie do nowego roku	3
	– ferie zimowe	10
	– ferie wiosenne	5
	– przygotowanie do promocji	5
	– egzamin dyplomowy	5
	– dni na naukę własną	27
	– dni dyspozycyjne i warty	10
	– inspekcje i kontrole	2
3.	**Razem dni pozaszkolnych**	**116**
4.	**Dni szkoleniowych**	**219, z tej liczby:**
5.	**170 dni po 7 godz.** **49 dni po 6 godz.**	**1190 godz. lekcyjnych** **294 godz. lekcyjne**
Ogółem godzin szkoleniowych		**1484**

Źródło: ASG w Szczecinie, Akta CS WOP, sygn. nr 1862, t. 106, Tymczasowy program szkolenia rocznej szkoły chorążych WOP (plutony operacyjno-kontrolerskie i plutony operacyjne), Kętrzyn 1972, s. 8.

Załącznik 2

Podział godzin nauki w SCh WOP w roku 1972 w plutonach operacyjno-kontrolerskim i operacyjnym

Lp.	Nazwa przedmiotu/profil szkolenia	Liczba godz. przeznaczonych na szkolenie	Odsetek godz. szkolenia
1.	**Szkolenie społ.-polit.**	135	**9,1**
2.	**Szkolenie specjalne**	692	**46,6**
3.	**Szkolenie graniczne**	90	**6,6**
4.	**Szkolenie techniczne (samochodowe)**	120	**8,1**
5.	**Maszynopisanie**	50	**3,4**
6.	**Język obcy (rosyjski, niemiecki)**	106	**7,1**
7.	**Regulaminy**	25	**1,7**
8.	**Musztra**	25	**1,7**
9.	**Wychowanie fizyczne**	75	**5,1**
10.	**Szkolenie ogniowe**	60	**4**
11.	**Szkolenie taktyczne**	55	**3,7**
12.	**Szkolenie innych rodzajów wojsk**	51	**3,4**
Ogółem godzin szkolenia		**1484**	**100**

Źródło: ASG w Szczecinie, Akta CS WOP, sygn. nr 1862, t. 106, Tymczasowy program szkolenia rocznej szkoły chorążych WOP (plutony operacyjno-kontrolerskie i plutony operacyjne), Kętrzyn 1972, s. 2.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 119–128 ROK 2017

ISSN 2543–7321

Andrzej Stec

Akademia Pomorska
Słupsk
stec75@wp.pl

POLSKA I UKRAINA NA TLE ZMIAN W UKŁADZIE GEOPOLITYCZNYM

POLAND AND UKRAINE AGAINST THE BACKGROUND OF CHANGES IN THE GEOPOLITICAL SYSTEM

***Zarys treści*:** Polskę i Ukrainę łączy przeszło tysiącletnie sąsiedztwo oparte na podobnych doświadczeniach oraz złożonej historii. Oba kraje z racji położenia geograficznego znalazły się na styku rywalizacji mocarstw, tj. Stanów Zjednoczonych i Chin, które chcą rozszerzyć swoje wpływy na państwa naszego regionu. Dużego znaczenia nabiera w tej sytuacji polityka Federacji Rosyjskiej, która dzięki potencjałowi obszarowemu uzyskuje możliwość rewizji ładu światowego i kwestionowania pozycji Stanów Zjednoczonych. Realizacja koncepcji chińskiego Nowego Jedwabnego Szlaku może doprowadzić do zasadniczego przewartościowania i podważenia koncepcji światowego systemu potęg morskich w drodze zmiany „architektury handlu", co będzie miało bezpośredni wpływ na bezpieczeństwo naszego regionu.

***Słowa kluczowe*:** Polska, Chiny, Ukraina, USA, geopolityka, geostrategia, bezpieczeństwo, Nowy Jedwabny Szlak

Key words: Poland, China, Ukraine, USA, geopolitics, geostrategy, security, the New Silk Road

Polskę i Ukrainę łączy przeszło tysiącletnie sąsiedztwo oparte na burzliwej i trudnej historii. Oba kraje przeszły przez rozbiory oraz objęły je procesy państwotwórcze w XX w., z tym że Ukrainie nie udało się wybić na niepodległość w dwudziestoleciu międzywojennym. Geopolityka to połączenie cech geograficznych naszej planety (np. surowców naturalnych) z działalnością człowieka (np. poprzez osiągnięcia technologiczne), zmieniające charakter (a także wartość) danego miejsca geograficznego w dłuższej perspektywie czasowej. Upraszczając znaczenie terminu

geopolityka, można zawęzić je do otoczenia (świata), w którym funkcjonuje na co dzień dane państwo[1]. Z geopolityki wynika z kolei geostrategia, która opisuje „gdzie i w jaki sposób podmiot polityczny (państwo) kieruje wysiłki wojskowe i dyplomatyczne w celu poprawienia swojej pozycji i optymalizacji własnego rozwoju, często kosztem innych"[2]. W związku z tym, że zasoby surowcowe są ograniczone, najsilniejsze mocarstwa muszą zdecydować, gdzie podejmować działania gospodarcze lub wojskowe, aby realizować swoją politykę zagraniczną. Ograniczenia mogą dotyczyć uwarunkowań geograficznych, takich jak: bariery naturalne (góry, morza i oceany), znaczne dystanse, zasoby surowcowe oraz potencjał rolniczy itp. Geostrategia, a właściwie jej komponent wojskowy i związana z nim projekcja siły wojskowej daleko od własnych baz, wskazuje na problem dystansu oraz uwarunkowań terenowych: gór, oceanów oraz brak dostępnych i dogodnych portów wojennych, jako czynników newralgicznych dla jej realizacji. Polska i Ukraina z racji swego położenia na styku rywalizacji mocarstw, tj. Stanów Zjednoczonych i Chin oraz pretendowania do tego grona Federacji Rosyjskiej, stały się krajami, które w przeszłości podlegały wpływowi doktryn słowianofilstwa i panslawizmu[3] a obecnie władze na Kremlu chętnie widziałyby „finlandyzację Ukrainy"[4] i zmarginalizowanie Polski w Unii Europejskiej. Imperialistyczne zakusy Federacji Rosyjskiej (FR) spowodowały, że Ukraina w 2016 r. znalazła się na skraju zapaści społeczno-ekonomicznej i finansowej. Pomimo aktywnej postawy polskiej dyplomacji, którą można określić mianem „adwokata Ukrainy" oraz poparcia dyplomatycznego, propagandowego i moralnego ze strony krajów UE i USA, w 2017 r. widoczne są już oznaki „zmęczenia" społeczeństw zachodnich wspomnianą problematyką oraz ograniczenia pomocy finansowej i wojskowej (wyposażenie nieśmiercionośne, doradcy woskowi itp.).

Kraje Unii Europejskiej i USA stosują presję ekonomiczną na FR, ta zaś wobec Ukrainy ograniczoną interwencję zbrojną. Dla Unii Europejskiej Polska i Ukraina liczą się przede wszystkim jako rynek zbytu i „kordon bezpieczeństwa". Z kolei Stany Zjednoczone zajmują postawę dość dwuznaczną względem Ukrainy. O ile amerykański Kongres i wysocy rangą wojskowi głośno domagają się rozpoczęcia dostaw broni do tego kraju, o tyle otoczenie prezydenta Baracka Obamy i Donalda Trumpa zachowuje się w tej materii dość – mówiąc oględnie – „powściągliwie", przedkładając rozwiązania dyplomatyczne i powrót do polityki „resetu"[5] z Moskwą. Wszystkie zainteresowane ośrodki siły wiedzą jednak, że Rosja nie „odpuści" Ukra-

[1] Zob. szerzej: J. Grygiel, Great Powers and Geopolitical Change, Baltimore 2006, s. 24.

[2] J. Bartosiak, Pacyfik i Eurazja. O wojnie, Warszawa 2016, s. 38.

[3] Zob. szerzej: L. Moczulski, *Geopolityka. Potęga w czasie i przestrzeni*, Warszawa 2000, s. 505––507.

[4] Finlandyzacja (fiń. Suomettuminen) – ograniczenie przez obce mocarstwo (dawniej Związek Socjalistycznych Republik Radzieckich a obecnie Federację Rosyjską) swobody polityki zagranicznej innego państwa w zamian za rzekomy brak interwencji w politykę wewnętrzną. Przejawiała się ona w ścisłych związkach gospodarczych oraz rosyjskich próbach interwencji w wewnętrzne sprawy Finlandii, dotyczące np. obsady wysokich stanowisk w tym kraju, oraz na niedrażnieniu Moskwy, a czasami wręcz wychodzeniu naprzeciw jej zamiarom.

[5] Por. M. Kaczmarski, *Kruchy „reset". Bilans i perspektywy prze*mian w relacjach rosyjsko-*-amerykańskich*, Warszawa 2011, s. 7–25.

iny i będzie destabilizować życie tego kraju, a państwa zachodnie nie stoczą wojny nuklearnej z Moskwą ani nie wywołają w Rosji stanu anarchii z wszelkimi konsekwencjami globalnymi[6]. Jeśli dotychczasowy przebieg konfliktu krymskiego i donbaskiego nie wywołały już nowej zimnej wojny ani też nie doprowadziły do liczącej się rekonfiguracji sytuacji geopolitycznej w regionie Międzymorza[7] – poruszamy się w sferze konkretnych faktów, nie zaś retoryki dyplomatycznej czy spektakularnych manifestacji wojskowych – to tym bardziej nie należy spodziewać się, aby politycy Zachodu pragnęli „umierać" za Sewastopol, Donieck, Kijów, Wilno czy Warszawę.

W związku z inicjatywą Nowego Jedwabnego Szlaku władze Chin chcą rozszerzyć swe wpływy polityczno-ekonomiczno-wojskowe na państwa naszego regionu. Projekt ten ma istotne znaczenie zarówno dla Ukrainy, jak i Polski, gdyż ekspansja chińska w Europie ma przebiegać z pominięciem tradycyjnych morskich szlaków komunikacyjnych, kontrolowanych przez USA. Gdyby inicjatywa ta została zrealizowana, to nasze kraje mogłyby znacząco rozwinąć się gospodarczo, co jest nie na rękę Federacji Rosyjskiej, która przypomina nieco Związek Radziecki tuż przed upadkiem[8], w sytuacji, gdy mamy moment zwrotny w dotychczasowym ładzie międzynarodowym[9]. W związku z powyższym dyplomacja rosyjska jest w stanie iść na duże ustępstwa wobec Chin w celu uzyskania doraźnych korzyści, choć kosztem własnego bezpieczeństwa[10]. Wymieniając podstawowe akty normatywne kształtują-

[6] Zarówno działania dyplomacji amerykańskiej oparte na założeniu, że FR jest zbyt słaba, aby wytrzymać długofalowy konflikt polityczno-wojskowy, co mogłoby rodzić chaos w szerokim wymiarze, jak i działania dyplomacji niemieckiej, dążącej za wszelką cenę do współpracy z Rosją opartej na zasadzie „po pierwsze Rosja", zmierzają do akceptacji agresji i okrucieństwa jako podstaw polityki FR względem sąsiadów. Gdy doda się do tego szeroko promowaną w rosyjskich mediach dezinformację, mówiącą o tym, iż FR otaczają zewsząd niebezpieczeństwa, wrogowie, a inne kraje przygotowują się do wojny z nią – to widzimy mit, powtarzany już od czasów carskich. Zob. szerzej: Є. Добровольський, *Сусіди*, Тернопіль, 2015, s. 186–187.

[7] Międzymorze – idea polityczna wysuwana przez Józefa Piłsudskiego, zakładająca utworzenie federacji państw Europy Środkowej i Wschodniej. Docelowo do Międzymorza należeć miał obszar między morzami Adriatyckim, Bałtyckim a Czarnym („Morza ABC"), a konkretnie Polska, Litwa, Łotwa, Estonia, Białoruś, Ukraina, Czechosłowacja, Węgry, Rumunia, Jugosławia oraz ewentualnie Finlandia, w celu stworzenia sił mogących stawić opór zarówno Niemcom, jak i Rosji. W ciągu dwóch dekad od porażki idei Międzymorza wszystkie państwa mające być członkami federacji znalazły się w strefie wpływów ZSRR lub III Rzeszy.

[8] Oficjalnie ok. 4,7% PKB FR przeznaczonych jest na wojsko (nieoficjalnie znacznie więcej, przyp. autor) a udział w światowym handlu bronią wynosi 23%, SIPRI, TRENDS IN INTERNATIONAL ARMS TRANSFERS, 2016, s. 1–3; www.sipri.org/sites/default/files/Trends-in-international-arms-transfers-2016.pdf (dostęp: 28.02.2017).

[9] System światowy utrzymywany przez potęgę wojskową USA wciąż obowiązuje, ale słabnie i jego przetrwanie nie jest pewne. Pauza geopolityczna, zwana jednobiegunową chwilą, trwająca od zakończenia zimnej wojny, właśnie się skończyła. Kluczowe elementy składające się na fundamenty systemu są kwestionowane, w szczególności: zdolność Stanów Zjednoczonych do swobodnej projekcji siły na morzach i oceanach oraz w strefie przybrzeżnej Eurazji (Rimland), siła i dynamika ekonomiczna Stanów Zjednoczonych oraz dominacja gospodarcza Ameryki w świecie w obliczu rosnącej potęgi gospodarczej Chin i kluczowego miejsca Chin w globalnej gospodarce. J. Bartosiak, Pacyfik i Eurazja…, s. 21.

[10] Rosja przerzuciła znaczną liczbę wojska ze swych wschodnich granic w pobliże Ukrainy. Nastąpił także przełom we współpracy energetycznej w postaci zgody na budowę odnogi ropocią-

ce rosyjską strategię bezpieczeństwa narodowego, należy uwzględnić: konstytucję, ustawy o bezpieczeństwie z lat 1992 i 2010, koncepcje bezpieczeństwa narodowego z lat 1997 i 2001[11], strategię bezpieczeństwa narodowego Federacji Rosyjskiej do 2020 r. z 12 maja 2009 r. oraz dwa strategiczne dokumenty Federacji Rosyjskiej z przełomu 2015/16 r., które już weszły w życie: jawną strategię bezpieczeństwa narodowego oraz tajny plan obrony do roku 2020.

Normy zawarte w wyżej wymienionych aktach prawnych odzwierciedlają pogorszenie relacji Rosji z Zachodem, które nastąpiło po aneksji Krymu i wojnie w Donbasie, jak również interwencji rosyjskiej w Syrii. Dokumenty te identyfikują USA, Polskę oraz inne kraje Sojuszu Północnoatlantyckiego jako główne zagrożenie. Euroatlantyckie aspiracje Ukrainy z kolei stanowią pośrednie zagrożenie. Wyraźny jest język otwartej konfrontacji, natomiast rozszerzenie NATO o Ukrainę[12] oraz budowa tarczy antyrakietowej (z jej elementami w Polsce) są dla Federacji Rosyjskiej nie do zaakceptowania. Należy zwrócić uwagę, iż coraz częściej w rosyjskich dokumentach definiuje się „zagrożenie" jako groźbę wybuchu konfliktu, a nie tylko obawę przed taką możliwością. Z tego wynika, iż Rosja przygotowuje się na dłuższy czas bardzo złych relacji z Zachodem. Nie można wykluczyć pełnej agresji na Ukrainę oraz zagrożenia dla państw bałtyckich i – w dalszej kolejności – Polski. W sytuacji dotarcia wojsk FR do brzegów Dniepru nastąpiłby masowy odpływ kapitału zachodniego z Polski i krajów bałtyckich (Estonii, Litwy i Łotwy). Gwarancją bezpieczeństwa byłaby stała obecność sił amerykańskich w zagrożonych państwach w wymiarze pięciokrotnie większym od zakładanego na początku 2017 r. w naszym regionie.

Na przełomie 2016 i 2017 r. Federacja Rosyjska bez wątpienia znalazła się w sytuacji kryzysowej – zarówno w obszarze gospodarczym, jak i bezpieczeństwa. Kryzys gospodarczy wynika ze zjawisk w dużym stopniu niezależnych od Rosji (np. spadek cen ropy i gazu stanowiących 65% eksportu) lub będących skutkiem wcześniejszej polityki Kremla i mających charakter głęboko systemowy (niewydolność wynikająca z przyjętego modelu funkcjonowania gospodarki oraz zbyt duże nakłady na wojsko, tj. 9% budżetu).[13] Jeśli chodzi o polityczny aspekt sytuacji kryzysowej,

---

gu Wschodnia Syberia–Ocean Spokojny do Chin i akceptacja kredytów chińskich na 25 mld USD. Chiny stały się kluczowym partnerem w rozwoju rosyjskiego Dalekiego Wschodu (program zaakceptowano w 2009 r.). Rosja zdecydowała się także na zaostrzenie relacji z Japonią (która jest potencjalnym partnerem w hamowaniu wzrostu Chin), eskalując spór terytorialny o Wyspy Kurylskie w momencie podobnych napięć między Pekinem a Tokio. Również postawa Moskwy w kryzysie koreańskim, taka sama jak podejście chińskie, demonstruje brak gotowości do zacieśnienia relacji z Koreą Południową. M. Kaczmarski, *Kruchy „reset"…*, s. 25.

[11] Zob. szerzej: T. Dmochowski, *Koncepcje bezpieczeństwa narodowego Federacji Rosyjskiej* 1997–2000, „Cywilizacja i Polityka" 2008, nr 6, s. 158–177.

[12] W Rosji nadal pokutuje mit, iż imperialność tego kraju bez kontroli nad Ukrainą byłaby nie w pełni wartościowa. Większość Rosjan uznaje Ukraińców nie za odrębny naród, lecz tzw. bratni naród. W podobnym tonie wypowiada się także kremlowska propaganda, propagując „federalizację Ukrainy", wspólne życie „dwóch bratnich narodów", z czego Rosjanie to ten rzekomo starszy brat – choć w rzeczywistości jest odwrotnie. Zob. szerzej: Є. Добровольський, *Cyciди*, Тернопіль, 2015, s. 178.

[13] Zob. szerzej: Raport Akademii Europejskiej Krzyżowa – Kryzys finansowy Rosji i gospodarka Zachodu, http://akademia.krzyzowa.org.pl/index.php?option=com_content&view=article&id=87&catid=12&Itemid=211&lang=pl (dostęp: 28.02.2017).

to jest on w dużym stopniu efektem świadomej i zarazem autorytarnej polityki Kremla. Polega ona na kreowaniu kolejnych kryzysów zewnętrznych, ognisk napięć czy wręcz na agresji (Gruzja, Ukraina, Naddniestrze i in.) Niewątpliwie ułatwia to utrzymywanie ostrego reżimu w kraju i umacnia pozycję przywódcy, jednocześnie utrudniając innym podmiotom międzynarodowym zorganizowaną i długofalową reakcję na „awanturniczą" politykę Moskwy. Należy jednak zauważyć, iż niezadowolenie społeczne rośnie w stopniu większym niż ten, który Kreml może łatwo kontrolować[14], natomiast formuła stawiania się w opozycji do Zachodu, co ma utrwalać jedność społeczeństwa, w końcu ulegnie wyczerpaniu. W związku z powyższymi kwestiami jawi się przed polską i ukraińską dyplomacją problem obalenia mitów masowo kolportowanych przez rosyjską dyplomację:

1. Ukazywania obrazu FR jako państwa otoczonego przez wrogów, stawiającego opór agresywnym krajom zachodnim, którym nie podoba się, że Moskwa prowadzi „niezależną i autonomiczną politykę zagraniczną"[15];
2. Rzekomego naruszania praw ludności rosyjskojęzycznej;
3. „Naruszania norm prawa międzynarodowego" poprzez intensyfikację aktywności militarnej NATO;
4. Ukazywania Zachodu (zwłaszcza USA) jako wyznawcy archaicznego poglądu na świat, czego dowodem ma być powtarzanie stereotypów zimnowojennych i dążenie do globalnej hegemonii;
5. Oskarżeń o organizację przez USA i UE „antykonstytucyjnego puczu" („przewrotu") na Ukrainie.

Powyższe mity mogą powstawać jedynie w kraju rządzonym autorytarnie dla zakamuflowania agresji wojskowej i innych działań destrukcyjnych, mających na celu zniewolenie krajów sąsiednich poprzez zajęcie kolejnych terenów. Takie kroki zmierzają do budowy kolejnego „mocarstwa na glinianych nogach", a dokładniej „kleptokracji z ładunkami atomowymi"[16]. W związku z powyższym nie można wykluczyć konfrontacji zbrojnej, na co wskazuje wysoki stopień gotowości bojowej armii, lotnictwa i floty FR. Konfrontacja ta może przybrać postać pełnego bądź ograniczonego w skali ataku, ale nie na Sojusz Północnoatlantycki jako całość, lecz np. na państwa bałtyckie bądź inne kraje sąsiednie, przy zaangażowaniu ludności rosyjskojęzycznej bądź wiernych wyznających prawosławie (projekt odbudowy państwowości rosyjskiej w granicach dawnego ZSRR, być może z wyłączeniem państw bałtyckich, lub też obejmujący jedynie Rosję, Białoruś i Ukrainę)[17].

