FAE Policy Paper
nr 7/2014

Andrzej KOZŁOWSKI

Cyberbezpieczeństwo infrastruktury energetycznej

Latem ub. roku w sieci jednego z największych przedsiębiorstw energetycznych wykryto wirusa, który zainfekował ponad 30 tys. komputerów. W następstwie tego zdarzenia maszyny te zostały odcięte od internetu. Szkodliwe oprogramowanie doprowadziło do utraty danych, co na pewien czas sparaliżowało działanie przedsiębiorstwa. Powyższy atak był sygnałem alarmowym, jak poważne zagrożenie dla sektora energetycznego (kluczowego dla funkcjonowania każdego wysokorozwiniętego państwa), niosą cyberataki. Problem ten stanowi zagrożenie niezależnie od długości i szerokości geograficznej i tym samym powinien zostać również szczegółowo przeanalizowany w Polsce.

Upowszechnienie się internetu na początku lat 90. zrewolucjonizowało każdy aspekt współczesnego świata i miało również wpływ na bezpieczeństwo państwa oraz jego infrastruktury krytycznej. Wprowadzenie nowych systemów kontrolujących wydobycie i dystrybucję ropy i gazu oraz powszechna automatyzacja w sektorze energetycznym spowodowała wzrost efektywności produkcji, ale jednocześnie wzrastało ryzyko wystąpienia nowego zagrożenia – cyberataku.

Śledząc rozwój zagrożeń w cyberprzestrzeni, należy wskazać, że początkowo cyberataki przeprowadzane były przez pojedynczych hakerów, motywowanych chęcią sprawdzenia swoich umiejętności oraz zdobycia pieniędzy. Ich działalność była raczej nieszkodliwa i nie zagrażała najważniejszym sektorom gospodarki państwa. Wśród poważniejszych operacji wymierzonych przeciwko sektorowi energetycznemu można wymienić m.in. włamanie do Departamentu Energetyki USA, dokonane pod koniec lat 80. ub. wieku przez „hakerów z Hanoweru" działających na zlecenie KGB. Zdecydowanie większe zagrożenie dla infrastruktury energetycznej przyniósł wiek XXI, kiedy to wykorzystaniem cyberprzestrzeni do realizowania własnych interesów zainteresowały się państwa oraz zorganizowane grupy przestępcze.

Obecnie cyberataki są powszechne, dobrze zorganizowane, a co najważniejsze – bardzo skuteczne. Dodatkowo, obserwujemy ich stałą ewolucję, przez co niezwykle trudno jest przewidywać, w jakim kierunku pójdzie zagrożenie, a brak ich identyfikacji uniemożliwia wdrożenie odpowiednich środków zapobiegawczych.

Podatność sektora energetycznego na ataki w cyberprzestrzeni

Z roku na rok rośnie liczba ataków, wymierzonych przeciwko sektorowi energetycznemu. Potwierdzają to raporty przygotowane przez różnorodne instytucje. Według zespołu ICS-CERT (*Industrial Control System-Cyber Emergency Response Team*) Departamentu Bezpieczeństwa Wewnętrznego USA, odpowiedzialnego za reagowanie na incydenty komputerowe przeciwko infrastrukturze krytycznej, w 2011 roku zanotowano 198 cyberataków. Stanowi to czterokrotny wzrost w porównaniu do roku poprzedniego. 41 proc. z nich było skierowanych przeciwko systemom i sieciom komputerowym sektora energetycznego. 67 proc. użytkowników zostało zaatakowanych za pomocą metody „brute force"[1], a 61 proc. stało się ofiarą złośliwego oprogramowania. W tym samym roku przeprowadzano również badania wśród 150 przedsiębiorstw sektora energetycznego. Pokazały one, że ponad tuzin z nich zmaga się z codziennymi próbami ataków.