Prezydent Federacji Rosyjskiej, wzorując się na największych dyktatorach XX w. (Hitlerze i Stalinie), skorzystał na Ukrainie z doświadczeń szefa propagandy 1. Rosyjskiej Armii Narodowej a następnie oficera wydziału propagandowego „Po-

[14] Zob. szerzej: K. Czerniewicz, *Konfrontacji ciąg dalszy. Co mówi rosyjska strategia bezpieczeństwa*, Ośrodek Analiz Strategicznych, https://oaspl.org/2016/02/16/konfrontacji-ciag-dalszy-co-mowi-rosyjska-strategia-bezpieczenstwa/ (dostęp: 28.02.2017).

[15] Tamże, s. 2.

[16] Zob. szerzej: C. Dawisha, *Putin's Klept*ocracy. Who Owns Russia, New York 2015, s. 104–317.

[17] Zob. szerzej: M. Menkiszak, Doktryna Putina: Tworzenie koncepcyjnych podstaw rosyjskiej dominacji na obszarze postradzieckim, Ośrodek Studiów Wschodnich im. M. Karpia, www.osw.waw.pl/pl (dostęp: 28.02.2017).

łudniowy Wschód" Wermachtu, Jewgienija Messnera. Ten teoretyk wojskowości, szczególnie lubiany przez głowę państwa rosyjskiego, opisywał i analizował konflikt zbrojny nowego typu, który opierał się na takich formach walki, jak globalny terroryzm, ruch powstańczy czy też partyzantka ludowa. Korzystając z teorii Messnera, władze kremlowskie po anschlussie Krymu rozpoczęły drugi etap wojny, który można określić jako „wojnę chaosu", składającą się z takich elementów, jak: wojna bez wojska (np. w mediach), wojna bez stałej linii frontu (ataki w różnych miejscach), wojna dyskretna i ekonomiczna, która toczyła się faktycznie od paru lat, przy dużym udziale służb specjalnych FR, na wielu płaszczyznach jednocześnie. Rozpoczęła się na szeroką skalę na terenie Europy walka dezinformacyjna, której kontynuacją było tworzenie spontanicznych, lokalnych grup separatystycznych mających na celu paraliż ośrodków władzy i niedoceniane do tej pory oddziaływanie psychologiczne.

Objawy podobnych zjawisk w postaci wrogich działań o podłożu celnym[18] oraz cyberataki[19] można zaobserwować także w relacjach Federacji Rosyjskiej z Polską, co stwarza realne zagrożenie dla sprawnego funkcjonowania państwa[20]. Trudno jest uważać władze na Kremlu za poważnego partnera zarówno w sprawach gospodarczych, jak i wojskowych, gdyż zarówno przy zawarciu tzw. porozumień z Mińska I (12.02.2014 r.), jak i tzw. porozumień z Mińska II (zawartych w nocy z 19 na 20.09.2015 r.), nie dotrzymywały one zawartych w nich ustaleń, mając na celu jedynie utrzymanie status quo, zajęcie kolejnych terenów Ukrainy, udawanie, że nie ma agresji rosyjskiej na terytorium Ukrainy a Krym już jest rosyjski, jednocześnie prowadząc regularną wojnę gospodarczą na ceny ropy i gazu oraz informacyjną i propagandową[21]. Systematyczne naruszanie przez FR swoich zobowiązań gospodarczych i wojskowych podważa stabilność globalnego systemu bezpieczeństwa, jak też stanowi dowód, że nie można ufać żadnym obietnicom ani zobowiązaniom rosyjskich władz. W działaniach Rosji (która używa potencjału surowcowego, obszarowego czy nawet atomowego)[22] widać realizację projektu strefy poradzieckiej nawet w postaci rozwiązań siłowych, co stwarza realne zagrożenie dla suwerenności i integralności Polski oraz Ukrainy.

Realizacja koncepcji chińskiego Nowego Jedwabnego Szlaku może doprowadzić do zasadniczego przewartościowania i podważenia koncepcji światowego systemu

[18] Zob. także: M. Kowalewski, Polsko-rosyjska wojna handlowa, „Wprost" 2016, nr 7, s. 4–5, www.wprost.pl/tylko-u-nas/532030/Polsko-rosyjska-wojna-handlowa-Przy-granicy-traca-wszyscy.html (dostęp: 28.02.2017).

[19] J. Grubicka, *Polityka cyberbezpieczeństwa Polski wobec kryzysu ukraińskiego*, [w:] Bezpieczeństwo państw Europy Środkowo-Wschodniej w kontekście konfliktu na Ukrainie, red. T. Pączek, Słupsk 2016, s. 273–290. Zob. także, S. Krawiec, Kobieta od cyberroboty, „Wprost" 2016, nr 7, s. 40–42.

[20] E. Żemła, *Batalia o bezpieczeństwo*, „Wprost" 2016, nr 7, s. 17–19.

[21] O odpowiedzialności państwa za działania zabronione zob. szerzej: M. Balcerzak, Odpowie*dzialność międzynarodowa państwa za działania zabronione a systemowy charakter prawa mię*dzynarodowego, [w:] *Państwo a prawo międzynarodowe jako system prawa*, red. R. Kwiecień, Lublin 2015, s. 319–335.

[22] C. Marcinkowski, Hybrydowy charakter konfliktu zbrojnego na Ukrainie (2014–2015). Implikacje dla przy*szłości*, [w:] *Bezpieczeństwo państw Europy Środkowo*-Wschod*niej…*, s. 61–70.

potęg morskich w drodze zmiany „architektury handlu". Wraz ze wzrostem potęgi Chin władze FR (dzięki potencjałowi obszarowemu) uzyskają kolejną możliwość rewizji ładu światowego i kwestionowania pozycji Waszyngtonu w Eurazji, co będzie miało wpływ na stan bezpieczeństwa nie tylko Polski i Ukrainy, lecz także regionu Europy Środkowo-Wschodniej, położonej na granicy skutecznej projekcji siły wojskowej Stanów Zjednoczonych, a także znaczący wpływ na architekturę bezpieczeństwa w Europie[23].

Wnioski

W związku ze swym centralnym położeniem oraz więzami historycznymi zarówno Polska, jak i Ukraina powinny odgrywać ważną rolę jako pomost pomiędzy Wschodem i Zachodem. Pozycja i współpraca są kształtowane przez: położenie geograficzne, potencjał demograficzny, gospodarczy oraz silnie w ostatnim czasie rozbudowane społeczeństwo obywatelskie (ruch „Solidarności" w Polsce i wydarzenia „pomarańczowej rewolucji" oraz „Majdanu" na Ukrainie), zdolne do rozstrzygających aktów politycznych, nawet kosztem własnej krwi. „Ukraina jest też jedynym państwem, którego decyzja – obranie wschodniego lub zachodniego wektora dalszego rozwoju – jest w stanie zmienić generalne geopolityczne położenie Polski. Postawa Ukrainy zarówno rozstrzygnie o pozycji Rosji w Europie Wschodniej, jak i w razie obioru przez Kijów wektora zachodniego, przesądzi o losie Mołdawii. Jest wysoce prawdopodobne, że będzie miała znaczenie także dla rozwoju sytuacji na Białorusi i w basenie Morza Czarnego, a zatem wpłynie też na rozwój wydarzeń na Kaukazie. Nie istnieje ponadto obecnie żadna istotna sprzeczność interesów narodowych Polski i Ukrainy"[24].

Ukraina jest według Zbigniewa Brzezińskiego państwem sworzniem[25], który jeśli zespoli Polskę, Rumunię i Węgry, to powstanie siła mogąca stawić opór zarówno Federacji Rosyjskiej, jak i Republice Federalnej Niemiec. Ważnym jest, aby spory o historię pomiędzy dwoma sąsiednimi narodami nie położyły się cieniem na przyszłych stosunkach między oboma państwami.

Za wysoce niestosowne opinia publiczna Zachodniej i Centralnej Ukrainy uważa podnoszenie stereotypów historycznych w sytuacji, gdy Ukraina walczy z agresją rosyjską o swój suwerenny byt. Jest to problem, którym powinni zająć się wyspecjalizowani historycy a nie politycy, gdyż daje to spore pole manewru służbom specjalny Federacji Rosyjskiej w celu skłócenia władz państw sąsiednich[26] (choćby przez

[23] J. Bartosiak, Pacyfik i Eurazja…, s. 572.

[24] P. Żurawski vel Grajewski, Polska polityka wschodnia 1989–2015, wymiar narodowy i unijny, Kraków 2016, s. 115.

[25] Termin państwa sworznia (pivotal states) oznacza państwa, których znaczenie geopolityczne przekracza ich potencjał, i których los wpływa na zachowanie graczy mocarstwowych. Z. Brzeziński, Wielka szachownica, Warszawa 1998, s. 41.

[26] W Polsce dużą wagę przywiązuje się do uczestnictwa w Pakcie Północnoatlantyckim, który jednak nie rozwiąże ani wszystkich, ani większości problemów bezpieczeństwa. Stosunki dobrosąsiedzkie zaś mogą w niektórych sytuacjach przechylić szalę zwycięstwa, np. pomoc węgierska

dewastacje cmentarzy mniejszości w Polsce i na Ukrainie, które już miały miejsce). Używanie nieadekwatnych słów oraz obrazów filmowych może doprowadzić do powstania mitów, których przezwyciężenie zajmie kolejne dziesiątki lat. Pamiętać także należy, iż Ukraina jest krajem o wiele bardziej zróżnicowanym pod względem religijnym, językowym i kulturowym niż Polska oraz jest na etapie budowania własnej tożsamości narodowej. Należy więc dbać o wzajemne stosunki polityczne, gospodarcze, samorządowe w myśl zasady, że wrogów szuka się daleko a przyjaciół blisko oraz szukać tego co łączy a nie dzieli!

Bibliografia

Balcerzak M., *Odpowiedzialność międzynarodowa państwa za działania zabronione a systemowy charakter prawa międzynarodowego*, [w:] *Państwo a prawo międzyn*arodowe jako system prawa, red. R. Kwiecień, Lublin 2015.

Bartosiak J., Pacyfik i Eurazja. O wojnie, Warszawa 2016.

Brzeziński Z., Wielka szachownica, Warszawa 1998.

Dawisha C., *Putin's Kleptocracy. Who Owns Russia*, New York 2015.

Добровольський Є., *Сусіди*, Тернопіль 2015.

Dmochowski T., Koncepcje bezpieczeństwa *narodowego Federacji Rosyjskiej 1997–*–2000, „Cywilizacja i Polityka" 2008, nr 6.

Grubicka J., *Polityka cyberbezpieczeństwa Polski wobec kryzysu ukraińskiego*, [w:] Bezpieczeństwo państw Europy Środkowo-Wschodniej w kontekście konfliktu na Ukrainie, red. T. Pączek, Słupsk 2016.

Grygiel J., Great Powers and Geopolitical Change, Baltimore 2006.

Kaczmarski M., *Kruchy „reset". Bilans i perspektywy przemian w relacjach rosyjsko-amerykańskich*, Warszawa 2011.

Kowalewski M., Polsko-rosyjska wojna handlowa, „Wprost" 2016, nr 7.

Krawiec S., Kobieta od cyberroboty, „Wprost"2016, nr 7.

Kupiecki R., *Organizacja Traktatu Północnoatlantyckiego*, Warszawa 2016.

Marcinkowski C., Hybrydowy charakter konfliktu zbrojnego na Ukrainie (2014–2015). *Implikacje dla przyszłości*, [w:] *Bezpieczeństwo państw Europy Środkowo*-Wschodniej *w kontekście konfliktu na Ukrainie*, red. T. Pączek, Słupsk 2016.

Moczulski L., *Geopolityka. Potęga w czasie i przestrzeni*, Warszawa 2000.

Żemła E., *Batalia o bezpieczeństwo*, „Wprost" 2016, nr 7.

Żurawski vel Grajewski P., Polska polityka wschodnia 1989–2015, Kraków 2016.

Czerniewicz K., *Konfrontacji ciąg dalszy. Co mówi rosyjska strategia bezpieczeństwa*, Ośrodek Analiz Strategicznych, https://oaspl.org/2016/02/16/konfrontacji-ciag-dalszy-co-mowi-rosyjska-strategia-bezpieczenstwa/ (dostęp: 28.02.2017).

w postaci dostaw broni i amunicji w wojnie polsko-bolszewickiej 1920 r. Należy w tym miejscu rozważyć analizę sojuszy, której dokonał Robert Kupiecki: „Na przestrzeni ostatnich 400 lat trzy czwarte zawieranych sojuszy nie zostało dotrzymanych, a w co dziesiątym sojusznik wystąpił przeciwko sojusznikowi". R. Kupiecki, *Organizacja Traktatu Półn*ocnoatlantyckiego, Warszawa 2016, s. 14.

Menkiszak M., Doktryna Putina: Tworzenie koncepcyjnych podstaw rosyjskiej dominacji na obszarze postradzieckim, Ośrodek Studiów Wschodnich im. M. Karpia, www.osw.waw.pl/pl (dostęp: 28.02.2017).

Raport Akademii Europejskiej Krzyżowa – Kryzys finansowy Rosji i gospodarka Zachodu,http://akademia.krzyzowa.org.pl/index.php?option=com_content&view=article&id=87&catid=12&Itemid=211&lang=pl (dostęp: 28.02.2017).

Raport SIPRI, TRENDS IN INTERNATIONAL ARMS TRANSFERS, 2016, https://www.sipri.org/sites/default/files/Trends-in-international-arms-transfers-2016.pdf (dostęp: 28.02.2017).

Summary

Poland and Ukraine have been joined over millennia based on similar experiences and a complex history. Both countries, due to their geographical location, have found themselves at the crossroads of great-power rivalry. The United States and China both want to expand their influence in the region. An important role in this situation is the policy of the Russian Federation which, thanks to the area's potential, has the opportunity to revise global governance and challenge the position of the United States. Implementation of the concept of the New Chinese Silk Road may lead to a fundamental reevaluation and undermine the concept of a global system of maritime powers, by amending the "trade architecture", which will have a direct impact on the security of the region.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 129–142 ROK 2017

ISSN 2543–7321

Ewa Matuska

Akademia Pomorska
Słupsk
ewa.matuska@apsl.edu.pl

ZAGROŻENIA PSYCHOSPOŁECZNE ZWIĄZANE Z PRACĄ

PSYCHOSOCIAL HAZARDS RELATED TO WORK

***Zarys treści*:** Artykuł omawia temat zagrożeń psychospołecznych związanych z pracą w kontekście polityki bezpieczeństwa i higieny pracy oraz efektywności pracy. Ujmuje ramy pojęciowe ryzyk psychospołecznych i ich wymiary w funkcjonowaniu współczesnych organizacji. Analizuje dominujące zagrożenia psychospołeczne w odniesieniu do Polski na podstawie wyników badań Europejskiej Agencji Zdrowia i Bezpieczeństwa w Pracy, ESENER-1 i ESENER-2. We wnioskach przedstawia postulat włączenia ewaluacji ryzyk psychospołecznych w przedsiębiorstwach do procedur stosowanych przez służby BHP.

***Słowa kluczowe*:** zagrożenia psychospołeczne w pracy, bezpieczeństwo i higiena pracy, stres organizacyjny, efektywność pracy

Key words: psychosocial work hazards, safety and hygiene at work, organizational stress, work efficiency

Wprowadzenie

Bezpieczeństwo pracy i ochrona zdrowia pracowników zajmują istotne miejsce w polityce społecznej Polski, a od 2004 r. podlegają także legislacyjnym regulacjom Unii Europejskiej. Kodeks pracy w art. 94 specyfikuje, że „Pracodawca jest obowiązany w szczególności […] zapewniać bezpieczne i higieniczne warunki pracy oraz prowadzić systematyczne szkolenie pracowników w zakresie bezpieczeństwa i higieny pracy […] organizować pracę w sposób zapewniający zmniejszenie uciążliwości pracy, zwłaszcza pracy monotonnej i pracy w ustalonym z góry tempie" oraz „jest obowiązany przeciwdziałać mobbingowi"[1]. Ochrona zdrowia w miejscu pracy w prawie unijnym opiera się głównie na zapisach Jednolitego Aktu Europejskiego z 1986 r., który uruchomił szereg dyrektyw socjalnych, w tym dyrektywę ramową

[1] Tekst jednolity: Dz.U. 2016, poz. 1666, z późn. zm.

dotyczącą bezpieczeństwa i ochrony zdrowia w miejscu pracy (89/391/EWG), nakazującą pracodawcom respektowanie godnych warunków pracy jako jednego z najważniejszych praw robotniczych[2]. Ta sama dyrektywa zobowiązuje pracodawców do wprowadzania środków zapobiegawczych chroniących pracowników przed wypadkami przy pracy i chorobami zawodowymi. Zgodnie z art. 151 Traktatu o funkcjonowaniu Unii Europejskiej, państwa członkowskie powinny aktywnie działać na rzecz promowania zatrudnienia i poprawy warunków pracy. Egzekwowanie od pracodawców konkretnych działań na rzecz tworzenia bezpiecznych warunków pracy, w zgodzie ze standardami obowiązującymi w krajach Europy zachodniej, jest jednak problematyczne.

Wymóg poddania się regulacjom prawnym i instytucjonalnym Unii Europejskiej w zakresie bezpieczeństwa i higieny pracy umożliwia natomiast stosowanie jednolitej metodologii badawczej i tym samym poszerza możliwość aplikacji wniosków uzyskanych z przeprowadzanych porównawczych badań naukowych. Europejska Agencja Zdrowia i Bezpieczeństwa w Pracy (European Agency for Safety and Health at Work, w skrócie: EU-OSHA)[3] prowadzi cykliczne badania w zakresie znanych i nowo pojawiających się zagrożeń związanych z pracą (job related hazards). Wynikiem tych badań jest klasyfikowanie i segmentacja różnych czynników ryzyka zawodowego oraz porównywanie wskaźników bezpieczeństwa pracy osiąganych w danym okresie przez poszczególne kraje Wspólnoty. Polska jest obecna w tych badaniach od ponad dziesięciu lat, co stanowi czas wystarczający do wnioskowania o status quo polskiego bezpieczeństwa pracy oraz o trendach w tym obszarze. Przedmiotem badań EU-OSHA są również tzw. *psychospołeczne zagrożenia w pracy*, które stanowią coraz baczniej obserwowaną sferę czynników ryzyka zawodowego[4].

Pojęcie psychospołecznych zagrożeń w pracy

Za zagrożenie dla człowieka, szeroko rzecz ujmując, można uznać każde zjawisko, sytuację, czynnik, które prawdopodobnie jest w stanie spowodować istotną dla niego szkodę[5]. Kryterium natury spodziewanej szkody wyznacza ogólny podział zagrożeń na:

- *zagrożenia fizyczne* (biologiczne, mechaniczne, chemiczne, radiologiczne) – oddziałujące bezpośrednio na jednostkę i generujące szkodę natury fizycznej oraz
- *zagrożenia psychospołeczne* – oddziałujące pośrednio, za pośrednictwem stresu psychologicznego i naruszające dobrostan psychiczny i społeczny jednostki, a w długiej perspektywie mogące również przynieść szkody psychosomatyczne i fizyczne.

[2] L. Vogel, Dyrektywa ramowa – *istotny element wdrażania skutecznej strategii zapobiegania wy*padkom przy pracy, „Bezpieczeństwo Pracy" 2002, nr 7/8.
[3] https://osha.europa.eu/pl (dostęp: 10.02.2017).
[4] M. Widerszal-Bazyl, *Pojęcie ryzyka psychospołecznego w pracy*, „Bezpieczeństwo Pracy" 2009, nr 6.
[5] T. Cox, A. Griffiths, S. Leka, Work organization and work-related stress, [w:] Occupational hygiene, red. K. Gardiner, J.M. Harrington, Oxford 2005, s. 421–432.

W kilku ostatnich dekadach obserwujemy istotne zmiany zarówno w zakresie profilu i organizacji pracy, jak i metod zarządzania jej procesami. W obecnej postindustrialnej fazie rozwoju ekonomicznego i w tzw. gospodarce opartej na wiedzy zmienił się przede wszystkim charakter pracy i warunki jej wykonywania. Coraz mniej osób zatrudnionych jest tradycyjnych sektorach, jak przemysł czy rolnictwo, gdzie praca, głównie fizyczna, wykonywana bywa na ogół w trudnych warunkach środowiskowych i związana jest z wieloma zagrożeniami fizykochemicznymi. Obecnie miejsca pracy tworzone są głównie w sektorze usług na rzecz przedsiębiorstw i instytucji (B2B, B2C[6]) oraz usług społecznych i osobistych. Jest to praca wysoce przetworzona, oparta na aktywności umysłowej, wymaga intensywnych kontaktów interpersonalnych, często przebiega w środowisku wielokulturowym. Zmiana modelu pracy wynika także z wpływu współczesnych zjawisk makroekonomicznych i politycznych, takich jak: globalizacja, zmiana wzorców zachowań konsumenckich, starzenie się siły roboczej, narastająca mobilność zasobów pracy, zasilana napływem imigrantów i uchodźców z regionów objętych konfliktami politycznymi etc. Wszystkie te zjawiska stały się źródłem nowych zagrożeń i ryzyk związanych z pracą i tym samym wyznaczyły nowe pola w badaniach szeroko pojętych zagadnień bezpieczeństwa i higieny pracy[7]. W spektrum nowych zagrożeń związanych z pracą ryzyka psychospołeczne postrzegane są obecnie jako jedno z kluczowych wyzwań dla praktyki zarządzania zasobami ludzkimi i utrzymania zadowalającej efektywności organizacji.

Po pierwsze, zagrożenia psychospołeczne w pracy stanowią ryzyko dla zdrowia pracownika, zarówno psychicznego, jak i fizycznego, poprzez pośredniczące działanie mechanizmu stresu organizacyjnego[8]. Stres związany z pracą (work-related stress) w raportach badawczych i dokumentach instytucji Unii Europejskiej definiowany jest jako „stan, któremu towarzyszą fizyczne, psychologiczne lub społeczne dolegliwości lub dysfunkcje sprawiające, że jednostka odczuwa, iż nie jest w stanie sprostać wymogom lub oczekiwaniom na nią nakładanym”[9]. Po drugie, ryzyka psychospołeczne pracy implikują wysoce prawdopodobne niekorzystne skutki dla rynkowej kondycji i konkurencyjności organizacji; nieobecności pracowników korzystających ze zwolnień lekarskich powodują spadek obrotów i tym samym produktywności, obniżone morale i brak zaangażowania często są związane z niepewnością zatrudnienia, przemocą, mobbingiem, niskopłatnymi umowami o pracę czy z presją na osiąganie wyśrubowanych wyników[10].

Systematyczne badania psychospołecznych aspektów pracy, prowadzone w ramach takich dyscyplin, jak psychologia pracy i środowisko pracy, sięgają lat pięć-

[6] B2B (Business to Business) – usługi dla firm; B2C (Business to Consumer) – usługi świadczone osobie fizycznej jako klientowi końcowemu.

[7] E. Brun, M. Milczarek, Expert forecast on emerging psychosocial risks related to occupational safety and health, European Agency for Safety and Health at Work, Office for Official Publications of the European Communities, Luxembourg 2007.

[8] D. Katz, R.L. Kahn, *Społeczna psychologia organizacji*, tłum. B. Czarniawska, Warszawa 1979.

[9] Work-related stress, European Foundation for the Improvement of Living and Working Conditions, Dublin 2010, s. 4.

[10] T. Cox, A. Griffiths, E. Rial-Gonzalez, Research on work-related Stress, Office for Official Publications of the European Communities, Luxembourg 2000.

dziesiątych – sześćdziesiątych XX w.[11] Ich skutkiem była zasadnicza zmiana paradygmatu badawczego – zrezygnowano z badań potencjalnie patogennego wpływu pojedynczych czynników środowiskowych (np. hałasu, presji czasu, konfliktów interpersonalnych) na rzecz *podejścia interakcyjnego*, proponując badanie konfiguracji różnych aspektów środowiska pracy jako potencjalnie etiologicznych w generowaniu negatywnych skutków dla fizycznego i psychicznego zdrowia pracownika[12].

Międzynarodowa Organizacja Pracy (ILO) w 1986 r. wprowadziła konceptualizację zagrożeń psychospołecznych jako pojęcia wyrażającego specyficzną, obarczoną ryzykiem szkody, interakcję pomiędzy:

- *treścią pracy* – sposobem organizowania i zarządzaniem pracą oraz innymi warunkami środowiskowymi i ekonomicznymi związanymi z pracą oraz
- kompetencjami i potrzebami pracownika.

Interakcja ta może być potencjalnie niebezpieczna dla zdrowia pracownika, który odzwierciedla wpływ różnych czynników zawodowych przez pryzmat swoich subiektywnych spostrzeżeń i doświadczeń związanych z pracą. Warto zaznaczyć, że materia badawcza jest tu bardzo skomplikowana: kilka rodzajów ryzyka psychospołecznego może występować w tym samym czasie, mogą one na siebie oddziaływać lub też wpływają na nie inne zmienne pośredniczące (uprzednie doświadczenia zawodowe pracownika, jego wiek, cechy osobowości itp.). Dlatego też zalecana jest ostrożność w uogólnianiu wyników badań dotyczących różnych rodzajów ryzyka psychospołecznego.

Klasycy eksploracji tego zagadnienia, Tom Cox i Amanda Griffiths, zagrożenia psychospołeczne podsumowali jako „[...] te aspekty projektowania pracy, organizacji pracy i zarządzania oraz ich społecznego i środowiskowego kontekstu, które mogą potencjalnie powodować szkody fizyczne lub psychiczne”[13]. W raporcie Europejskiej Agencji Zdrowia i Bezpieczeństwa w Pracy w 2007 r. zagrożenia psychospołeczne ujęto szeroko jako: „jakiekolwiek zagrożenie zawodowe, które narusza psychologiczny dobrostan pracownika, w tym jego możliwość uczestniczenia w środowisku pracy wśród innych osób […]; mające związek ze sposobami planowania, organizacji i zarządzania pracą w jej kontekście społeczno-ekonomicznym, które mogą powodować szkodę psychiczną, psychologiczną, fizyczną czy też chorobę”.

Wszystkie definicje podkreślają, że psychospołeczne ryzyka zawodowe uruchamiane są poprzez mechanizm stresu zawodowego (occupational stress) oraz że często towarzyszy im przemoc w pracy (workplace violence), które to dwa zjawiska są postrzegane jako współczesne najważniejsze wyzwania dla bezpieczeństwa i higieny pracy[14].

Warto zauważyć, że ryzyka psychospołeczne to de facto nowe kategorie stresorów zawodowych, czyli czynników prowokujących stres w pracy. Jeśli mają one charakter długotrwały, powodują chroniczny stan stresu u pracownika i z dużym prawdopodobieństwem uaktywniają w nim mechanizm zaburzeń psychicznych i fi-

[11] J.V. Johnson, E.M. Hall, Dialectic between conceptual and causal enquiry in psychosocial work environment research, “Journal of Occupational Health Psychology” 1996, t.1, nr 4, s. 362–374.
[12] T. Cox, A. Griffiths, E. Rial-Gonzalez, *Research on Work …*
[13] T. Cox, A. Griffiths, The nature and measurement of work-related stress and practice, [w:] Evaluation of Human Work, red. J.R. Wilson, N. Corlett, London 2005.
[14] E. Brun, M. Milczarek, *Expert forecast on emerging…*, 2007.

zycznych. Wśród możliwych dysfunkcji zdrowotnych spowodowanych szeroko pojętym stresem znajduje się cały przekrój zaburzeń psychogennych, w tym: nerwice, stany lękowe, depresje psychogenne, uzależnienia psychoaktywne, zespół stresu po-

Tabela 1

Klasyfikacja zagrożeń psychospołecznych związanych z pracą

Table 1

Taxonomy of work related psychosocial hazards

Zagrożenie psychospołeczne	Charakterystyka
Treść pracy	Brak różnorodności pracy (monotonia), zbyt krótkie cykle zadaniowe, praca fragmentaryczna/bez rozpoznawalnego sensu, praca poniżej posiadanych umiejętności, niepewność w pracy
Obciążenie pracą i tempo pracy	Przeciążenie zadaniami, niedociążenie zadaniami (nuda), tempo pracy dyktowane cyklem maszynowym, silna presja czasowa, wymogi terminowe
Kontrola	Niska partycypacja w procesie decyzyjnym, brak kontroli nad przeciążeniem pracą, tempem pracy, stylem pracy itp.
Czasowe ramy pracy	Praca zmianowa, praca nocna, sztywne ramy godzinowe pracy, ramy czasowe nieregularne, zbyt długie lub w niedogodnych godzinach
Środowisko pracy i wyposażenie stanowiska	Niekorzystne czynniki środowiska: ciasnota, złe oświetlenie, nadmierny hałas itp., nieodpowiedni sprzęt (mało użyteczny lub źle konserwowany)
Rola w organizacji	Stres roli organizacyjnej: niejasność, konflikt, odpowiedzialność
Kultura i funkcje organizacji	Słaba komunikacja wewnętrzna, brak wsparcia w rozwiązywaniu problemów i rozwoju osobistym, słabo zdefiniowane/uzgodnione cele organizacji
Relacje interpersonalne w pracy	Społeczna i fizyczna izolacja w pracy, złe relacje z przełożonymi, konflikty interpersonalne, brak wsparcia społecznego, zastraszanie, nękanie
Rozwój zawodowy	Stagnacja lub niepewność kariery, brak awansu lub zbyt wysoki awans, niskie wynagrodzenie, niepewność zatrudnienia, niski status społeczny pracy
Relacja praca–dom	Sprzeczne wymagania pracy i życia rodzinnego, słabe wsparcie społeczne w domu dla wykonywanej pracy, problem z godzeniem karier obu małżonków

Źródło: opracowanie własne na podstawie: T. Cox, A. Griffiths, E. Rial-Gonzalez, Research on Work-Related Stress, Office for Official Publications of the European Communities, Luxembourg 2000.

urazowego, zaburzenia psychosomatyczne, zespoły napięć szkieletowo-mięśniowych, zaburzenia zachowania[15].

Podkreśla się, że nowe formy pracy, wprowadzane jako postęp w praktykach organizacyjnych, generują także nowe ryzyka, które nie stają się od razu przedmiotem badań naukowych[16]. Tym niemniej badacze są zgodni w specyfikacji zasadniczych problemowych obszarów pracy, stanowiących potencjalne zagrożenia psychospołeczne (tab.1).

W długookresowej prognozie (forecast) trendu w rozwoju zagrożeń psychospołecznych Europejskiej Agencji Zdrowia i Bezpieczeństwa w Pracy jako najważniejsze ryzyka w 2007 r. wskazywano[17]:

- niskopłatne i niepewne (tzw. prekarialne, inaczej „śmieciowe") umowy o pracę,
- niepewność pracy ze względu na globalizację (ryzyko transferu miejsc pracy),
- nowe formy umów o pracę (tymczasowe, na żądanie, w niepełnym wymiarze),
- ogólne poczucie niepewności zatrudnienia,
- starzenie się siły roboczej (warunki pracy nie respektujące pogarszających się z wiekiem parametrów wydolności i zdrowia pracownika),
- zbyt długie i nieregularne godziny pracy,
- nadmierna intensyfikacja pracy (zbyt dużo zadań, presja czasu i terminów),
- trendy wyszczuplania (lean) struktury organizacyjnej powodujące obciążanie stanowisk dodatkowymi zadaniami,
- wysokie wymagania emocjonalne w pracy (przeżywany silny stres potęgowany przez kulturowy nakaz jego ukrywania w pracy),
- niedostatek równowagi praca – życie (work-life balance).

Przewidywane dziesięć lat temu negatywne trendy w środowisku psychospołecznym pracy są potwierdzane w licznych badaniach, w tym w przekrojowych badaniach benchmarkingowych porównujących natężenie tych samych czynników ryzyka w kolejnych cyklach badawczych i identyfikujących nowe ryzyka. Jednym z takich badań jest *Europejskie badanie przedsiębiorstw na temat nowych i* pojawiających *się zagrożeń* – ESENER, prowadzone przez Europejską Agencję Zdrowia i Bezpieczeństwa w Pracy (EU-OSHA). Pierwsza edycja badania – ESENER-1[18], była wykonana w roku 2009 (opublikowana w 2010), druga – ESENER-2[19], w roku 2014 (opublikowana w 2016). Porównanie wyników badań obydwu paneuropejskich

[15] Psychologia kliniczna, red. H. Sęk, Warszawa 2005.
[16] T. Cox, Stress Research and Stress Management: Putting Theory to Work, Sudbury 1993.
[17] E. Brun, M. Milczarek, Expert forecast on emerging…., s. 24–26.
[18] European Survey of Enterprises on New and Emerging Risks. Managing Safety and Health at Work. European Risk, ESENER – Overview Report, red. E. Rial-González, W. Cockburn, X. Irastorza, European Agency for Safety and Health at Work, Luxembourg 2010.
[19] Second European Survey of Enterprises on New and Emerging Risks (ESENER-2). Overview Report: Managing Safety and Health at Work. European Risk Observatory, red. X. Irastorza, M. Milczarek, W. Cockburn, Publications Office of the European Union, European Agency for Safety and Health at Work, Luxembourg 2016.

edycji badań pozwala na analizę natężenia i kierunków rozwoju zagrożeń w pracy w Unii Europejskiej.

W niniejszym opracowaniu skupiono się na wynikach ESENER-1 i ESENER-2 dotyczących Polski jako tła rozważań na temat krajowych trendów ryzyk psychospołecznych w pracy zawodowej[20].

Psychospołeczne ryzyka pracy w Polsce i w Unii Europejskiej w świetle badań ESENER

Badania ESENER są organizowane przy wsparciu rządów i partnerów społecznych na poziomie europejskim w celu lepszego zrozumienia problemów i potrzeb pracowników oraz zidentyfikowania czynników ułatwiających i utrudniających bezpieczną i nieszkodzącą zdrowiu pracę. Wywiady kwestionariuszowe z kadrą kierowniczą, specjalistami do spraw BHP i przedstawicielami pracowników przeprowadzane są na reprezentatywnej próbie przedsiębiorstw z wszystkich krajów UE, według tożsamej metodologii[21]. W badaniu ESENER ewaluacji poddawane są cztery obszary funkcjonowania zagadnień bezpieczeństwa i higieny pracy w organizacjach:

1. Ogólne podejście zakładu pracy do zarządzania BHP;
2. **Sposób traktowania ryzyka psychospołecznego jako nowego obszaru badań BHP**;
3. Główne czynniki motywujące do zarządzania BHP i bariery w tym obszarze;
4. Jak w praktyce jest zapewniane uczestnictwo pracowników w zarządzaniu BHP.

W ESENER-1 zbadano ok. 38 tys. organizacji, w przypadku ESENER 2 już prawie 50 tys., pytając pracowników najbardziej kompetentnych w kwestii zarządzania BHP w danej organizacji. Odpowiadali oni na pytania dotyczące najistotniejszych czynników ryzyka występujących w zakładzie pracy, informowali, w jaki sposób zarządzają takimi czynnikami, a także wskazywali bariery w podejmowaniu działań prewencyjnych w obszarze BHP.

Jedna z sekcji pytań kwestionariusza adresowana była do grupy tematycznej nr 2, czyli **sposobu traktowania ryzyka psychospołecznego jako nowego obszaru badań BHP**. Pytania tej sekcji dotyczyły oceny problemów zdrowia pracowników w związku z ewentualnymi zagrożeniami psychospołecznymi w miejscu pracy. Respondenci mogli wskazać (odpowiedź „tak" lub „nie"), czy którykolwiek z wymienionych kilku możliwych czynników stanowi istotny problem w ich zakładzie pracy,

[20] W ESENER-1 uczestniczyło 360 polskich organizacji, w ESENER-2 – 2257.

[21] W ESENER-1 badano firmy zatrudniające co najmniej 10 pracowników w firmach państwowych i prywatnych, reprezentujących wszystkie sektory działalności gospodarczej z wyłączeniem rolnictwa, leśnictwa i rybactwa z 31 państw: wszystkie 27 państw UE, kraje kandydujące (Chorwacja i Turcja) i państwa EFTA (Norwegia i Szwajcaria). W ESENER-2 zbadano organizacje z różnych sektorów działalności z 36 państw europejskich (28 krajów UE oraz z Albanii, Islandii, Czarnogóry, Macedonii, Serbii, Turcji, Norwegii i Szwajcarii).Uwzględniono też przedsiębiorstwa z sektora rybactwa i rolnictwa oraz mikrofirmy zatrudniające od 5 do 10 pracowników.

z punktu widzenia zagrożenia zdrowia pracownika. W tabeli 2 przedstawiono procentowe wyniki wskazań ryzyk psychospołecznych dla Polski przedstawione na tle średniej wartości dla danego czynnika, uzyskanej z wyników wszystkich krajów UE w danym cyklu badania. Porównano wyniki dla tych samych pytań uzyskane w obydwu edycjach, tj. w ESENER-1 oraz ESENER-2.

Tabela 2

Wskaźniki zagrożeń psychospołecznych związanych z pracą: PL – UE

Table 2

Indexes of work related psychosocial hazards: PL – EU

CZYNNIK RYZYKA PSYCHOSPOŁECZNEGO	ESENER 1 % odpowiedzi „ Tak”		ESENER 2 % odpowiedzi „Tak”	
	PL %	UE %	PL %	UE %
Presja czasu	**43**	52	**39**	43
Słaba komunikacja/koordynacja wewnątrz organizacji	15	27	8	17
Brak kontroli pracowników nad organizacją swojej pracy	16	19	10	13
Niepewność pracy	**31**	27	**16**	15
Konieczność kontaktów z trudnymi klientami, pacjentami, uczniami	**58**	50	**50**	58
Długie lub nieregularne godziny pracy	12	22	14	23
Dyskryminacja (na przykład ze względu na płeć, wiek lub pochodzenie etniczne)	2	7	0	2

Źródło: opracowanie własne na podstawie danych ESENER-1 (2010) i ESENER-2 (2016).

Zarówno w edycji ESENER-1, jak i w ESENER-2, najważniejszą dostrzeganą przez specjalistów BHP kwestią ryzyka psychospołecznego pracy **w polskich organizacjach** była:

- „konieczność kontaktów z trudnymi klientami, pacjentami, uczniami itp.”: w 2009 r. 58% w PL w stosunku do 50% w UE; w 2014 r. 50% w PL wobec 58% w UE;
- „presja czasu”: w 2009 r. 43% w PL wobec 52% w UE; w 2014 r. 39% w PL wobec 43% w UE;
- „niepewność pracy”: w 2009 r. w PL 31% wskazań wobec 27% średnio w UE; w 2014 r. w PL 16% wskazań wobec 15% średnio w UE.

Pierwszy ze wskaźników (kontakty interpersonalne) sygnalizuje rosnącą grupę zawodową prawdopodobnie borykającą się z problemem syndromu wypalenia za-

wodowego[22]. Drugi czynnik ryzyka (presja czasu) wskazuje na silną intensyfikację pracy i przeciążenie nią. Koresponduje z nim nieznacznie wzrostowa tendencja czynnika „długie lub nieregularne godziny pracy". Z kolei wysoki czynnik „niepewność pracy" w roku 2009 miał zapewne związek z realnym zagrożeniem bezrobociem w czasie rozwoju globalnego kryzysu gospodarczego. Analiza porównawcza pozwala też zauważyć pozytywne trendy dla krajowych przedsiębiorstw:

- Prawie o połowę zmniejszył się wskaźnik „słaba komunikacja/koordynacja wewnątrz organizacji" (z 15% w 2009 r. do 8% w 2014 r.);
- spadł wskaźnik „brak kontroli pracowników nad organizacją swojej pracy" (z 16% w 2009 r. do 10% w 2014 r.);
- w 2014 r. zerowy wskaźnik miał czynnik „dyskryminacja" (wobec 2% w 2009 r.).