Wiele czynników składa się na podatność systemu energetycznego na cyberataki. Wśród nich można wymienić:

- Popularność systemów SCADA (*Supervisory Control And Data Acquisition*), czyli systemów nadzorujących przebieg procesu technologicznego oraz produkcyjnego. Używane są one do kontrolowania gazociągów i ropociągów oraz sieci elektrycznych. Powszechnie uważane są za podatne na ataki hakerów, które stają się coraz częstsze. Dobrze obrazuje to przykład kanadyjskiej firmy energetycznej Telvent – operatora ponad połowy gazociągów i ropociągów w Ameryce Północnej i Łacińskiej, której systemy SCADA zostały zhakowane w 2012 roku. Zdaniem przedstawicieli firmy napastnicy, którzy stali za tymi działaniami, zyskali możliwość przeprowadzenia akcji sabotażu.

- Powszechne korzystanie z podwykonawców – większość głównych firm energetycznych korzysta z usług podwykonawców, którymi są najczęściej niewielkie przedsiębiorstwa nie mające funduszy ani możliwości wprowadzenia odpowiednich zabezpieczeń. Systemy komputerowe dużych firm energetycznych i podwykonawców są ze sobą połączone, co znacznie ułatwia hakerom przeprowadzenie skutecznej operacji.

[1] Ataki typu „brute force" polegają na sprawdzeniu każdej możliwej konfiguracji w celu znalezienia rozwiązania.

- **Wysokie koszty bezpieczeństwa** – cześć przedsiębiorstw kalkuluje, że wprowadzenie drogich programów oraz zatrudnienie ekspertów jest nieopłacalne i znacznie taniej wychodzi naprawa zniszczeń, niż wdrażanie środków zapobiegawczych. Prowadzi to do sytuacji, w której przedsiębiorcy nie wiedzą, że są celem ataków, a nie niepokojeni hakerzy mogą przez lata cieszyć się dostępem do sieci i wykradać informacje.
- **Użytkowanie personalnych urządzeń przenośnych**. Wiele przedsiębiorstw dopuszcza korzystanie przez ich pracowników z własnych, prywatnych urządzeń przenośnych. Stanowią one doskonały cel dla hakerów.
- **Wykorzystywanie własnego oprogramowania**, często niezabezpieczonego właściwie, co zwiększa podatność na ataki.
- **Element ludzki –** wciąż jeszcze w sektorze energetycznym wiedza na temat bezpiecznego użytkowania Internetu stoi na bardzo niskim poziomie. Pracownicy używają prostych haseł czy też przeglądają podejrzane strony internetowe w pracy.

Rodzaje ataków i ich motywacja

Sektor energetyczny atakowany jest przy użyciu wielu różnorodnych metod, jedne z nich są stosunkowo proste i nieskomplikowane, inne wymagają długiego przygotowania oraz posiłkowania się inżynierią społeczną. Różne są również motywacje napastników.

Stosunkowo najmniejsze zagrożenie związane jest z działalności *haktywistów* – politycznych aktywistów w sieci, którzy za pomocą prostych ataków DDoS[2] czy Web Defacement[3] manifestują swoje poglądy polityczne, a często sprzeciw wobec poczynań koncernów energetycznych. Służą temu również włamania do systemów komputerowych w celu poszukiwania informacji. Najczęściej operacje te przeprowadzane są przez ekologów, którzy zarzucają firmom z sektora energetycznego brak poszanowania dla środowiska naturalnego. Przykładem takiej akcji jest sprzeciw grupy hakerów, powiązanych z globalnym ruchem Anonymous, którzy w 2012 roku ukradli tysiące e-maili oraz danych personalnych klientów

[2] Distributed Denial of Service (DDoS) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania, poprzez zajęcie wszystkich wolnych zasobów.
[3] Web Defacement – atak, którego celem jest zmiana zawartości strony internetowej.

w celu wyrażenia sprzeciwu wobec polityki najważniejszych koncernów energetycznych w Arktyce.

Zagrożeniem, które stosunkowo rzadko pojawia się w różnorodnych analizach, jest szkodliwa działalność pracowników przedsiębiorstw z sektora energetycznego, którzy posiadają dostęp do najważniejszych informacji i mogą je wykorzystać na szkodę swojego pracodawcy publikując te dane, sprzedając je konkurencji lub po prostu je niszcząc. Osoby te mogą być motywowane chęcią zemsty, lub też zostać opłacone przez konkurencję. Tego typu wewnętrzne przecieki stanowiły ponad połowę naruszeń bezpieczeństwa, według badań przeprowadzonych przez PricewaterhouseCoopers.