Odnosząc się do szerzej przedstawionych w raporcie ESENER-2 (2016) wyników z badań wszystkich krajów członkowskich, można wskazać, że zazwyczaj najwyższe wskaźniki ryzyka psychospołecznego odnotowywane są w krajach Europy Północnej, i tak:

- „presja czasu" (i to w obydwu edycjach badania) na poziomie znacznie powyżej średniej europejskiej występuje w: Finlandii, Szwecji, Danii, Islandii i Norwegii (czynnik ten zgłaszany jest w ponad 70% zakładów pracy), zaś najniższy poziom odnotowują tu Litwa i Turcja (obydwa kraje po ok. 15%); w Polsce wskaźnik ten w obu edycjach badania plasuje się na poziomie nieznacznie poniżej średniej europejskiej;
- „długie lub nieregularne godziny pracy" są charakterystyczne dla Danii, Islandii i Norwegii (39%), w porównaniu z najniższymi wskaźnikami (ok. 10%) w Bułgarii, Turcji i Włoszech;
- „słaba komunikacja i współpraca w ramach organizacji" to problem 35% organizacji w Szwecji, ponad 25% w Danii, Finlandii i Belgii, najniższy poziom uzyskuje zaś na Litwie, w Bułgarii i Albanii (mniej niż 5%);
- czynnik „brak kontroli pracowników nad organizacją swojej pracy" występuje w 20–24% zakładów pracy Szwecji, Łotwy i Danii, a jedynie w 5% Cypru i Grecji;
- „niepewność zatrudnienia" jest najczęściej podnoszona w Finlandii, Chorwacji i Portugalii (30% lub więcej organizacji), natomiast w znikomym stopniu w Turcji i na Malcie (5–8%);
- „dyskryminacja, na przykład ze względu na płeć, wiek czy pochodzenie etniczne" jest najbardziej rozpowszechniona w Holandii i Wielkiej Brytanii (po 5% wskazań), w wielu krajach deklarowano zerowy poziom tego wskaźnika: m.in. w Albanii, Bułgarii, Czechach, Estonii, Litwie, Czarnogórze, Rumunii, Słowacji czy w Polsce, co z kolei wydaje się informacją nie w pełni obiektywną.

[22] E. Matuska, *Bezpieczeństwo psychologiczne w zarządzaniu zasobami lu*dzkimi – potrzeba prewencji wypalenia zawodowego, [w:] *Bezpieczeństwo w administracji i biznesie we współczesnym świecie*, red. M. Chrabkowski, C. Tatarczuk, J. Tomaszewski, cz. 1, Gdynia 2011, s. 326––327.

Warto podkreślić, że ewaluacja poziomu psychospołecznych czynników ryzyka w miejscu pracy może odzwierciedlać nie tylko rzeczywistą częstotliwość ich występowania, ale również poziom świadomości istnienia tych zagrożeń oraz możliwość ich identyfikacji. Są to uwarunkowania bardzo różniące się w poszczególnych zakładach pracy i w różnych krajach. Niedostrzeganie wagi poszczególnych rodzajów ryzyka przez respondentów nie przesądza, iż takowe w rzeczywistości nie występują w badanych przedsiębiorstwach, a jedynie wskazuje na subiektywną opinię badanych na ten temat.

Tym niemniej główne wnioski ESENER-2 w odniesieniu do ryzyk psychospołecznych dla krajów europejskich są następujące:

- „Konieczność kontaktów z trudnymi klientami, pacjentami, uczniami itp." (58%) oraz „presja czasu" (43%) stanowią najczęściej zgłaszane czynniki ryzyka psychospołecznego wśród zakładów pracy w całej UE-28;
- Czynniki te występują w podobnych obszarach działalności, z przewagą zakładów pracy w sektorach: edukacji, opieki zdrowotnej i pracy społecznej oraz administracji publicznej, w najmniejszym stopniu – w zakładach pracy w rolnictwie, leśnictwie i rybactwie oraz przetwórstwie przemysłowym;
- Wielkości obydwu ww. czynników ryzyka zwiększają się wraz z wielkością zakładu pracy, co widoczne jest w szczególności w przypadku czynnika „presja czasu";
- Czynniki ryzyka psychospołecznego są uznawane zgodnie za trudniejsze w prewencji niż inne czynniki ryzyka zawodowego: prawie 20% przedsiębiorstw, które zgłosiły konieczność „kontaktów z trudnymi klientami" lub „presję czasu", stwierdziło, że brakuje im informacji lub odpowiednich narzędzi umożliwiających skuteczne przeciwdziałanie temu ryzyku;
- Około 33% zakładów pracy zatrudniających więcej niż 20 pracowników w UE-28 zgłasza posiadanie planu działania na rzecz zapobiegania stresowi związanemu z pracą, przy czym procent takich zakładów wzrasta wraz z wielkością zakładu pracy i jest największy w obszarach: edukacji, opieki zdrowotnej i pracy społecznej. Najwięcej takich zakładów zidentyfikowano w Wielkiej Brytanii (57%), Rumunii (52%), Szwecji (51%) i Danii (51%), a najmniej w Chorwacji (9%), Estonii (9%) oraz Czechach (8%); w Polsce – 12%;
- Wśród zakładów pracy, w których zgłoszono „konieczność kontaktów z trudnymi klientami, pacjentami lub uczniami" w 55% z nich, które zatrudniają 20 lub więcej pracowników deklarowano istnienie procedury unikania tego rodzaju ryzyka (średnia z UE-28). Odsetek ten wzrastał do 72% wśród zakładów pracy z sektorów: edukacji, opieki zdrowotnej oraz pracy społecznej. Najwięcej takich zakładów pracy stwierdzono w Wielkiej Brytanii (91%), Szwecji (80%) oraz Irlandii (80%), a najmniej w Bułgarii (29%) i na Węgrzech (21%);
- Wśród podejmowanych działań prewencyjnych w zakładach pracy w UE-28 najczęściej wskazywano na reorganizację pracy w celu zmniejszenia obciążenia i presji w miejscu pracy (38%) oraz udzielanie poufnej (zazwyczaj psy-

chologicznej) porady pracownikom (36%). Największy procent takich zakładów stwierdzono w sektorach: edukacji, opieki zdrowotnej i pracy społecznej i w krajach nordyckich;
- Jako główne bariery we wdrażaniu środków prewencji ryzyk psychospołecznych w pracy wskazywano najczęściej: „niechęć do szczerej rozmowy na ten temat" oraz „brak świadomości wśród pracowników", nieco rzadziej zaś: „brak wiedzy fachowej i wsparcia specjalistów" oraz „brak świadomości wśród kierownictwa".

We wnioskach raportu z badań ESENER-2 i na podstawie benchmarkingu z danymi zgromadzonymi w raporcie ESENER-1 podkreślono, iż chociaż poszczególne ryzyka psychospołeczne zmieniają swoje natężenie w kolejnych latach – w zależności od zmian sytuacji mikro- i makroekonomicznej, w jakiej działają organizacje – ich treść ulega niewielkiej modyfikacji, aczkolwiek pojawiają się też nowe – dotąd nieznane czynniki ryzyka zawodowego. Takim nowym czynnikiem ryzyka okazuje się np. trudność w komunikacji wewnątrz organizacji z uwagi na brak lub bardzo słabą znajomość języka, w którym porozumiewają się pracownicy. Jest to skutek pojawienia się w Europie w ostatnich latach dużej grupy pracowników werbowanych spośród migrantów/uchodźców z krajów objętych konfliktami politycznymi, nieznających języka kraju ich przyjmującego.

Postulaty wskazywane we wnioskach z obydwu badań ESENER są następujące:
- Decydenci polityczni i zarządzający organizacjami powinni uważnie monitorować zagrożenia psychospołeczne typowe dla poszczególnych grup pracowniczych i uwzględniać je w programach zarządzania ryzykiem zawodowym w organizacjach;
- Zgodnie z celem strategii „Europa 2020", dotyczącym zwiększenia zatrudnienia, należy zwrócić uwagę na bardziej skuteczną walkę z zagrożeniami najczęściej występującymi i związanymi z rodzajem wykonywanych zadań lub dużą intensywnością pracy, a także z zagrożeniami mającymi duży wpływ na trwałość zatrudnienia, takimi jak mobbing czy przemoc w pracy;
- Zdecydowanego wzmocnienia wymaga polityka prewencyjna w krajach, w których niewiele przedsiębiorstw wprowadziło dotąd procedury przeciwdziałania zagrożeniom psychospołecznym. Wskazane jest opracowanie praktycznych wytycznych na poziomie krajowym, uzupełniających unijne wymogi prawne, zwłaszcza w przypadku sektora małych i średnich przedsiębiorstw;
- Środki zapobiegania zagrożeniom psychospołecznym w zakładach pracy zaleca się wprowadzać w ramach procedur zarządzania ryzykiem w przedsiębiorstwie. Prewencja tych ryzyk powinna być włączona do procedur zarządzania bezpieczeństwem i higieną pracy;
- Potrzebne jest krzewienie świadomości na temat istnienia zagrożeń psychospołecznych oraz mechanizmu ich psychogennego przekładania się na różne schorzenia nie tylko psychiczne, ale i fizyczne;
- Niezbędne jest upowszechnianie wyjaśnień i specyfikacji kosztów ekonomicznych ponoszonych przez przedsiębiorstwo i społeczeństwo na skutek zaniedbywania lub niedostrzegania ryzyk psychospołecznych w pracy. Brak

wskaźników konkretnego ryzyka może być sygnałem ignorancji, a nie rozwiązania problemu (tak, jak jest to w przypadku wskaźników dyskryminacji w niektórych krajach).

Podsumowanie

Intensywne zmiany w środowisku pracy prowadzą do powstawania nowych wymiarów ryzyka zawodowego, niemającego już dominującej natury fizycznej, ale psychospołeczną. Czynniki te są związane przede wszystkim ze sposobem organizacji pracy i zarządzaniem organizacją, a także z gospodarczym i społecznym kontekstem pracy. Dlatego też tradycyjne postrzeganie zagadnień BHP w przedsiębiorstwach musi być bezwzględnie rozszerzone o kontekst psychospołeczny, zwłaszcza w sektorze małych i średnich przedsiębiorstw, gdzie problem ten jest często ignorowany. Zgodnie z dyrektywą ramową Unii Europejskiej z 1989 r. zagrożenia psychospołeczne powinny być uwzględniane w strategiach przedsiębiorstw dotyczących zdrowia i bezpieczeństwa pracowników.

Kontrola ryzyk psychospołecznych, to przede wszystkim ochrona zdrowia zasobów pracy, coraz bardziej cenionych Polsce, gdzie po wielu latach wysokich wskaźników bezrobocia kształtuje się rynek pracownika i firmy mają trudności ze znalezieniem wartościowych kandydatów do pracy. To jednak także wymierne korzyści ekonomiczne: oszczędzanie wydatków na pokrycie kosztów absencji chorobowej pracowników, unikanie obniżonej wydajności pracy, wzrost morale i satysfakcji pracowników z własnej pracy. Żyjemy dłużej i dłużej pracujemy, przez ten czas otoczenie miejsca pracy, sama organizacja i metody pracy ulegają coraz szybszym przemianom. Elastyczne przystosowanie się pracownika do tych zmian wymaga ochrony i odnawiania jego zasobów psychicznych i fizycznych.

Bibliografia

Brun E., Milczarek M., *Expert forecast on emerging psychosocial risks related to occupational safety and health*, European Agency for Safety and Health at Work, Office for Official Publications of the European Communities, Luxembourg 2007.

Cox T., Griffiths A., Leka S., *Work organization and work-related stress*, [w:] *Occupational hygiene*, red. K. Gardiner, J.M. Harrington, Oxford 2005.

Cox T., Griffiths A., Rial-Gonzalez E., *Research on Work-Related Stress*, Office for Official Publications of the European Communities, Luxembourg 2000.

Cox T., Griffiths A., *The nature and measurement of work-related stress and practice*, [w:] *Evaluation of Human Work*, red. J.R. Wilson, N. Corlett, London 2005.

Cox T., *Stress Research and Stress Management: Putting Theory to Work*, Sudbury 1993.

European Survey of Enterprises on New and Emerging Risks. Managing Safety and Health at Work. European Risk, ESENER – Overview Report, red. E. Rial-González, W. Cockburn, X. Irastorza, European Agency for Safety and Health at Work, Luxembourg 2010.

Johnson J.V., Hall E.M., *Dialectic between conceptual and causal enquiry in psychosocial work environment research*, "Journal of Occupational Health Psychology" 1996, t. 1, nr 4.

Katz D., Kahn R.L., *Społeczna psychologia organizacji*, tłum. B. Czarniawska, Warszawa 1979.

Matuska E., *Bezpieczeństwo psychologiczne w zarządzaniu zasobami ludzkimi – potrzeba prewencji wypalenia zawodowego*, [w:] *Bezpieczeństwo w administracji i biznesie we współczesnym świecie*, red. M. Chrabkowski, C. Tatarczuk, J. Tomaszewski, cz. 1, Gdynia 2011.

Psychologia kliniczna, red. H. Sęk, t. 1 i 2, Warszawa 2005.

Second European Survey of Enterprises on New and Emerging Risks (ESENER-2). Overview Report: Managing Safety and Health at Work. European Risk Observatory, red. X. Irastorza, M. Milczarek, W. Cockburn, Publications Office of the European Union, European Agency for Safety and Health at Work, Luxembourg 2016.

Vogel L., *Dyrektywa ramowa – istotny element wdrażania skutecznej strategii zapobiegania wypadkom przy pracy*, „Bezpieczeństwo Pracy" 2002, nr 7/8.

Widerszal-Bazyl M., *Pojęcie ryzyka psychospołecznego w pracy*, „Bezpieczeństwo Pracy" 2009, nr 6.

Work-related stress, European Foundation for the Improvement of Living and Working Conditions, Dublin 2010

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz.U. 2016, poz. 1666, z późn. zm.).

https://osha.europa.eu/pl (dostęp: 10.02.2017).

http://osha.europa.eu/en/publications/reports/7807118 (dostęp: 14.02.2017).

Work-related stress, European Foundation for the Improvement of Living and Working Conditions, Dublin 2010. www.eurofound.europa.eu / work related stress EU2010. pdf (dostęp: 16.02.2017).

Summary

This article is dedicated to the psychosocial hazards associated with work in the context of the policy of occupational health and safety and work efficiency. In the introduction we point out the provisions of national and European law obliging the entrepreneur to control psychosocial risks in the workplace. The theoretical part of the article defines the concept of psychosocial risks, describes their classification and the social and economic conditions, and forecasts the long-term trends in their development. The empirical part of the article presents proposals for professional psychosocial risks in relation to Poland, based on a comparative analysis of the results of a study published in the reports ESENER-1 (2010) and ESENER-2 (2016), conducted by the European Agency for Safety and Health at Work. The analysis pooled the results of ESENER-2 for member countries of the European Union and identifies key messages in the field of prevention of occupational risks. In summary, the importance of psychosocial risk management strategies is highlighted in domestic enterprises, especially in the SME sector, where the problems are usually ignored.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 143–162 ROK 2017

ISSN 2543–7321

Mariusz Terebecki

Akademia Pomorska
Słupsk
mariusz.terebecki@apsl.edu.pl

Marcin Olkiewicz

Politechnika Koszalińska
Koszalin
marcin.olkiewicz@tu.koszalin.pl

JAKOŚĆ ZABEZPIECZEŃ INFORMACJI DETERMINANTĄ ROZWOJU BANKOWOŚCI INTERNETOWEJ

QUALITY OF INFORMATION SECURITY FOR DETERMINANTS DEVELOPMENT OF INTERNET BANKING

***Zarys treści*:** W warunkach szybko zmieniającego się otoczenia banki poszukują nowych sposobów na uzyskanie przewagi konkurencyjnej na rynku. Znaczącą determinantą kreującą zmiany jest jakość, a w szczególności jakość bezpieczeństwa informacji. To właśnie między innymi ona zmusza banki do ponoszenia nakładów na dostosowanie systemów informatycznych do oczekiwań międzynarodowych i światowych rynków finansowych oraz interesariuszy. Współczesny, wymagający interesariusz coraz częściej domaga się usług o wysokim standardzie, często dostarczanych za pomocą nowych technologii. Dlatego banki podejmują strategiczne działania mające na celu dostosowanie swoich produktów, usług do wymagań i oczekiwań interesariuszy a jednocześnie, poprzez wdrażane innowacje, generowanie nowych potrzeb. Należy jednak pamiętać, że wszystkie działania bankowe muszą gwarantować interesariuszom banku bezpieczeństwo informacji. Celem pracy jest ukazanie, jakie aspekty zabezpieczeń, które pośrednio wpływają na jakość oferowanej usługi bankowej, są kluczowe w bankowości elektronicznej. W publikacji zostaną przeanalizowane certyfikaty i zabezpieczenia, które są wykorzystywane w chwili kontaktu klienta z badanym bankiem poprzez platformę internetową. Do celów badawczych wykorzystano raporty PRNews.pl o stanie bankowości w Polsce w IV kwartale 2016 r.

***Słowa kluczowe*:** zabezpieczenia, jakość, bankowość internetowa, bank
Key words: security, quality, online banking, bank

Wprowadzenie

Jakość obsługi klienta jest jednym z ważniejszych elementów kreowania przewagi konkurencyjnej przedsiębiorstwa. Widoczne jest to również w bankowości, a szczególnie w bankowości elektronicznej. Bankowość elektroniczna, jako innowacyjność procesu świadczenia usług, w obecnych czasach stała się standardem w bankowości, tworząc wartość dodaną dla poszczególnych banków oraz ich klientów. Brak bezpośredniego kontaktu z pracownikami banku sprawia, że istotna jest jakość oferowanej elektronicznie usługi, która w odpowiedni sposób musi przekazywać, przetwarzać i generować informacje, poprzez odpowiednie zabezpieczenia gwarantujące i kreujące odpowiednią relację banku z klientem.

Należy zatem uznać, że jakość oferowanych produktów, asortyment oraz dostępność stały się determinantami rozwoju banków w Polsce. Dowodzą tego ostatnie trzy raporty opublikowane przez PRNews.pl pod koniec marca 2017 r., które podsumowują IV kwartał 2016 r. w obszarach: liczby klientów w bankach[1], rynku kont osobistych[2] oraz bankowości internetowej[3]. Przedstawione dane wyraźnie wskazują, iż liczba klientów z dostępem do bankowości elektronicznej sukcesywnie wzrasta i wynosi około 31 mln[4]. Widoczny trend wynikać może z odpowiedniego sposobu zarządzania bankami, w ramach odpowiednich systemów zarządzania, poprzez podejmowane i realizowane strategiczne działania ukierunkowane na jakość[5]. Odpowiednie i odpowiedzialne zarządzanie jakością, w ramach ciągłego doskonalenia, jest wynikiem rosnących oczekiwań i wymagań klientów, a także zagrożeń rynkowych widocznych w szczególności w sieci bankowości internetowej. Zaspokajanie potrzeb oraz zwiększanie satysfakcji interesariuszy sektora bankowego wymaga wysokiej skuteczności banku m.in. z zakresu marketingu – oferowania nowych produktów, a także teleinformatyki – gwarantowania bezpiecznego sposobu dostarczania i zakupu usługi.

Celowe zatem staje się sprawdzenie wdrożonych przez poszczególne banki zabezpieczeń dostępu do usług z rodziny e-bankingu. Ponadto przyjęta[6] przez banki

---

[1] Raport PRNews.pl: Liczba klientów w bankach – IV kw. 2016, http://prnews.pl/wiadomosci/raport-prnewspl-liczba-klientow-w-bankach-iv-kw-2016-6554091.html (dostęp: 31.03.2017).

[2] Raport PRNews.pl: Rynek kont osobistych – IV kw. 2016, http://prnews.pl/raporty/raport-prnewspl-rynek-kont-osobistych-iv-kw-2016-6553975.html (dostęp: 31.03.2017).

[3] Raport PRNews.pl: Rynek bankowości internetowej – IV kw. 2016, http://prnews.pl/wiadomosc/raport-prnewspl-rynek-bankowosci-internetowej-iv-kw-2016-6554056.html (dostęp: 31.03.2017).

[4] Wartość ta nie może być bezpośrednio zestawiona z liczbą ludności w Polsce, wynika to z prostego faktu – istnieje na pewno spora grupa klientów, którzy są klientami równocześnie kilku banków.

[5] M. Olkiewicz, *Zarządzanie jakością w sektorze bankowym w dobie wejścia do Unii Europejskiej*, [w:] Rynki finansowe w przestrzeni elektronicznej, red. B. Świecka, Szczecin 2004.

[6] W dniu 8 stycznia 2013 r. Komisja Nadzoru Finansowego jednogłośnie przyjęła Rekomendację D dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach. KNF przewidywała, że zalecenia zostaną wprowadzone nie później niż do dnia 31 grudnia 2014 r.

Rekomendacja D[7], dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, zobowiązuje je m.in. do systematycznego wykonywania analizy ryzyka teleinformatycznego. Zatem świadczone usługi powinny być na najwyższym poziomie, zgodnym z obowiązującą wiedzą informatyczną z dziedziny bezpieczeństwa oraz winny być odporne na znane rodzaje ataków wymierzone we wdrożone zabezpieczenia.

Rekomendacja D

Banki, uważane za instytucje zaufania publicznego, szczególną uwagę zwracają na jakość usługi bankowej, a przede wszystkim bezpieczeństwo finansowe[8] odbiorcy informacji. Poczucie bezpieczeństwa odczuwane przez interesariuszy banku wpływa pośrednio między innymi na wymianę informacji o bankach i ich produktach dostosowanych do jakości życia społeczeństwa (fora internetowe, portale społecznościowe itd.) a także na kreowanie wizerunku oraz marki.

Mając na uwadze fakt, że na ocenę końcową jakości usługi determinujący wpływ ma efekt końcowy procesu świadczenia, należy w działaniach strategicznych ochrony informacji banku zwrócić szczególną uwagę na zagrożenia dla bezpieczeństwa informacji wynikające między innymi z: dostępności, poufności, integralności, rozliczalności informacji oraz niezgodności z przepisami. Analiza ryzyk występujących w scenariuszach zagrożeń powoduje konieczność eliminacji lub minimalizacji zagrożeń lub ich efektów przez zabezpieczenie się w ramach Rekomendacji D.

Rekomendacja D zawiera 22 wytyczne szczegółowe, obejmujące cztery „obszary ryzyk" środowiska teleinformatycznego[9]:

- strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa,
- rozwój środowiska IT,
- utrzymanie i eksploatacja IT,
- zarządzanie bezpieczeństwem IT.

Rekomendacja wprowadza zdefiniowane pojęcie dotyczące bezpieczeństwa informacji jako zachowanie poufności, integralności i dostępności informacji; w ramach bezpieczeństwa informacji mogą być uwzględniane również inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (na podstawie ISO/IEC 27000:2009)[10].

Z punktu widzenia niniejszego artykułu bardzo ważna jest Szczegółowa Rekomendacja nr 16 ww. dokumentu, której brzmienie jest następujące: „Bank świadczący usługi z wykorzystaniem elektronicznych kanałów dostępu powinien posiadać skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsa-

[7] https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf (dostęp: 22.02.2017).
[8] S. Wojciechowska-Filipek, *Zarządzanie jakością informacji w organizacjach zhierarchizowa*nych, Warszawa 2015, s. 11.
[9] https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf (dostęp: 22.02.2017).
[10] Tamże, s. 6.

mości i bezpieczeństwo danych oraz środków klientów, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów”[11].

Należy również podkreślić, że w punkcie 16.4. wskazano, iż „dodatkowo, bank powinien zapewnić, że: sesje połączeniowe bankowości elektronicznej są szyfrowane oraz prowadzone są dodatkowe mechanizmy, które w możliwie największym stopniu uodparniają te sesje na manipulacje”[12].

Warto w tym momencie zaznaczyć, że w procesie odpowiedniego zarządzania jakością podejmowane są działania proinnowacyjne[13], które pozwolą interesariuszom korzystać z multikanałowości banków. Oznacza to, iż obecnie interesariusze banku korzystają z przeróżnych systemów operacyjnych, które w różnym stopniu obsługują standardy dotyczące używanych protokołów internetowych mających za zadanie zabezpieczyć kanał komunikacji elektronicznej pomiędzy klientem a serwerem. Jednocześnie wykorzystują różne urządzenia końcowe – nie są to tylko komputery PC lub laptopy, ale także tablety, smartfony, iPady, czyli urządzenia mobilne.

Identyfikacja polskiego sektora bankowego

Sektor bankowy w Polsce jest jednym z najbardziej rozwijających się obszarów gospodarki. Wysoka jakość usług oferowanych przez banki wynikać może z realizowanych odpowiedzialnych strategii ukierunkowanych na wzrost efektywności i konkurencyjności. Zarządzanie jakością w bankach pozwoliło stworzyć standaryzację usług, które w znaczący sposób oddziaływały na optymalizację kosztów, a także zmianę kreowania podejścia do interesariuszy i generowania innowacyjnych produktów. Natomiast odpowiednie zarządzanie finansami banku ukierunkowane było na proces podejmowania decyzji finansowych i inwestycyjnych (pozyskiwania źródeł finansowania działalności operacyjnej od interesariuszy), ich zagospodarowania tak, aby realizować cel strategiczny, jakim jest wzrost wartości banku przy określonym regulacjami nadzorczymi poziomie ryzyka[14]. Należy jednak pamiętać, że wszystkie podejmowane działania ukierunkowane są na kształtowanie odpowiednich relacji i interakcji w ujęciu interesariusze – bank.

Obszerną analizę obszarów rozwoju bankowości przedstawiają Raporty PR-News.pl, w których poddana została ocenie działalność 19 banków działających na terenie Polski. Ze względu na tematykę publikacji, zwrócono szczególną uwagę w raportach na: liczbę klientów ogółem[15], liczbę klientów indywidualnych[16], liczbę

[11] Tamże, s. 48–49.
[12] Tamże, s. 49.
[13] M. Olkiewicz, Knowledge management as a determinant of innovation in enterprises, [w:] Proceedings of the 9th International Management Conference. Management and Innovation For Competitive Advantage, Bucharest 2015, s. 399–409.
[14] M. Capiga, *Zarządzanie bankami*, Warszawa 2010, s. 63.
[15] Każdy bank do struktury swoich klientów wlicza nie tylko osoby fizyczne, dla banku klientem są: korporacje, spółki, firmy, szkoły, gminy, miasta, stowarzyszenia, fundacje itp.
[16] Niektóre banki do klientów indywidualnych zaliczają także małe firmy, np. jednoosobowe działalności gospodarcze.

Tabela 1

Podsumowanie IV kwartału 2016 r. w polskim sektorze bankowym

Table 1

Summary of IV quarter 2016 in the Polish banking sector

Bank	[1]	[2]	[3]	[4]	[5]	[6]
PKO BP i Inteligo	9 199 000	8 756 000	8 805 000	3 579 000	6 850 000	52,25%
Bank Pekao SA	5 232 748	4 939 652	3 176 917	1 708 571	3 773 443	45,28%
mBank i Orange Finanse	4 476 000	4 455 000	3 960 712	1 982 578	3 542 509	55,97%
BZ WBK	4 400 000	4 000 000	2 875 360	1 770 338	3 120 000	56,74%
ING Bank Śląski	4 318 400	4 270 000	3 172 806	1 836 129	2 689 000	68,28%
Alior Bank	3 505 685	3 318 429	1 771 434	734 391	1 944 299	37,77%
Bank BGŻ BNP Paribas i BGŻOptima	2 600 000	2 400 000	928 825	451 072	763 006	59,12%
Credit Agricole Bank Polska	2 100 000*	1 000 000	761 715	382 092	970 610	39,37%
Bank Millennium	2 088 000	2 026 000	1 798 731	b.d.	1 898 888	b.d.
Getin Noble Bank	2 000 000*	1 900 000*	b.d.	321 200	971 300	33,07%
Eurobank	1 453 208	1 453 208	446 866	197 060	1 453 208	13,56%
Bank Pocztowy	1 324 801	1 142 918	510 867	161 912	831 235	19,48%
Raiffeisen Polbank	763 300	680 500	680 450	232 070	630 950	36,78%
Citi Handlowy	687 000	680 800	669 930	322 000	267 000	120,60%[17]
T-Mobile Usługi Bankowe	608 768	608 768	608 768	b.d.	534 171	b.d.
Deutsche Bank	396 200	356 000	296 639**	186 824***	250 000	74,73%
Plus Bank	290 129	280 536	122 980	54 640	197 903	27,61%
BOŚ	255 000*	250 000*	133 100**	b.d.	263 900****	b.d.
Santander Consumer Bank	b.d.	2 017 151	b.d.	b.d.	b.d.	b.d.
RAZEM:	**45 698 239**	**44 534 962**	**30 721 100**	**13 919 877**	**30 951 422**	

Legenda:
[1] Liczba klientów ogółem
[2] Liczba klientów indywidualnych
[3] Liczba klientów indywidualnych mających podpisaną umowę umożliwiającą korzystanie z bankowości internetowej (nie tylko ROR)
[4] Liczba klientów indywidualnych, którzy przynajmniej raz w miesiącu logują się do ROR za pomocą bankowości internetowej
[5] Liczba ROR (klienci indywidualni – jedynie konta złotowe, bez rachunków oszczędnościowych)
[6] Procentowy udział klientów aktywnych w stosunku do liczby ROR-ów
* Bank nie podał danych na koniec 2016. Przyjęto szacunki
** Deutsche Bank i BOŚ nie podały danych za IV kw. 2016 r. Przyjęto dane z III kw. 2016 r.[18]
*** Deutsche Bank nie podał danych za IV kw. 2016 r. Przyjęto dane z III kw. 2016 r.
**** BOŚ wyniki za IV kw. 206 r. poda dopiero 31.III.2016 r. Podane są dane za III kw. 2016 r.

Źródło: Opracowanie własne na podstawie PRNews.pl

[17] Niektóre banki umożliwiają aktywowanie dostępu do bankowości internetowej bez zakładania rachunku.

[18] Raport PRNews.pl: Rynek bankowości internetowej – III kw. 2016, http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-internetowej-iii-kw-2016-6553450.html (dostęp: 31.03.2017).

klientów indywidualnych mających podpisaną umowę umożliwiającą korzystanie z bankowości internetowej[19], liczbę „klientów aktywnych"[20] oraz liczbę prowadzonych przez banki ROR-ów. Mimo że nie wszystkie banki podały pełne informacje, to jednak nie zdecydowano się usunąć żadnej pozycji, gdyż uniemożliwiałoby to późniejsze porównanie otrzymanych wyników.

Wszystkie banki posiadają w swoich portfelach ogółem około 46 mln umów. Istotny dla prowadzonych rozważań jest fakt, iż aż około 30 mln z nich, to umowy umożliwiające korzystanie z bankowości elektronicznej. Również z 30 mln rachunków typu ROR około 14 mln ma aktywnych użytkowników bankowości elektronicznej. W celu lepszej prezentacji jakościowej i ilościowej wskazanych parametrów sporządzono tabelę 1.

Analiza danych w tabeli 1 pozwoliła na zidentyfikowanie, w każdej kategorii, pierwszej piątki wiodących banków oraz wyliczenie procentowego udziału aktywnych klientów w stosunku do liczby ROR-ów[21]. Głównymi parametrami i wielkościami charakteryzującymi wielką piątkę są[22]:

- liczba klientów ogółem – 60,45% (ok. 28 mln klientów);
- liczba klientów indywidualnych – 59,33% (ok. 26 mln klientów);
- liczba klientów indywidualnych mających podpisaną umowę umożliwiającą korzystanie z bankowości internetowej (nie tylko ROR) – 71,58% (ok. 22 mln klientów);
- liczba klientów indywidualnych, którzy przynajmniej raz w miesiącu logują się do ROR za pomocą bankowości internetowej – 78,14% (ok. 11 mln klientów);
- liczba ROR – 64,54% (ok. 20 mln rachunków typu ROR[23]);
- średni procentowy udział klientów aktywnych w stosunku do liczby ROR-ów – 55,70% (średnia wszystkich banków 49,37%).

Warto podkreślić, iż udział „wielkiej piątki", w każdym przedstawionym aspekcie przekracza 50% ogólnego portfela. Zatem zarządzanie bezpieczeństwem informacji ma istotne znaczenie dla rozwoju usług on-line.

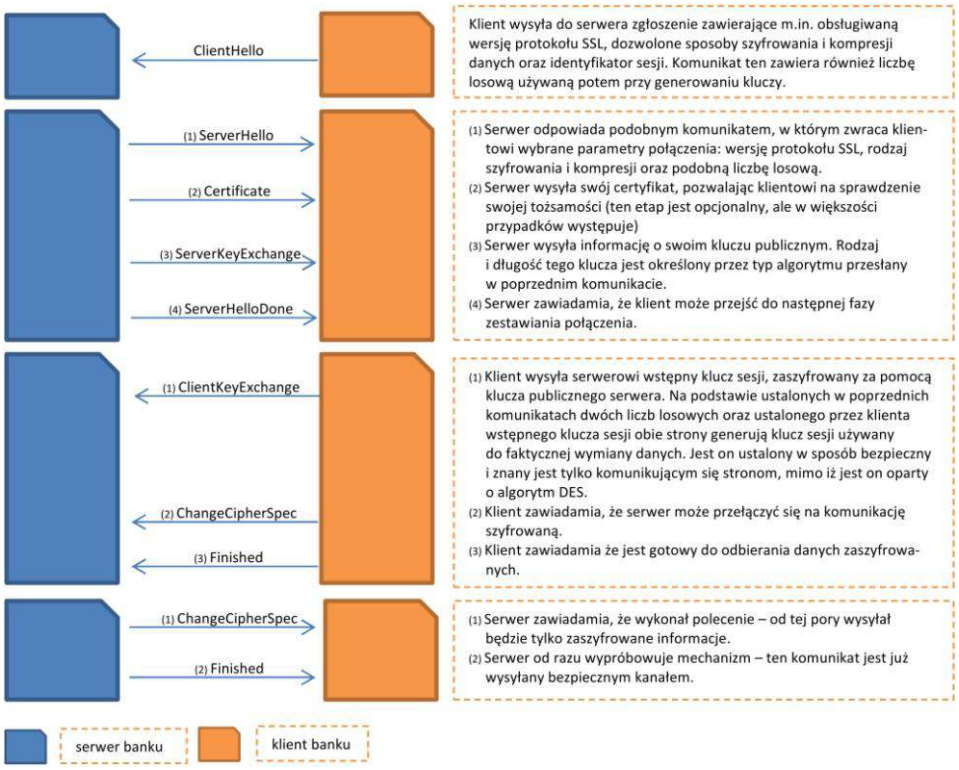
Kanał informatyczny jako uwierzytelnienie relacji serwer – klient

Podczas korzystania z usług e-bankingu musi zajść zdarzenie polegające na tym, że dwie strony (serwer i klient), które zamierzają się skomunikować ze sobą, są zobowiązane przeprowadzić „pewne" ustalenia dotyczące kanału komunikacyjnego. Podczas tego procesu dochodzi do wymiany określonych komunikatów (nazwanych standardem komunikacyjnym), w których między innymi określana jest wersja pro-

[19] Liczba umów nie dotyczy tylko i wyłącznie rachunków ROR.
[20] ROR – rachunek oszczędnościowo-rozliczeniowy.
[21] Niektóre banki umożliwiają aktywowanie dostępu do bankowości internetowej bez zakładania rachunku.
[22] Wielka piątka: PKO BP i Inteligo, Bank Pekao SA, mBank i Orange Finanse, BZ WBK, ING Bank Śląski.
[23] Klienci indywidualni – jedynie konta złotowe, bez rachunków oszczędnościowych.

tokołu[24], sposobu szyfrowania i kompresji danych. Wysyłane są również certyfikaty bezpieczeństwa, które umożliwiają sprawdzenie tożsamości jednej ze stron lub obydwóch stron.

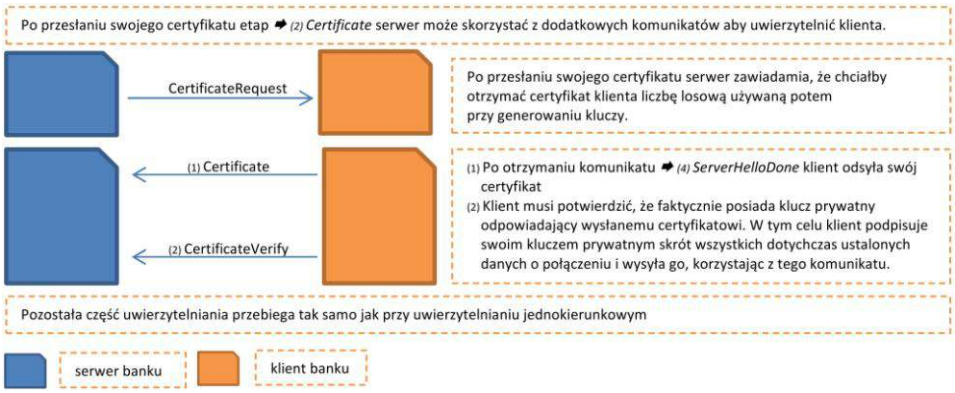
Celem przybliżenia mechanizmu działania procesu komunikacji przedstawiono na rysunku 1 schematy uwierzytelniania jednokierunkowego (uwierzytelnienie serwera) pomiędzy serwerem a klientem i na rysunku 2 uwierzytelniania dwukierunkowego (uwierzytelnienie klienta).



Rys. 1. Uwierzytelnienie jednokierunkowe – uwierzytelnienie serwera
Fig. 1. One-way authentication – server authentication

Źródło: Opracowanie własne, na podstawie https://pl.wikipedia.org/wiki/Transport_Layer_Security.

[24] Protokół SSL (ang. Secure Socket Layer) – protokół służący do bezpiecznej transmisji zaszyfrowanego strumienia danych i jego rozwinięcie, czyli protokół TLS (ang. Transport Layer Security) – protokół zapewnia poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy klienta; opiera się na szyfrowaniu asymetrycznym oraz certyfikatach X.509; więcej informacji: https://pl.wikipedia.org/wiki/Transport_Layer_Security.



Rys. 2. Uwierzytelnienie dwukierunkowe – uwierzytelnienie klienta
Fig. 2. Two-way authentication - client authentication

Źródło: Opracowanie własne, na podstawie https://pl.wikipedia.org/wiki/Transport_Layer_Security.

Jak można zauważyć analizując powyższe schematy, proces uzgadniania odpowiednich poziomów bezpieczeństwa jest procesem długotrwałym oraz dodatkowo wymaga skomplikowanych obliczeń. Aby podczas przerwania kanału komunikacyjnego lub w przypadkach krótkich połączeń nie dochodziło do sytuacji ponownego zestawiania odpowiednich parametrów komunikacyjnych, istnieje możliwość kontynuowania wcześniej rozpoczętej sesji (klient musi wysłać odpowiedni komunikat ⬅ *ClientHello* zawierający parametr SessionId).

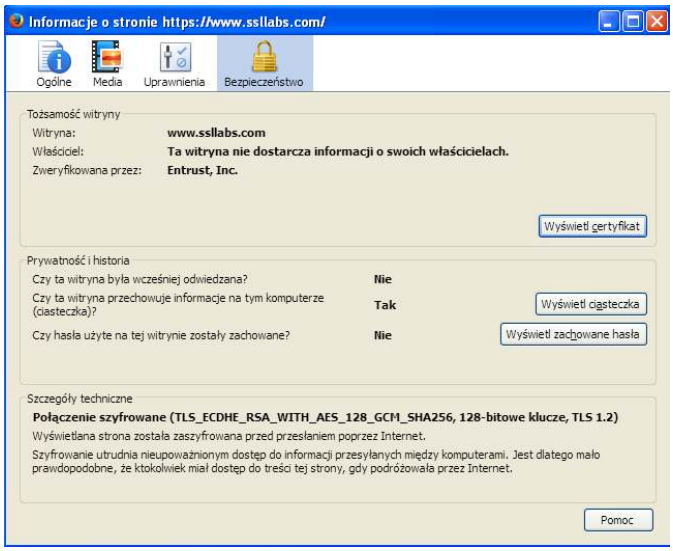
Oczywiście długość pamiętania poprzedniej sesji jest nadzorowana przez serwer i w przypadku jej minięcia klient mimo wysłania identyfikatora równego parametrowi SessionId nie będzie mógł jej kontynuować ze względu na jej przeterminowanie (wygaśnięcie).

Warto zaznaczyć, że gdyby nawet pominąć skomplikowanie ustalenia parametrów kanału komunikacyjnego na drodze klient – serwer, to i tak nie można zapomnieć o tym, iż obecne bezpieczeństwo kanału komunikacyjnego, bez względu na rodzaj użytego szyfrowania, opiera się na krytycznym parametrze określającym siłę szyfrowania, czyli długości klucza. Im dłuższy klucz, tym trudniej go złamać, a przez to odszyfrować transmisję.