Drugim zdecydowanie poważniejszym rodzajem działań, które jest znacznie bardziej szkodliwe, jest działalność szpiegowska oraz idąca z nią w parze kradzież własności intelektualnej. W obecnym świecie informacja stała się towarem jak każdy inny, a większość danych ma postać cyfrową. Stad olbrzymie zainteresowania danymi personalnymi klientów, strategiami rozwoju, informacjami geologicznymi, dokładnymi mapami czy prognozami o przyszłości rynku energetycznego. Duże zainteresowanie wzbudzają również nowoczesne technologie, takie jak technologia szczelinowania, pozwalająca na pozyskiwanie gazu z łupków. Większość z tych danych ma olbrzymie znaczenie dla firm z tej branży, dlatego też hakerzy wchodzący w ich posiadanie mogą liczyć na duże zyski.

Szpiegostwo i kradzież danych mogą być dokonywane przez osoby działające na rzecz państw, konkurencji lub niezależnych hakerów, którzy później oferują skradzione dane podmiotowi, który zaoferował największą sumę pieniędzy. Przykładów takiej działalności jest bardzo wiele. Ostatni raport firmy CrowdStrike z 2013 r. szczególnie akcentuje działalność tzw. „elektronicznych niedźwiedzi", blisko związanych z Kremlem. Ich głównym obiektem zainteresowania było szpiegowanie zachodnich firm z sektora energetycznego, co nie stanowi zaskoczenia, biorąc pod uwagę zależność rosyjskiej gospodarki od eksportu ropy i gazu. Informacje dostarczone przez „elektroniczne niedźwiedzie" z pewnością ułatwią planowanie kolejnych inwestycji strategicznych przez Gazprom i Rosnieft.

Zdecydowanie najpoważniejszymi i mającymi największe skutki są próby dokonania sabotażu, poprzez cyberatak na infrastrukturę krytyczną. Najczęściej są one dokonywane przez wyspecjalizowane jednostki hakerów, wyszkolone i wyekwipowane przez państwa. Jednym

z najpoważniejszych w skutkach cyberataków był *blackout* z 2003 roku w Stanach Zjednoczonych, który dotknął północnowschodnie i środkowe regiony kraju. Ponad 50 milionów osób zostało wówczas odciętych od dostaw prądu. W niektórych regionach stan ten trwał przez dwa dni. Początkowo uznano, że był to wypadek spowodowany błędem oprogramowania systemu kontrolnego korporacji FirstEnergy w Ohio. W 2007 roku były agent CIA Tom Donahue oraz Tim Bennett, ekspert ds. cyberbezpieczeństwa, przyznali, że *blackout* z 2003 roku został spowodowany przez chińskich hakerów, którzy przejęli kontrolę nad system kontrolnym sieci energetycznych. W wyniku ich działania zginęło ponad 11 osób, a straty szacowane były na miliony dolarów. Był to przykład potwierdzający, że hakerzy są w stanie przeprowadzić akcję w cyberprzestrzeni, w wyniku której mogą pojawić się ofiary śmiertelne i realne zniszczenia.

Dość znaną operacją była też kampania „Night Dragon", która rozpoczęła się na początku 2009 roku. Eksperci jednej z najbardziej popularnych firm zajmujących się bezpieczeństwem w sieci – Mcafee, określili ją jako: świetnie zorganizowaną, ukierunkowaną na konkretne cele, wykorzystującą zaawansowane oprogramowanie oraz metody inżynierii społecznej. Celem operacji była kradzież wrażliwych danych takich jak szczegóły operacyjne, bilanse finansów oraz wyniki badań, należące do największych przedsiębiorstw energetycznych oraz petrochemicznych. Zdaniem ekspertów metody ataków oraz użyte narzędzia jednoznacznie wskazują na chińskich hakerów. Informacja ta nie jest żadnym zaskoczeniem, biorąc pod uwagę zaangażowanie Państwa Środka w cyberszpiegostwo oraz rosnące zainteresowania sektorem energetycznym, a w szczególności importem gazu i ropy ze strony tego państwa.