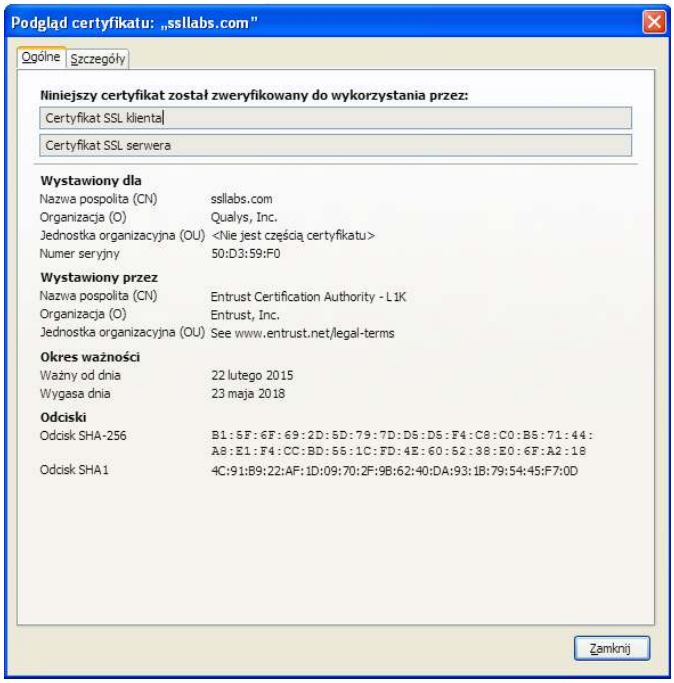
Określenie długości klucza jest wymogiem każdego banku, gdyż to właśnie on gwarantuje swemu klientowi bezpieczeństwo, gdyż przejęcie kanału komunikacyjnego i jego odszyfrowanie pozwala stronie trzeciej na dowolną modyfikację przesyłanych wiadomości przez ten kanał i np. dokonanie zmiany parametrów przelewu.

Analiza bezpieczeństwa użytej metody szyfrowania – przegląd zabezpieczeń

Klienci bankowi edukowani są, iż powinni zwracać uwagę na fakt występowania „zielonej kłódki" na pasku przeglądarki, gdyż taki stan świadczy o zabezpieczonym połączeniu. Dodatkowo wszystkie połączenia z usługami e-bankingu powinny być



Rys. 3. Informacje bezpieczeństwa dla witryny
Fig. 3. Security information for your site
Źródło: Opracowanie własne.



Rys. 4. Podgląd informacji dotyczących certyfikatu
Fig. 4. View information about the certificate
Źródło: Opracowanie własne.

poprzedzone przez adres internetowy zaczynający się od https://[25]. Cóż zatem kryje się za zieloną kłódką i protokołem https? Za pomocą zwykłego sprawdzenia bezpieczeństwa danej witryny użytkownik może się przekonać o tożsamości witryny oraz zobaczyć dla kogo i przez kogo został wystawiony certyfikat bezpieczeństwa. Przykładowa informacja, jaka jest dostępna dla użytkownika z poziomu każdej przeglądarki internetowej, przedstawiona została rysunkach 3 i 4. Rysunki przedstawiają informację na temat strony www firmy Qualys i jej produktu SSL Labs.

Warto zastanowić się, czy takie informacje wystarczają, aby stwierdzić, że dana witryna jest bezpieczna? W większości wypadków można odpowiedzieć twierdząco. Ale czy można zweryfikować tę jakość poprzez niezależne źródło? Oczywiście, że tak, gdyż w erze powszechnego dostępu do informacji i niezależnych usług nie stanowi to większego problemu.

Na potrzeby publikacji wszystkie testy[26] zostały oparte na raportach generowanych przez specjalne ogólnodostępne narzędzie[27] SSL Server Test[28]. Jednocześnie, aby ograniczyć ilość informacji przedstawionych w danym raporcie postanowiono, że pokazane zostanie tylko podsumowanie dla wielkiej piątki oraz odnośniki do raportów dla pozostałych banków.

PKO BP i INTELIGO

A. iPKO (https://www.pkobp.pl/)[29]

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów[30]: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)
- Algorytmy szyfrowania[31] dla TLS 1.2[32]:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,

[25] HTTPS (ang. Hypertext Transfer Protocol Secure), to szyfrowana wersja protokołu HTTP w relacji serwer – klient/klient – serwer, szyfrowanie to zapobiega to przechwytywaniu i zmienianiu przesyłanych danych.

[26] Zabezpieczenia oceniane są za pomocą liter: A+, A, B, C, D, E, F; gdzie A+ ocena najwyższa, zaś F ocena najniższa.

[27] Narzędzie te jest dostępne na stronach https://www.ssllabs.com/ (dostęp: 31.03.2017).

[28] Metodologia wykorzystywana podczas rankingu serwisów https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide (dostęp: 31.03.2017).

[29] https://www.ssllabs.com/ssltest/analyze.html?d=www.ipko.pl (dostęp: 31.03.2017).

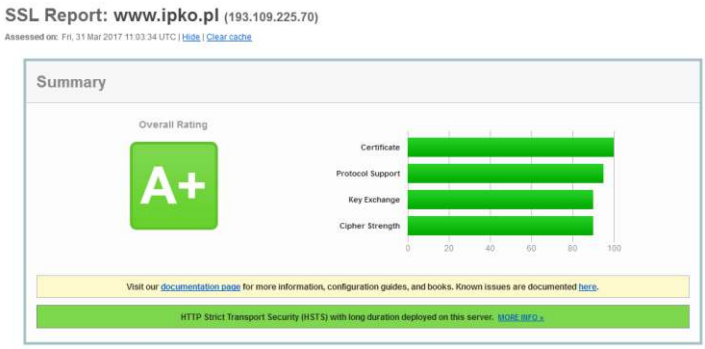
[30] Kwestia istotna ze względu na używanie danego systemu i agenta (przeglądarki internetowej, dedykowanego oprogramowania) w realizowaniu połączenia serwer – klient – nie każdy agent potrafi nawiązać połączenia, wykorzystując najlepszy/najbezpieczniejszy protokół.

[31] Tylko dla najwyższego protokołu, reszta informacji dla innych protokołów dostępna w pełnym raporcie.

[32] Algorytmy opisane zostały w dokumencie referencyjnym RFC5289, https://www.ietf.org/rfc/rfc5289.txt (dostęp: 31.03.2017).

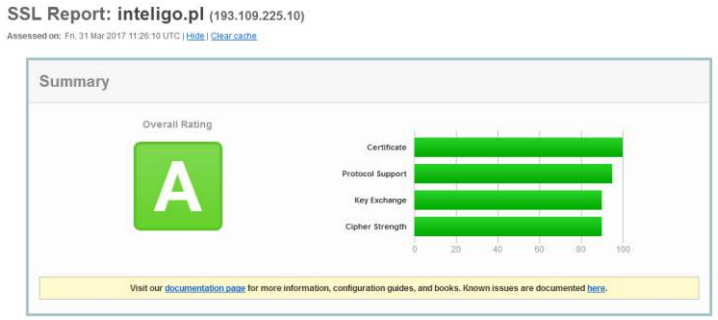
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_3DES_EDE_CBC_SHA.

- Nieudana symulacja połączenia: IE 6 / XP.



Rys. 5. Podsumowanie raportu dla ipko
Fig. 5. Summary report for ipko
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

B. Inteligo (https://inteligo.pl/secure)[33]



Rys. 6. Podsumowanie raportu dla Inteligo
Fig. 6. Summary report for Inteligo
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.*com*

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)
- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,

[33] https://www.ssllabs.com/ssltest/analyze.html?d=inteligo.pl (dostęp: 31.03.2017).

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_3DES_EDE_CBC_SHA.

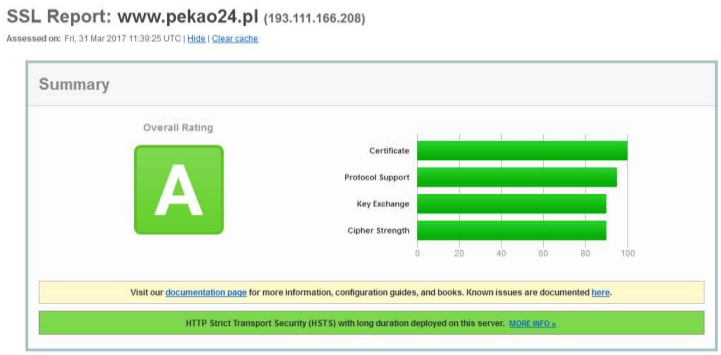
- Nieudana symulacja połączenia: IE 6 / XP.

BANK PEKAO SA

C. Pekao24 (https://www.pekao24.pl/)[34]

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)
- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
  TLS_RSA_WITH_AES_256_GCM_SHA384,
  TLS_RSA_WITH_AES_256_GCM_SHA384,
  TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_RSA_WITH_AES_128_CBC_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA,
  TLS_RSA_WITH_AES_128_CBC_SHA,
  TLS_RSA_WITH_3DES_EDE_CBC_SHA.
- Nieudana symulacja połączenia: IE 6 / XP.

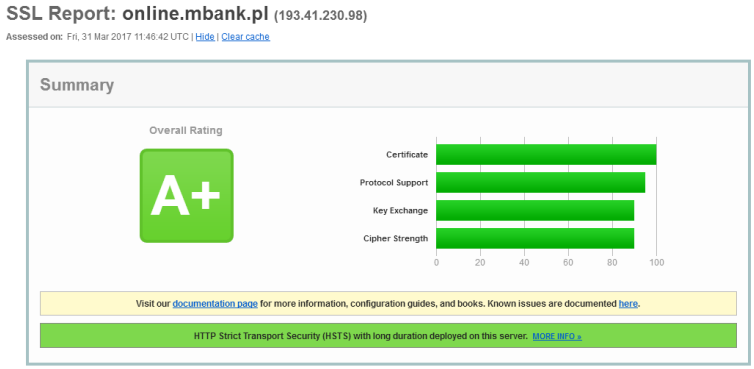


Rys. 7. Podsumowanie raportu dla Pekao24
Fig. 7. Summary report for Pekao24
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

[34] https://www.ssllabs.com/ssltest/analyze.html?d=www.pekao24.pl (dostęp: 31.03.2017).

MBANK i ORANGE FINANSE

D. mbank (https://online.mbank.pl/)[35]



Rys. 8. Podsumowanie raportu dla mbank
Fig. 8. Summary report for mbank
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)
- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
  TLS_RSA_WITH_AES_256_GCM_SHA384,
  TLS_RSA_WITH_AES_128_GCM_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_RSA_WITH_AES_128_CBC_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA,
  TLS_RSA_WITH_AES_128_CBC_SHA.
- Nieudana symulacja połączenia: IE 6 / XP, IE 8 / XP.

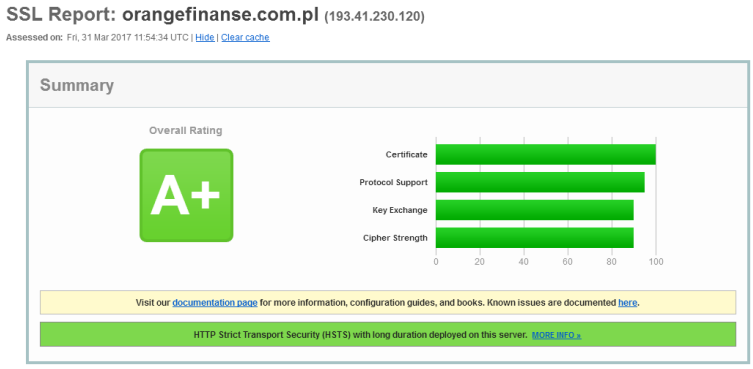
E. Orange Finanse (https://orangefinanse.com.pl/)[36]

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)

[35] https://www.ssllabs.com/ssltest/analyze.html?d=online.mbank.pl (dostęp: 31.03.20107).
[36] https://www.ssllabs.com/ssltest/analyze.html?d=orangefinanse.com.pl (dostęp: 31.03.2017).

- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
  TLS_RSA_WITH_AES_256_GCM_SHA384,
  TLS_RSA_WITH_AES_128_GCM_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA256,
  TLS_RSA_WITH_AES_128_CBC_SHA256,
  TLS_RSA_WITH_AES_256_CBC_SHA,
  TLS_RSA_WITH_AES_128_CBC_SHA.
- Nieudana symulacja połączenia: IE 6 / XP, IE 8 / XP.



Rys. 9. Podsumowanie raportu dla Orange Finanse
Fig. 9. Summary report for Orange Finance
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

BZ WBK

F. BZWBK24 (https://www.centrum24.pl/)[37]

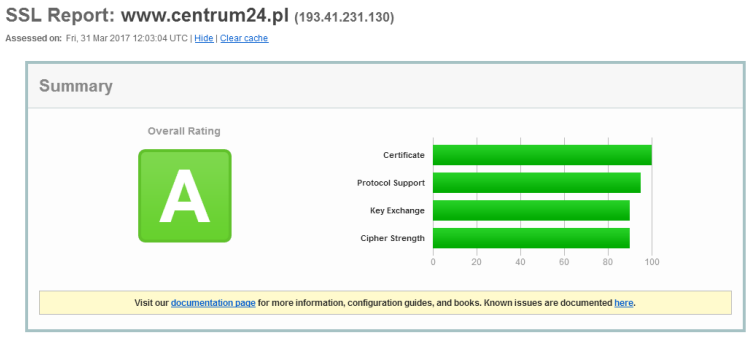
Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)
- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_RSA_WITH_AES_256_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,

[37] https://www.ssllabs.com/ssltest/analyze.html?d=www.centrum24.pl (dostęp: 31.03.2017).

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA.

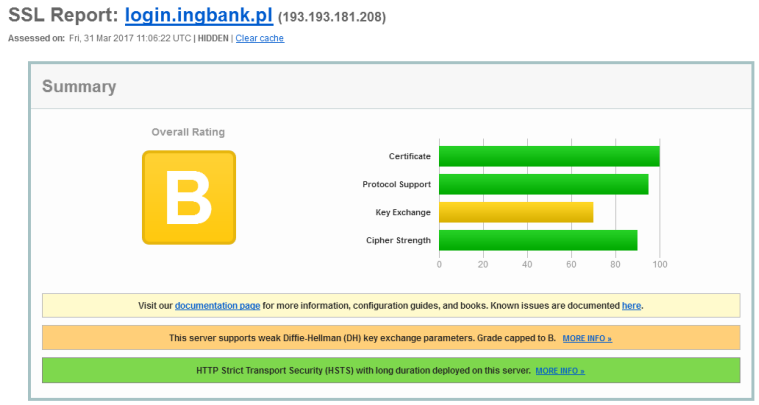
- Nieudana symulacja połączenia: IE 6 / XP, IE 8 / XP, Java 6u45.



Rys. 10. Podsumowanie raportu dla BZWBK24
Fig. 10. Summary report for BZWBK24
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

ING BANK ŚLĄSKI

G. Moje ING (https://login.ingbank.pl/)[38]



Rys. 11. Podsumowanie raportu dla Moje ING
Fig. 11. Summary report for My ING
Źródło: Opracowanie własne, na podstawie https://www.ssllabs.com

Główne dane:

- Posiadany certyfikat: RSA 2048 bits (SHA256withRSA).
- Wsparcie protokołów: TLS 1.2 (Tak); TLS 1.1 (Tak); TLS 1.0 (Tak); SSL 3 (Nie), SSL 2 (Nie)

[38] https://www.ssllabs.com/ssltest/analyze.html?d=login.ingbank.pl&s=193.193.181.208 (dostęp: 31.03.2017).

- Algorytmy szyfrowania dla TLS 1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA.
- Nieudana symulacja połączenia: IE 6 / XP.

POZOSTAŁE BANKI

Analiza pozostałych banków pozwoliła zidentyfikować i ocenić na:

- Alior Bank (https://aliorbank.pl/hades/)[39] – ocena ogólna[40] A;
- Bank BGŻ BNP Paribas i BGŻOptima (https://login.bgzbnpparibas.pl/)[41] – ocena ogólna A;
- Credit Agricole Bank Polska (https://e-bank.credit-agricole.pl/)[42] – ocena ogólna C;
- Bank Millennium (https://www.bankmillennium.pl/)[43] – ocena ogólna A+;
- Getin Noble Bank (https://secure.getinbank.pl)[44] – ocena ogólna A+;
- Eurobank (https://online.eurobank.pl/)[45] – ocena ogólna A+ z perspektywą obniżenia oceny do poziomu C;
- Bank Pocztowy (https://www.pocztowy24.pl/)[46] – ocena ogólna A;
- Raiffeisen Polbank (https://moj.raiffeisenpolbank.com/)[47] – ocena ogólna A[48];
- Citi Handlowy (https://www.online.citibank.pl/)[49] – ocena ogólna A;
- T-Mobile Usługi Bankowe (https://online.t-mobilebankowe.pl/)[50] – ocena ogólna A;
- Deutsche Bank (https://dbeasynet.deutschebank.pl/)[51] – ocena ogólna A;
- Plus Bank (https://plusbank24.pl/)[52] – ocena ogólna A;

[39] https://www.ssllabs.com/ssltest/analyze.html?d=aliorbank.pl (dostęp: 31.03.2017).
[40] poziomu zabezpieczeń.
[41] https://www.ssllabs.com/ssltest/analyze.html?d=login.bgzbnpparibas.pl (dostęp: 31.03.2017).
[42] https://www.ssllabs.com/ssltest/analyze.html?d=e-bank.credit-agricole.pl (dostęp: 31.03.2017).
[43] https://www.ssllabs.com/ssltest/analyze.html?d=www.bankmillennium.pl (dostęp: 31.03.2017).
[44] https://www.ssllabs.com/ssltest/analyze.html?d=secure.getinbank.pl (dostęp: 31.03.2017).
[45] https://www.ssllabs.com/ssltest/analyze.html?d=online.eurobank.pl (dostęp: 31.03.2017).
[46] https://www.ssllabs.com/ssltest/analyze.html?d=www.pocztowy24.pl (dostęp: 31.03.2017).
[47] https://www.ssllabs.com/ssltest/analyze.html?d=moj.raiffeisenpolbank.com (dostęp: 31.03.2017).
[48] Bank w raporcie ma wskazanie dotyczące zmiany funkcji skrótu do certyfikatu z SHA1 do SHA2. Na początku roku 2017 firma Google udostępniła dokumenty, z których jasno wynika, iż możliwe są udane, efektywne i praktyczne ataki na funkcję skrótu SHA1.
[49] https://www.ssllabs.com/ssltest/analyze.html?d=www.online.citibank.pl (dostęp: 31.03.2017).
[50] https://www.ssllabs.com/ssltest/analyze.html?d=online.t-mobilebankowe.pl (dostęp: 31.03.2017).
[51] https://www.ssllabs.com/ssltest/analyze.html?d=dbeasynet.deutschebank.pl (dostęp: 31.03.2017).
[52] https://www.ssllabs.com/ssltest/analyze.html?d=plusbank24.pl (dostęp: 31.03.2017).

- BOŚ (https://bosbank24.pl/)[53] – ocena ogólna A[54];
- Santander Consumer Bank (https://online.santanderconsumer.pl/)[55] – ocena ogólna A+ z perspektywą obniżenia oceny do poziomu C.

Podsumowanie

Zmieniające się otoczenie oraz niepewność i związane z nią ryzyko wymusza na organizacjach podejmowanie strategicznych działań. Banki poszukują metod, narzędzi, które zwiększając efektowność działania zminimalizują ryzyka i ich skutki. Jednym z obszarów ciągłego zarządzania jest jakość bezpieczeństwa informacji. Przeprowadzając analizę raportów stwierdzono, że wszystkie banki korzystają z silnego szyfrowania opartego na kluczu o długości 2048 bitów[56]. Szyfrowanie to oparte jest o szyfrowanie asymetryczne RSA. Wykazano również, że banki wspierają bezpieczne protokoły z rodziny TLS, jednocześnie wykluczając przestarzałe już protokoły SSL. Ważne jest, że wspierane protokoły posiadają wszystkie zalecane algorytmy szyfrowania. Należy również dodać, iż serwery poprawnie odrzucają przestarzałych agentów (m.in.: IE 6, IE 8 pracujących na systemie Microsoft XP; środowisko Java 6u45) oraz wspierają systemy mobilne.