Najbardziej spopularyzowaną w mediach akcją sabotażową, wymierzoną w infrastrukturę energetyczną, było użycie robaka *Stuxnet* w celu zneutralizowania programu atomowego Iranu w 2009 roku. Operacja, która została przygotowana najpewniej przez USA i Izrael, miała na celu zniszczenie wirówek odpowiedzialnych za wzbogacanie uranu w ośrodku Natanaz oraz przekonać Irańczyków, że nie dysponują odpowiednią technologią i umiejętnościami do zbudowania broni atomowej. Była ona wyjątkowo trudna do przeprowadzenia ze względu na fakt, że ośrodek w Natanaz nie jest podłączony do sieci zewnętrznej. Amerykanie poradzili sobie z tym problemem, wprowadzając złośliwe oprogramowanie poprzez zainfekowane urządzenie przenośne. Mimo, iż operacja doprowadziła do zniszczenia ¼ wszystkich wirówek, ostatecznie zakończyła się niepowodzeniem. Jej los został przypieczętowany, kiedy złośliwe

oprogramowanie zostało wypuszczone do Internetu, gdzie zostało zidentyfikowane i zneutralizowane przez ekspertów z branży cyberbezpieczeństwa.

Powszechnie uznaje się tezę, że w przypadku wystąpienia konfliktu zbrojnego pomiędzy dwoma potęgami, najczęściej przytacza się tutaj przykład Chin i Stanów Zjednoczonych, infrastruktura energetyczna stanie się celem zaawansowanych cyberataków. Atakując cele na amerykańskim terytorium Chińczycy zamierzają zniechęcić Amerykanów do interwencji w razie wystąpienia konfliktu lokalnego. Jankesi w obawie przez zniszczeniem elementów infrastruktury krytycznej mieliby powstrzymać się od działania. Biorąc pod uwagę informacje dostarczone przez *The Wall Street Journal* o bombach logicznych[4], umieszczonych przez Rosjan i Chińczyków w sieciach energetycznych Stanów Zjednoczonych, zagrożenie to staje się jak najbardziej realne. Wprawdzie obecnie sytuacja nie wskazuje na to, żeby miałyby być one aktywowane – taka możliwość istnieje tylko w przypadku znacznego pogorszenia się wzajemnych relacji – to przykład ten, wraz z *blackoutem* z 2003 roku, pokazuje podatność sieci energetycznych na ataki.

Przykładowy sposób ataku

Przeprowadzając ataki często wykorzystuje się kontraktorów dużych firm energetycznych. Są to najczęściej małe przedsiębiorstwa, które nie mają odpowiednich funduszy na zapewnienie bezpieczeństwa. Przykładowy atak może wyglądać następująco:

1. Określenie celu ataku – dużego przedsiębiorstwa energetycznego, a następnie wyszukanie jego kontraktorów.
2. Znalezienie danych dotyczących pracowników firmy-kontraktora przy użyciu portali społecznościowych. Następnie atakujący przechodzi do stworzenia listy osób odpowiedzialnych za systemy komputerowe, określając ich stopień zaawansowania oraz poziom dostępu.
3. Uzyskanie kontroli nad systemami kontraktora poprzez *phishing*[5] lub wykorzystanie dziur w oprogramowaniu.

[4] Jest to złośliwy program umieszczony w systemie bez wiedzy jego użytkownika, który aktywowany jest w danej chwili.
[5] Wyłudzenie poufnych informacji poprzez podszywanie się pod zaufaną osobą lub instytucję.

4. Wykorzystując komputery kontraktorów, następuje włamanie do sieci głównego celu ataku.
5. Znalezienie interesujących danych, a następnie przesłanie ich do bezpiecznego miejsca.

Jest to tylko jeden przykładowy sposób przeprowadzania operacji przeciwko sektorowi energetycznemu. Rodzaje ataków bardzo szybko ewoluują i pojawią się nowe odmiany oraz rodzaje. Ostatni raport opublikowany przez West Point's Network Science Center informuje, że hakerzy mogą sparaliżować sieci energetyczne, wykorzystując tzw. efekt kaskadingu. Polega on na tym, że zamiast koncentrować się na najważniejszych i najlepiej bronionych elementach infrastruktury energetycznej, celem ataku stają się podstacje, które najczęściej są słabo chronione. Ich wyłączenie na skutek cyberataku wymusza przekazanie ich obciążenia innym stacjom, co prowadzi do ich przeładowania i w konsekwencji pozbawienia dostępu do energii elektrycznej znacznej części ludzi. Niezwykle trudno jest zapobiec takim atakom ze względu na brak czasu i odpowiednich środków do zapewnienia obrony wszystkim elementom infrastruktury energetycznej.

Działania, które powinny zostać podjęte przez sektor energetyczny

Przedsiębiorstwa sektora energetycznego, w celu utrzymania swojej konkurencyjności, muszą wprowadzać nowe technologie oraz innowacyjne rozwiązania, co sprawia, że rośnie ich zależność od systemów komputerowych. Jednoznacznie wiąże się to ze zwiększonym ryzykiem ataku hakerskiego. Ostatnie dwa nowe, popularne rozwiązania to inteligentne systemy dostarczania energii elektrycznej (*smart grids*) i technologia chmury obliczeniowej. Pierwsze z nich pozwala na integrację i idącą z nią w parze większą optymalizację działania, drugie zaś zyskuje coraz większą popularność w biznesie, oferując szybszą i tańszą wymianę danych oraz korzystanie z usług. Nowe metody niosą ze sobą jednak duże ryzyko i mogą zostać wykorzystane przez osoby zainteresowane spowodowaniem zniszczeń.

Jednym z kluczowych aspektów jest zwiększenie bezpieczeństwa w relacjach z podwykonawcami. Postuluje się wprowadzenie dodatkowego kryterium bezpieczeństwa przy ocenie potencjalnej współpracy. Będzie to stanowiło bodziec motywacyjny dla podwykonawców, którzy zainwestują więcej środków w cyberbezpieczeństwo, dążąc do konkurencyjności na rynku.

Biorąc pod uwagę, że większość ataków przeprowadzana jest przy użyciu niezbyt skomplikowanych metod, takich jak „brute force" czy wykorzystanie złośliwego oprogramowania, konieczne jest przywiązanie większej uwagi do podstaw bezpiecznego użytkowania internetu. Obejmuje to aktualizowanie wszystkich programów, używanie oprogramowania zwalczającego lub minimalizującego zagrożenie oraz zwiększenie świadomości dotyczącej zagrożenia wśród pracowników.

Wnioski dla Polski

Polska jak każde inne państwo na świecie jest zagrożone cyberatakami wymierzonymi w sektor energetyczny. W odniesieniu do naszego kraju występują jednak dwa dodatkowe czynniki, które zagrożenie to potęgują. Pierwszym z nich jest uzależnienie od dostaw rosyjskiego gazu, a drugim potencjał wydobywczy gazu łupkowego, który jest zdolny zagrozić interesom rosyjskim w regionie. Hakerzy powiązani z władzami na Kremlu wielokrotnie w przeszłości dokonywali aktów cyberszpiegostwa, wykradając informacje zachodnim koncernom energetycznym. Ponadto Rosjanie udowodnili, że są w stanie przeprowadzić skomplikowane, skoordynowane cyberataki, jak np. w Estonii lub Gruzji. Dlatego też groźba ta nie powinna być pod żadnym pozorem lekceważona.

Postępujące prace nad wydobyciem gazu łupkowego w Polsce z pewnością mogą przyczynić się do wzrostu intensywności akcji, dokonywanych przez rosyjskich hakerów, którzy będą dążyli do poznania planów firm inwestujących w to przedsięwzięcie. Biorąc pod uwagę znaczenie surowców energetycznych dla rosyjskiej gospodarki, nie można wykluczyć nawet bardziej zaawansowanych ataków na polską infrastrukturę energetyczną.