Z przeprowadzonej analizy banków funkcjonujących w kraju wynika, że najgorzej z wielkiej piątki wypadła bankowość elektroniczna oferowana przez ING Bank Śląski – ocena B. Obniżenie oceny wynikło z faktu wspierania przez serwer bankowy słabego protokołu Diffiego-Hellmana[57]. Wśród pozostałych banków najgorzej zostały ocenione:

- Credit Agricole Bank Polska – ocena C, obniżenie oceny nastąpiło ze względu na fakt używania szyfru strumieniowego RC4[58] oraz za niewspieranie technologii utajnienia przekazywania[59].
- Eurobank i Santander Consumer Bank – spowodowane jest to zmianami w sys-

[53] https://www.ssllabs.com/ssltest/analyze.html?d=bosbank24.pl (dostęp: 31.03.2017).
[54] Bank w raporcie ma wskazanie dotyczące zmiany funkcji skrótu do certyfikatu z SHA1 do SHA2.
[55] https://www.ssllabs.com/ssltest/analyze.html?d=online.santanderconsumer.pl (dostęp: 31.03.2017).
[56] Dla kluczy asymetrycznych długością sugerowaną jest obecnie 2048 bitów.
[57] Protokół uzgadniania kluczy szyfrujących.
[58] RC4 należy do szyfrów strumieniowych. Używany jest w protokołach, takich jak SSL oraz WEP. Szyfr ten nie jest odporny na kryptoanalizę liniową i kryptoanalizę różnicową. Obecnie jest uznawany za niedostatecznie bezpieczny. Szyfr ten nie jest zalecany do używania w nowych systemach.
[59] Utajnienie przekazywania (ang. Forward Secrecy – FS) jest własnością zabezpieczonych protokołów komunikacyjnych; powoduje ono zabezpieczenie w sytuacji, gdy zostaje złamany tzw. klucz długoterminowy. Złamanie jednak tego klucza nie rodzi dalszych konsekwencji, czyli nie powoduje skompromitowania kluczy użytych w poprzednich sesjach. Jeżeli FS jest wykorzystywany, szyfrowane komunikacje oraz sesje utworzone w przeszłości nie mogą zostać odzyskane i odszyfrowane w przypadku kompromitacji haseł lub kluczy długoterminowych w późniejszymi okresie.

temie klasyfikacji[60] oraz wspieraniem szyfrowania, które nie jest już uznawane za bezpieczne[61].

Należy zauważyć, że Getin Noble Bank jest najbardziej wymagający, jeżeli chodzi o dopuszczone systemy operacyjne.

Reasumując, zielona kłódka i zaufany certyfikat wcale nie oznaczają bezpiecznego kanału informacyjnego. Zbadany też został tylko jeden aspekt bezpieczeństwa – obsługa protokołów szyfrujących po stronie serwera. Każdy kanał zaś ma dwie strony, co za tym idzie ta druga strona (klient) może mieć szereg innych mankamentów, które mogą obniżyć ogólne standardy bezpieczeństwa.

Bibliografia

Capiga M., *Zarządzanie bankami*, Warszawa 2010.

Olkiewicz M., Knowledge management as a determinant of innovation in enterprises, [w:] Proceedings of the 9th International Management Conference. Management and Innovation For Competitive Advantage, Bucharest 2015.

Olkiewicz M., *Zarządzanie jakością w sektorze bankowym w dobie wejścia do Unii E*uropejskiej, [w:] Rynki finansowe w przestrzeni elektronicznej, red. B. Świecka, Szczecin 2004.

Wojciechowska-Filipek S., *Zarządzanie jakością informacji w organizacjach zhierarch*izowanych, Warszawa 2015.

http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-internetowej-iii-kw-2016-6553450.html (dostęp: 31.03.2017).

http://prnews.pl/raporty/raport-prnewspl-rynek-kont-osobistych-iv-kw-2016-6553975.html (dostęp: 31.03.2017).

http://prnews.pl/wiadomosc/raport-prnewspl-rynek-bankowosci-internetowej-iv-kw-2016-6554056.html (dostęp: 31.03.2017).

http://prnews.pl/wiadomosci/raport-prnewspl-liczba-klientow-w-bankach-iv-kw-2016-6554091.html (dostęp: 31.03.2017).

https://blog.qualys.com/ssllabs/2017/01/18/ssl-labs-grading-changes-january-2017 (dostęp: 31.03.2017).

https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide (dostęp: 31.03.2017).

https://www.ietf.org/rfc/rfc5289.txt (dostęp: 31.03.2017).

https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf (dostęp: 22.02.2017).

https://www.ssllabs.com/ (dostęp: 31.03.2017).

https://www.ssllabs.com/ssltest/analyze.html?d=aliorbank.pl (dostęp: 31.03.2017).

https://www.ssllabs.com/ssltest/analyze.html?d=bosbank24.pl (dostęp: 31.03.2017).

https://www.ssllabs.com/ssltest/analyze.html?d=dbeasynet.deutschebank.pl (dostęp: 31.03.2017).

[60] https://blog.qualys.com/ssllabs/2017/01/18/ssl-labs-grading-changes-january-2017 (dostęp: 31.03.2017).

[61] Kara za użycie szyfrowania 3DES w połączeniu z protokołem TLS 1.1 lub nowszym.

https://www.ssllabs.com/ssltest/analyze.html?d=e-bank.credit-agricole.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=inteligo.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=login.bgzbnpparibas.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=login.ingbank.pl&s=193.193.181.208 (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=moj.raiffeisenpolbank.com (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=online.eurobank.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=online.mbank.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=online.santanderconsumer.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=online.t-mobilebankowe.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=orangefinanse.com.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=plusbank24.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=secure.getinbank.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.bankmillennium.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.centrum24.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.ipko.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.online.citibank.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.pekao24.pl (dostęp: 31.03.2017).
https://www.ssllabs.com/ssltest/analyze.html?d=www.pocztowy24.pl (dostęp: 31.03.2017).

Summary

Internet banking is becoming an important part of life in the information society. Risk management in services related to broadly understood e-banking is becoming an extremely important issue, and even a factor determining the existence of a bank in cyberspace. This process must be continually monitored and rapidly modified as new threats are detected. The issue of implementing server-side procedures and their implementation in security is another important issue as well.

With the current development of internet technologies and the dangers of using them, special attention is paid to security - the "green padlock" in the browser does not give 100% certainty in the area of information security. It only tells you that the certificate is secure and has been signed by a trusted authentication center. The "green padlock" also has its security levels that affect the quality of the service provided, since the certificate, friendly application and nice layout of the site will not guarantee the security of the communication channel.

S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 163–173 ROK 2017

ISSN 2543–7321

Małgorzata Beskosty

Akademia Pomorska
Słupsk
menturia@gmail.com

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

INFORMATION SECURITY MANAGEMENT

***Zarys treści*:** Obecnie możemy zaobserwować dynamiczny rozwój przedsiębiorstw nie tylko ze względu na postępującą globalizację, ale także szeroko rozumiany dostęp do nowoczesnych technologii. Wraz z ciągłym rozpowszechnianiem się sieci informacyjnych i telekomunikacyjnych znacznie obniżył się koszt pozyskania informacji, co ma ogromny wpływ na przyspieszenie procesów gospodarczych[1]. Celem niniejszego artykułu jest analiza informacji jako zasobu, przedstawienie charakterystycznych cech systemu bezpieczeństwa informacji, wyjaśnienie takich pojęć, jak informacja, bezpieczeństwo oraz przedstawienie działań wspomagających ochronę informacji w przedsiębiorstwie.
***Słowa kluczowe*:** informacja, ochrona danych, system bezpieczeństwa informacji, zarządzanie
Key words: information, data protection, security of information system, management

Wstęp

Aby sprostać rosnącym wyzwaniom współczesnej gospodarki, ważna jest ochrona i dbanie o jakość zasobów. Pragnę poruszyć więc problem ochrony zasobu, jaki stanowi informacja, co jest o tyle problematyczne, że informacja stale ewoluuje, dlatego, aby mieć nad nią kontrolę, należy wdrożyć w przedsiębiorstwie system ochrony jej bezpieczeństwa. Stanowi to jednak przedsięwzięcie kosztowne, dlatego poprawa ochrony informacji powinna być opłacalna przede wszystkim dla przedsiębiorstwa oraz umacniać bądź zwiększać jego konkurencyjność[2].

[1] Z. Olesiński, *Środowiskowe uwarunkowania zarządzania informacją w małych przedsiębiorstwach*, [w:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, red. R. Borowiecki, J. Czekaj, Warszawa 2010, s. 91.

[2] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006, s. 28.

Czym jest informacja?

Niewątpliwie informacja jest jednym z najważniejszych aktywów firmy. Ona właśnie czyni przedsiębiorstwo wyjątkowym, decyduje o jego wartości, a także o sukcesie lub porażce[3]. Informacją jest komunikat, wiadomość, przekaz lub wskazówka, przekazywane w sposób zrozumiały i płynny za pomocą kodu lub języka. Możemy podzielić informację na trzy typy:

- niezbędną dla funkcjonowania przedsiębiorstwa,
- taką, na której opiera się przewaga konkurencyjna na rynku,
- dotyczącą bezpieczeństwa informacji i ich kontroli[4].

W dzisiejszych czasach „informacja jest kluczem do sukcesu rynkowego i staje się głównym elementem rozwoju gospodarczego”[5]. Dzieje się tak dlatego, że to jedyny zasób, do którego dostęp zapewnia możliwość prognozowania procesów zachodzących na rynku, a także podejmowania odpowiednich działań i reagowania na nie, porównywania czy decyzje podjęte przez przedsiębiorców są właściwe, czy też nie oraz ich dopracowania, co stanowi ogromną wartość dla strategii firmy.

Obecnie przedsiębiorstwa cierpią z powodu natłoku informacji, które niekontrolowane lub niepoprawnie zarządzane mogą spowodować ogromne szkody. Aby prawidłowo zarządzać informacją, należy wiedzieć przede wszystkim, gdzie jej szukać. Podstawowym jej nośnikiem są systemy informatyczne, sprzęt komputerowy, dokumenty papierowe bądź w formie elektronicznej oraz ludzka pamięć. W każdym z tych przypadków mamy do czynienia z ryzykiem utracenia lub dostania się informacji w niepowołane ręce[6]. Informacja zmienia się nieustannie, tak naprawdę trudno jest zdefiniować dzisiaj, co nią nie jest. Rozwój technologii i telekomunikacji spowodował, że ogromne wyzwanie dla przedsiębiorstwa i niejako jego sukces stanowi zapanowanie nad ogromem przepływu informacji, nie mówiąc już o ich usystematyzowaniu, podporządkowaniu i zarządzaniu nimi. Informacja może być dostarczana z wielu źródeł, niekoniecznie wiarygodnych, a ponadto w czasie swojej „wędrówki” może ulegać wielu przekształceniom, a tym samym zmniejsza się jej wartość. Dlatego należy chronić takie atrybuty informacji, jak poufność, dokładność i dostępność[7].

Poufnością informacji nazywamy zdolność do dzielenia się informacją wyłącznie z tymi instytucjami lub grupami osób, którym jest to niezbędne oraz do odmowy dostępu do informacji tym osobom, które nie są do tego powołane. Natomiast dokładność przekłada się na wiarygodność informacji, tzn. mówi o tym, że informacja pochodzi z wiarygodnego i sprawdzonego źródła i wiąże się z jej integralnością, czyli pewnością, że z upływem czasu nie została ona zniekształcona bądź nie straciła swojej pierwotnej wartości wskutek modyfikacji. O dostępności mówimy zaś wtedy, gdy

---

[3] D.L. Pipkin, *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, tłum. E. Andrukiewicz, Warszawa 2002, s. 15.
[4] T. Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Gliwice 2013, s. 14.
[5] Z. Gródek, *Sieci informacyjne dla przedsiębiorczości* – czynnik przewagi konkurencyjnej opartej na informacji, [w:] Zarz*ądzanie zasobami informacyjnymi…*, s. 203.
[6] T. Kifner, *Polityka bezpieczeństwa…*, s. 15.
[7] D.L. Pipkin, *Bezpieczeństwo informacji…*, s. 16.

wszystkie osoby mające pozwolenie na dostęp do danej informacji korzystają z niej, ponieważ należy ona do zasobów informacyjnych przedsiębiorstwa[8].

Pierwszym krokiem zmierzającym do ochrony informacji jest zrozumienie, dlaczego zapewnienie jej bezpieczeństwa jest tak ważne dla całego przedsiębiorstwa. W dobie gospodarki rynkowej nieustannie walczy się o informacje stanowiące o „być albo nie być" firmy, a ujawnienie wrażliwych danych może pociągnąć za sobą poważne straty finansowe.

Polityka bezpieczeństwa w przedsiębiorstwie

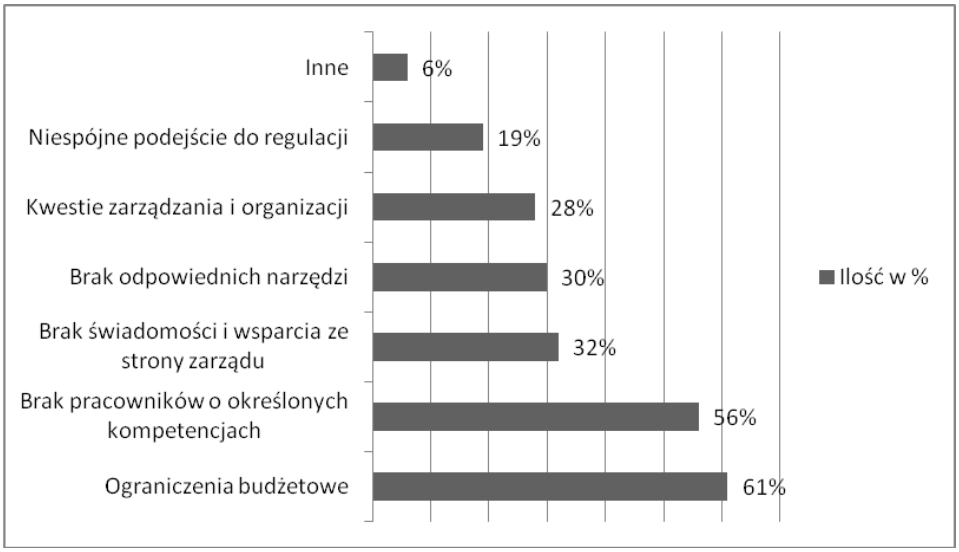
Mówiąc o bezpieczeństwie często mamy na myśli stan, w którym dane dobra są zabezpieczone, tzn. nie istnieje obawa ich utraty. W praktyce stan ten jest niemożliwy, ponieważ nigdy nie będziemy mieć stuprocentowej pewności, że zasoby, takie jak wiedza czy informacja, nie są narażone na ataki lub próby przejęcia. „Zapewnienie bezpieczeństwa jest procesem ograniczenia ryzyka lub prawdopodobieństwa szkody"[9], a, co się z tym wiąże, prowadzenie odpowiedniej polityki bezpieczeństwa służy jedynie stałemu zmniejszaniu bądź ograniczaniu stanu zagrożenia. Wynika więc z tego, że zagrożenie zawsze będzie istnieć. Wprowadzając jednak parę prostych zasad w przedsiębiorstwie, możemy zmniejszyć ryzyko ujawnienia cennych informacji.

Polityka bezpieczeństwa to system zarządzania nie tylko systemami informatycznymi, ale także organizacją i postępowaniem pracowników. To zapewnianie bezpieczeństwa informacji poprzez jasne zakomunikowanie i przedstawienie obowiązujących zasad i reguł pracownikom. Jest to świadome zarządzanie informacją i jej bezpieczeństwem za pomocą zaleceń i procedur, które w sposób klarowny opisują przepływ informacji w przedsiębiorstwie oraz między nim i jego kontrahentami[10]. Działania te powinny być sprecyzowane, przemyślane i skuteczne, a polityka bezpieczeństwa powinna dawać możliwość niezakłóconej pracy przedsiębiorstwa[11]. Podstawowy plan bezpieczeństwa informacji możemy podzielić na:

- analizę skutków finansowych określającą, które procesy w firmie można uznać za krytyczne, czyli niezbędne, aby instytucja przetrwała,
- analizę ryzyka przewidującą prawdopodobieństwo wystąpienia zagrożenia oraz wielkość przewidywanych szkód,
- planowanie działań w sytuacjach kryzysowych wskazujące, co należy zrobić, aby w jak najszybszy sposób przywrócić w przedsiębiorstwie stan sprzed incydentu,
- planowanie utrzymania ciągłości działania określające, co należy zrobić, aby pomimo sytuacji nadzwyczajnych oraz niezależnie od nich przedsiębiorstwo mogło dalej funkcjonować[12].

[8] Tamże, s. 16.
[9] Tamże, s. 17.
[10] T. Kifner, Polityka *bezpieczeństwa…*, s. 26.
[11] A. Białas, *Bezpieczeństwo informacji i usług…*, s. 34–35.
[12] D.L. Pipkin, *Bezpieczeństwo informacji…*, s. 19.

Bardzo ważne jest, aby dostrzec, że współczesna gospodarka i stopień zaawansowania technologii nie pozwalają na postrzeganie bezpieczeństwa jako możliwości, lecz jako niezbędnej konieczności, aby przedsiębiorstwo przetrwało. Bezpieczeństwo stanowi dzisiaj gwarancję gospodarczego postępu, dlatego plan bezpieczeństwa informacji powinien być ściśle związany z podstawowymi założeniami działania firmy oraz czynnościami kontrolnymi. Ważna jest również współpraca kadry zarządzającej. Powinna być ona świadoma zagrożeń oraz przygotowana na ewentualne reakcje niezbędne do ochrony zasobów.



Rys. 1. Główne przyczyny ograniczeń w zapewnianiu bezpieczeństwa informacji
Fig. 1. The main reasons of restrictions while providing information security

Źródło: Raport EY: Rośnie świadomość cyberzagrożeń, lecz firmom wciąż brakuje spójnego podejścia do bezpieczeństwa systemów informatycznych, EY, 13 stycznia 2017 www.ey.com/pl/pl/newsroom/news-releases/news-ey-20170113-swiatowe-badanie-bezpieczenstwa-informacji/ (dostęp: 14.03.2017).

Zarządzanie systemem bezpieczeństwa

Często bagatelizuje się wartość, jaką dla przedsiębiorstwa ma bezpieczeństwo, czego następstwem jest brak jakichkolwiek zabezpieczeń. Ten model „ochrony" może mieć wiele przyczyn, natomiast zazwyczaj wiąże się z brakiem finansów, czasu bądź po prostu z nieodpowiednim podejściem kadry zarządzającej. Prowadzi to do całkowitej bezczynności w sferze zabezpieczeń, gdyż przedsiębiorstwo, stanowiąc potencjalnie mało interesujący obiekt ataków, rezygnuje z jakichkolwiek form ochrony, wierząc, że bardziej zagrożone są firmy konkurencyjne. Ten model zabezpieczeń jest ryzykowny i w dłuższej perspektywie czasu nieopłacalny, gdyż straty, jakie ponosi się wskutek naruszenia dóbr firmy okazują się o wiele większe,

a przedsiębiorstwo może ponosić jego konsekwencje jeszcze długo po wyciszeniu sprawy[13].

Nieco lepszy jest model ochrony niektórych jednostek organizacyjnych, z punktu widzenia ekonomicznego bardziej opłacalny, natomiast niedający pewności, że dobra firmy nie zostaną utracone. Przedsiębiorstwo skupia się na zabezpieczeniu jedynie wybranych środków lub jednostek, stosując jednocześnie różne manewry mające na celu zmylenie potencjalnych włamywaczy, np. uwydatniając i wskazując najmocniejsze strony zabezpieczeń jako słabe[14].

Oczywiście, cel każdej firmy stanowi możliwość stworzenia ogólnego systemu zabezpieczeń obejmującego wszystkie sektory przedsiębiorstwa. Jest to niestety proces bardzo kosztowny, długotrwały i zawiły, w dzisiejszych czasach jednak konieczny[15].

Polityka bezpieczeństwa powinna obejmować stały dostęp do informacji i zarządzanie nią oraz przyczyniać się do ciągłego aktualizowania zmian i procedur systemu bezpieczeństwa. Nie bez znaczenia są także pracownicy, którzy powinni ponosić odpowiedzialność za wyznaczony im zakres bezpieczeństwa informacji. Polityka bezpieczeństwa każdego przedsiębiorstwa powinna charakteryzować się starannością w obsłudze sprzętu komputerowego, dbałością o miejsca pracy i ich zabezpieczanie, a także o możliwie jak największe zminimalizowanie błędów ludzkich. Te wszystkie elementy mają realny wpływ na politykę bezpieczeństwa, dlatego powinny podlegać uwadze kierownictwa przedsiębiorstwa i być wynikiem planowanych działań, a nie przypadku. Ponadto, aby uchronić dane wrażliwe firmy przed wypływem na zewnątrz, należy przechowywać je w sejfach lub miejscach pilnie strzeżonych. Aby firma mogła skutecznie chronić swoje zasoby, musi dokładnie zdawać sobie sprawę z ich wartości i ilości, dlatego należy na bieżąco prowadzić rejestr zakupionych urządzeń, sprzętu, oprogramowania i zaopatrzenia biurowego.

Ogólnie rzecz ujmując, możemy wyróżnić w planie bezpieczeństwa informacji pięć elementów. Pierwszym z nich jest inspekcja, czyli oszacowanie aktualnych zdolności przedsiębiorstwa, poziomu bezpieczeństwa i zależności występujących między zasobami a funkcjami firmy. Kolejny etap stanowi ochrona. Są to wszelkie działania zmierzające do zmniejszenie ryzyka utraty danych bądź przerwania ciągłości pracy firmy. Może to być tworzenie kopii zapasowych danych krytycznych firmy, kupno dodatkowego sprzętu lub oprogramowania, zwiększenie liczby dostawców. Na tym etapie podejmowane są decyzje, jakiej ochrony potrzeba, co należy chronić i jaki sposób wdrożyć planowany system bezpieczeństwa. Następne w kolejności jest wykrywanie, czyli monitorowanie zmian zachodzących w systemach i wyłapywanie tych uznanych za podejrzane. Może się jednak okazać, że system wykryje działania niepożądane lub dojdzie do próby włamania. Wtedy kluczowa okazuje się reakcja. To od niej zależy, czy przedsiębiorstwo przerwie pracę i na jak duże narazi się straty. W celu jak najszybszej reakcji opracowuje się plan awaryjny, w którym definiuje się, jaki powinien być odzew na zaistniały atak, dokumentuje się, a następnie testuje

[13] T. Kifner, *Polityka bezpieczeństwa…*, s. 31.
[14] Tamże.
[15] Tamże, s. 33.

daną odpowiedź, aby w czasie kryzysu nie budzić paniki i postępować według planu. Ostatnim etapem, nie mniej istotnym, jest refleksja. Po zażegnaniu niebezpieczeństwa przychodzi czas na podjęcie wszelkich kroków mogących udoskonalić plan ochrony informacji, ocenę dokonanych działań i dalszy rozwój. Dlatego tak ważne jest, aby opracować ogólny kierunek bezpieczeństwa i koordynować wszelkie procedury i zasady z nim związane[16].

Organizacja firmy

Przedsiębiorstwa, chcąc zaistnieć na rynku światowym i zapewnić sobie przewagę konkurencyjną, podejmują coraz to nowe wyzwania obejmujące gromadzenie wiedzy i umiejętne gospodarowanie nią[17]. Aby wdrażany system bezpieczeństwa był skuteczny, należy przede wszystkim opierać się na wiedzy ludzi, którzy są specjalistami w swoich dziedzinach. Trzeba jednak wziąć również pod uwagę, że zarządzanie wiedzą nie stanowi rozwiązania wszystkich problemów przedsiębiorstwa, jest natomiast idealnym instrumentem doskonalącym jego funkcjonowanie[18].

O ile zabezpieczenie papierowej dokumentacji czy też wydruków nie wymaga większych umiejętności, o tyle dobór optymalnego dla przedsiębiorstwa systemu informatycznego, oprogramowania czy systemu kodowania nie jest już rzeczą tak zwykłą i prostą. Jeśli zależy nam na całościowej ochronie informacji, niezbędne jest powierzenie tego zadania odpowiednim ludziom, którzy wezmą pełną odpowiedzialność za powzięte decyzje. Dlatego często zaleca się zorganizowanie w strukturze przedsiębiorstwa odrębnej komórki organizacyjnej, która zajmuje się bezpieczeństwem[19]. Nie bez znaczenia jest także oficjalne zatwierdzenie systemu oraz wprowadzanych w nim zmian. Ma to na celu nie tylko uświadomienie pracownikom wagi przedsięwzięcia, jakim jest ochrona informacji, ale także uniknięcie niepotrzebnych nieporozumień mogących się pojawić w przyszłości. Zatwierdzanie wszelkich działań przez zarząd podkreśla także ich znaczenie i zmusza do wywiązywania się z podjętych zadań. Bezwzględną koniecznością jest w takim wypadku powołanie komisji ds. bezpieczeństwa, której zadaniem byłaby kontrola przestrzegania wdrożonych procedur oraz konstruktywna krytyka zastanej sytuacji. Kontrole te powinny odbywać się systematycznie, aby zapewnić ciągłość systemu bezpieczeństwa i na bieżąco korygować zachowania odbiegające od pożądanych działań. Tylko w taki sposób zatwierdzony system ma szansę przetrwać i rozwijać się. Kontrola raportów i protokołów sporządzanych przez odpowiednich pracowników daje możliwość oceny realnej sytuacji i wprowadzenia ewentualnych poprawek. Równie niezbędny jest tu kontakt między komisją a kierownictwem kontrolowanego działu, który również

[16] D.L. Pipkin, *Bezpieczeństwo informacji…*, s. 20–21.
[17] W.M. Grudzewski, I. Hejduk, *Systemy zarządzania wiedzą warunkiem wzrostu wartości firmy*, [w:] *Współczesne źródła wartości przedsiębiorstwa*, red. B. Dobiegała-Korona, A. Herman, Warszawa 2006, s. 244.
[18] B. Siuta-Tokarska, *Zarządzanie wiedzą jako czynnik rozwoju współczesnej organizacji*, [w:] *Zarządzanie zasobami informacyjnymi…*, s. 108.
[19] T. Kifner, *Polityka bezpieczeństwa…*, s. 35.

podlegałby nadzorowi. Takie rozwiązanie daje poważną przewagę w samoorganizacji i zarządzaniu bezpieczeństwem i świadczy o zamiarze prowadzenia dalekosiężnej polityki.

Do obowiązków kadry zarządzającej należy także delegowanie uprawnień, czyli powierzanie podległym pracownikom zadań oraz odpowiedzialności za nie. Jest to warunek efektywnego zarządzania z tego względu, że pracownicy również wpływają na osobisty sukces kierowników. By zarząd mógł pełnić funkcje kierownicze, wymaga się od jego członków szerokiego zakresu wiedzy i kompetencji[20]. Obecnie zarządzanie jest raczej wyrazem ciągłego adaptowania się do postępujących zmian. Nie walczy się już o stabilność, lecz o rozwój i zmianę[21]. W związku z tym nieodzowna jest zarówno współpraca kierownictwa, jak i odpowiedni dobór kadry. Na kierownictwie ciąży obowiązek utrzymywania stabilności wprowadzonego systemu bezpieczeństwa oraz prognozowanie możliwych zmian technologicznych i strukturalnych mających wpływ na przedsiębiorstwo. Kierownictwo, wyrażając publicznie wolę przestrzegania procedur, informując o intencjach i wspierając pracowników w obowiązkach, pozwala im także przyzwyczaić się do nowych warunków, co znacznie usprawnia działanie przedsiębiorstwa. To również od kierownictwa zależy przepływ informacji. Powinno ono ustalić poziom dostępu do informacji poszczególnych działów firmy, aby zminimalizować ryzyko ujawnienia wrażliwych danych. Dotychczas często stosowano model pionowy, tzn. dostęp do informacji był taki sam dla przełożonych, jak i dla pracowników. Stwarza to ogromne ryzyko, gdyż osoby, które nie orientują się w informacjach, do których mają dostęp, nie są też w stanie zweryfikować ich wartości. Znacznie lepszym rozwiązaniem jest macierzowy dostęp do informacji, który charakteryzuje się dostępem do informacji szczegółowych, związanych bezpośrednio z wykonywaną pracą, zatem ograniczeniem przepływu informacji do minimum i ulepszeniem ochrony systemu informacyjnego[22].

Kolejne zagadnienie stanowi dobór kadry. Niezależnie od tego czy mówi się o kadrze zarządzającej czy o innych pracownikach, nie mogą być to ludzie przypadkowi. Zatrudnienie pracownika powinno wiązać się z przeprowadzeniem testów wiedzy czy doświadczenia lub badaniem skłonności psychicznych, zasad moralnych itd. W przedsiębiorstwie nastawionym na bezpieczeństwo informacji to od nich właśnie będzie zależeć poziom bezpieczeństwa, dlatego, obsadzając takie stanowiska, jak inspektor bezpieczeństwa czy administrator, szczególną uwagę powinniśmy zwrócić na wykształcenie. Innym problemem jest częste pomijanie pracownika jako integralnej części firmy. O wiele prostszym rozwiązaniem będzie przeszkolenie go w stosowaniu zasad bezpieczeństwa niż zakup skomplikowanego oprogramowania do gospodarowania dokumentami[23]. Istotą działania jest zaangażowanie pracownika w sprawy firmy poprzez zatrudnienie na umowę stałą, przeprowadzanie szkoleń, po-

[20] P. Bartkowiak, D. Sobczyński, B. Płokarz, *Zintegrowany system zarządzania a przepływ info*rmacji, [w:] Za*rządzanie zasobami informacyjnymi…*, s. 84.

[21] W.M. Grudzewski, I. Hejduk, *Kierunki zmian w systemie zarządzania,* [w:] Wyzwania bezpie*czeństwa cywi*lnego XXI wieku – *inżynieria działań w obszarach nauki, dydaktyki i praktyki*, red. B. Kosowski, A. Włodarski, Warszawa 2007, s. 69.

[22] T. Kifner, *Polityka bezpieczeństwa…,* s. 37–38.

[23] Tamże, s. 40.

zwalających wyeliminować prawdopodobieństwo popełniania błędów. Informowanie o wchodzących zmianach w systemie czy zapoznanie z nowymi jego elementami z odpowiednim wyprzedzeniem pozwoli pracownikom oswoić się z nową sytuacją i przez to wpłynie na ich bardziej efektywną pracę. Ciągła edukacja pracowników, inwestowanie w ich rozwój jest także inwestycją w rozwój przedsiębiorstwa i gwarantem jego elastyczności i niepodzielności.

Zakończenie

Ochrona informacji w warunkach współczesnej gospodarki stanowi poważne wyzwanie dla rozwijających się przedsiębiorstw i powinna być zagadnieniem stale poruszanym przy omawianiu problematyki zmieniającego się rynku. Ogrom przepływu informacji między firmami, kontrahentami i światem zewnętrznym jest zjawiskiem powszechnym i pożądanym, ale także niebezpiecznym, jeżeli nie podejmuje się działań wspierających politykę bezpieczeństwa. Dany system bezpieczeństwa informacji obejmuje poza odpowiednim oprogramowaniem, sprzętem i zasobami materialnymi także pracowników, których przeszkolenie oraz przygotowanie w zakresie ochrony informacji znacznie zwiększa poziom bezpieczeństwa w przedsiębiorstwie.

Bibliografia

Bartkowiak P., Sobczyński D., Płokarz B., *Zintegrowany system zarządzania a przepływ informacji*, [w:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, red. R. Borowiecki, J. Czekaj, Warszawa 2010.

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006.

Gródek Z., *Sieci informacyjne dla przedsiębiorczości – czynnik przewagi konkurencyjnej opartej na informacji*, [w:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, red. R. Borowiecki, J. Czekaj, Warszawa 2010.

Grudzewski W.M., Hejduk I., *Kierunki zmian w systemie zarządzania*, [w:] *Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, dydaktyki i praktyki*, red. B. Kosowski, A. Włodarski, Warszawa 2007.

Grudzewski W.M., Hejduk I., *Systemy zarządzania wiedzą warunkiem wzrostu wartości firmy*, [w:] *Współczesne źródła wartości przedsiębiorstwa*, red. B. Dobiegała-Korona, A. Herman, Warszawa 2006.

Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Gliwice 2013.

Olesiński Z., *Środowiskowe uwarunkowania zarządzania informacją w małych przedsiębiorstwach*, [w:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, red. R. Borowiecki, J. Czekaj, Warszawa 2010.

Pipkin D.L., *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, tłum. E. Andrukiewicz, Warszawa 2002.

Siuta-Tokarska B., *Zarządzanie wiedzą jako czynnik rozwoju współczesnej organizacji*, [w:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, red. R. Borowiecki, J. Czekaj, Warszawa 2010.

Raport EY: Rośnie świadomość cyberzagrożeń, lecz firmom wciąż brakuje spójnego podejścia do bezpieczeństwa systemów informatycznych, EY, 13 stycznia 2017 www.ey.com/pl/pl/newsroom/news-releases/news-ey-20170113-swiatowe-badanie-bezpieczenstwa-informacji/(dostęp: 14.3.2017).

Summary

The purpose of this article is to present the question of effective protection of information security management. The article begins with an explanation of the concept what the information is, its attributes and features. Moreover, the paper describes the models of security systems and the security policy in a company. Besides, the author shows what measures should be applied to manage information and what to do to implement security system which is both efficient and permanent.

STUDIA NAD BEZPIECZEŃSTWEM

NR 2 ss. 173–176 ROK 2017

ISSN 2543–7321

Bolesław Sprengel
Katarzyna Amrozy

Uniwersytet Mikołaja Kopernika
Toruń
ebsprengel@wp.pl
katarzynaamrozy@wp.pl

RECENZJA KSIĄŻKI

Joanna i Rafał Pasztelańscy, *Policjanci. Za cenę życia*

„Ja, obywatel Rzeczypospolitej Polskiej, świadom podejmowanych obowiązków policjanta, ślubuję: służyć wiernie Narodowi, chronić ustanowiony Konstytucją Rzeczypospolitej Polskiej porządek prawny, strzec bezpieczeństwa Państwa i jego obywateli, nawet z narażeniem życia”[1] – tak brzmią pierwsze słowa policyjnej roty, składanej przed podjęciem służby przez policjantów. Te słowa również znajdują się na początku książki małżeństwa Pasztelańskich *Policjanci. Za cenę życia* oraz towarzyszą czytelnikowi podczas jej lektury.

Jest to zbiór dziewięciu reportaży. Wszystkie opisują przypadki policjantów, którzy stracili życie – nie tylko w trakcie czynnej służby, ale także w czasie wolnym od pełnienia obowiązków. W rozpoczynającym publikację prologu Joanna Pasztelańska stwierdza: „Będzie trochę hołdem, trochę rozliczeniem z przeszłością”[2]. By zrelacjonować wydarzenia, autorzy sięgają nie tylko do oficjalnych źródeł, takich jak opinie ekspertów, zapiski z sekcji zwłok, komunikaty, orzeczenia sądowe, ale przede wszystkim do wspomnień świadków tych tragicznych wydarzeń – kolegów, bliskich, członków rodziny. To na tej podstawie kreślą portrety poszczególnych policjantów oraz całej formacji.

Historie zostały zilustrowane zdjęciami oraz krótkim podsumowaniem policyjnej kariery funkcjonariusza. Na końcu książki znajduje się swoista księga pamięci, zawierająca nazwiska zmarłych policjantów i policjantek, list prezesa zarządu Fundacji Pomocy Wdowom i Sierotom po Policjantach, Ireny Zając, a także krótki fragment poświęcony funkcjonariuszom poległym na służbie w II RP.

---

[1] Art. 27 ustawy z dnia 6 kwietnia 1990 roku o Policji (Dz.U. 1990, nr 30, poz. 179, z późn. zm.).
[2] J. Pasztelańska, R. Pasztelański, *Policjanci. Za cenę życia*, Społeczny Instytut Wydawniczy Znak, Kraków 2016, s. 7.

Z pewnością wyodrębnienie tylko dziewięciu historii było trudnym wyzwaniem. Jakie bowiem powinny być kryteria wyboru? Joanna i Rafał Pasztelańscy skupili się na różnych aspektach policyjnej rzeczywistości. Niektóre sprawy, takie jak chociażby akcja w Magdalence, są obecne w medialnej debacie o policji do dzisiaj, inne pokazują zmiany, które nastąpiły od początku lat dziewięćdziesiątych ubiegłego wieku oraz zwracają uwagę na ówczesne błędy. Natomiast część zdarzeń uświadamia, że na przebieg służby policyjnej wpływa nie tylko profesjonalizm, umiejętności czy osobowość, ale także przypadek i znalezienie się w niewłaściwym czasie i miejscu.

Marek Sienicki – zmarł w wyniku postrzelenia przez złodziei w Bytomiu. Robert Stefanik – nie przeżył upadku w trakcie pokazów lotniczych w Inowrocławiu. Marek Cekała – ofiara porachunków polskiej mafii, zastrzelony w Mikołajkach. Andrzej Werstak, Wiktor Będkowski, Bartłomiej Kulesza – ponieśli śmierć z ręki więziennego strażnika z Sieradza. Justyna Zawadka, Tomasz Twardo – zginęli w wypadku samochodowym po tym, gdy przewozili służbowym autem nieupoważnioną osobę na polecenie warszawskiego komendanta. Mirosław Żak, Marian Szczucki, Dariusz Marciniak – brali udział w strzelaninie w Parolach i Magdalence. Piotr Molak – nie przeżył wybuchu ładunku bombowego na stacji paliw w Warszawie. Andrzej Struj – zasztyletowany przez chuligana, również w Warszawie. Marek Dziakowicz – wałbrzyski policjant, który utonął próbując uratować młodego człowieka.

Takich wydarzeń jest więcej. Rafał Pasztelański komentuje to następująco: „Kolejne artykuły o niedofinansowaniu stróżów prawa, o złych przepisach, bzdurnych pomysłach czy robieniu prywatnych folwarków z jednostek policji nie robiły na kolejnych władzach większego wrażenia”[3]. Czasami musiało dojść do tragedii, by zostały podjęte odpowiednie kroki pozwalające zapewnić bezpieczeństwo tym, którzy na co dzień za nie odpowiadają. Jeden z rozmówców gorzko stwierdził, że odpowiedni sprzęt był cenniejszy niż obsługujący go funkcjonariusz. Rozpoczynający książkę reportaż zwraca uwagę na to, jaka była polska policja w trakcie transformacji po okresie funkcjonowania milicji i PRL-u. Zmieniła się nie tylko sama formacja, regulacje prawne, ekipy rządzące, ale także społeczeństwo. Rosnący wzrost zaufania obywateli do policji jest chyba najlepszym tego przykładem.

Pisząc o tak bolesnych przeżyciach, trudno czasami uniknąć patosu i gloryfikowania zmarłego. Choć autorzy nieustannie podkreślali, że zmarli policjanci byli tylko ludźmi, mającymi swoje wady, można odnieść wrażenie idealizowania ich jako funkcjonariuszy. Przeszkadza również teoretyzowanie na temat tego, o czym mogli myśleć bohaterowie historii przed śmiercią. Reportaż różni się od naukowej publikacji, jednak nie oznacza to, że można stosować w nim takie niepotwierdzone domysły.

Nie zostało to wprost nazwane, jednak w książce *Policjanci. Za cenę życia* można było zaobserwować elementy kultury policyjnej, takie jak poczucie solidarności (według stwierdzenia, że policjant nigdy nie będzie sam), specyficzny sposób postrzegania rzeczywistości, żargon, relacje z przełożonymi i osobami spoza Policji. To jednocześnie próba pokazania policyjnych realiów szerszemu gronu odbiorców, nie tylko spośród osób mundurowych. Wybór akurat takiej tematyki miał służyć za-

[3] Tamże, s. 8–9.

akcentowaniu trudów służby, która nie zawsze jest tak kolorowa, jak pokazują popularne filmy lub co można wyczytać w kryminałach.

„Nie zdążył się pożegnać, zostawił płaczącą wdowę. Bo śmierć ma wliczoną w ryzyko zawodowe. Miał pogrzeb na koszt państwa i pośmiertny awans. Ból serca bliskich, a przesłanie dla Was: »Obudźcie się ludzie i przejrzyjcie na oczy. Jesteśmy tacy jak Wy i może to Was zaskoczy«"[4] – zacytowany fragment piosenki, autorstwa policjanta z Oddziału Prewencji Olsztyn, został również umieszczony w książce *Policjanci. Za cenę życia*. Skłania on do refleksji nad tym, dlaczego, mimo wielu trudów i niedogodności, ludzie wciąż chce wstępować w szeregi Policji i służyć na rzecz bezpieczeństwa.

Bibliografia

Pasztelańska J., Pasztelański R., *Policjanci. Za cenę ży*cia, Kraków 2016.

Ustawa z dnia 6 kwietnia 1990 roku o Policji (Dz.U. 1990, nr 30, poz. 179, z późn. zm.).

Kowalewski M., Kurs T., *Biały kask, czarna pała* – rapowany hymn policji, http://wiadomosci.gazeta.pl/wiadomosci/1,114873,3892305.html (dostęp: 04.01.2017) .

[4] M. Kowalewski, T. Kurs, *Biały kask, czarna pała* – rapowany hymn Policji, http://wiadomosci.gazeta.pl/wiadomosci/1,114873,3892305.html (dostęp: 4.1.2017).

SPIS TREŚCI