Polska potrzebuje zacieśnia współpracy z przedsiębiorstwami z tej dziedziny, celem wzmocnienia ich ochrony sieci komputerowych. W szczególności staje się to istotne w związku z planową budową elektrowni atomowych. Obiekty te wymagają szczególnych standardów bezpieczeństwa, w tym również przeciwko zagrożeniu atakami elektronicznymi. Głównym dokumentem, wyznaczającym strategiczne kierunku rozwoju cyberbezpieczeństwa Polski, jest „Polityka Ochrony Cyberprzestrzeni", zwracająca uwagę na konieczność zaktywizowania współpracy z przedsiębiorcami odpowiedzialnymi za zaopatrzenie w energię, surowce energetyczne i paliwa oraz rekomendująca stworzenie wewnętrznych gremiów wymiany

informacji i doświadczeń, a także zacieśnienie kontaktów z administracją publiczną. Niestety zapisy te, podobnie jak cały dokument, są bardzo ogólne i brakuje zaproponowanych konkretnych działań, które należałoby podjąć. Podobny problem tyczy się „Białej Księgi Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej", która wskazuje na konieczność budowy ochrony teleinformatycznej infrastruktury krytycznej, ale nie podaje żadnych rozwiązań.

Zdecydowanie istotniejszym dokumentem, w którym zawarto bardziej szczegółowe informacje dotyczące sposobów ochrony sieci teleinformatycznych sektora energetycznego, jest „Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK)". Oferuje on szereg dobrych praktyk, które mogą przyczynić się do wzmocnienia ochrony sieci. Proponuje się również podzielenie ochrony infrastruktury krytycznej na sześć obszarów, w tym na ochronę teleinformatyczną, jak równie wiele inicjatyw o charakterze edukacyjnym, słusznie zauważając istniejące braki w tej dziedzinie. Dobrym uzupełnieniem NPOIK w tej jest kwestii jest krajowy plan zarządzania kryzysowego, który w ramach identyfikacji zagrożeń wymienia zakłócenie funkcjonowania systemów łączności i systemów teleinformatycznych oraz wskazuje na podmioty, które są odpowiedzialne za koordynację działań w przypadku cyberataków.

Działania zaplanowane w dokumentach strategicznych są pozytywnym sygnałem, traktowania tego zagrożenia z należytą uwagą. Należy jednak ciągle monitorować sytuację i sprawdzać stopień wcielania proponowanych rozwiązań w życie. Najważniejszą sprawą jest wymiana informacji i umożliwienie dostępu do danych o zagrożeniach dla przedsiębiorców z sektora energetycznego.

Może dziwić, że pojawiają się w Polsce głosy mówiące, że to przedsiębiorcy powinni tylko i wyłącznie odpowiadać za ochronę biznesu. Jest to jednak nieuzasadnione, w szczególności w przypadku obiektów o znaczeniu strategicznym i państwo powinno tutaj wystąpić z szeregiem inicjatyw wspierających sektor prywatny. Infrastruktura energetyczna była i będzie jednym z najważniejszych elementów infrastruktury krytycznej państwa i z tego powodu wymaga dodatkowej, wzmocnionej obrony. Nasilające się cyberataki i zwiększający się stopień ich zaawansowania rodzą poważne zagrożenie dla przedsiębiorstw energetycznych, które nie poradzą sobie z nimi bez wsparcia państwa.

Tezy przedstawiane w serii „Policy Papers" Fundacji Amicus Europae nie zawsze odzwierciedlają jej oficjalne stanowisko !

Kontakt

**Fundacja
Aleksandra Kwaśniewskiego
„Amicus Europae"**

Aleja Przyjaciół 8/5
00-565 Warszawa, Polska

Tel. +48 22 622 66 33
Tel. +48 22 622 66 03
Fax:+48 22 629 48 16

email: fundacja@fae.pl, www.fae.pl

FAE Policy Paper nr 7/2014

Cyberbezpieczeństwo infrastruktury energetycznej

Autor: Andrzej Kozłowski

Ekspert Instytutu Kościuszki. Członek redakcji pisma „Stosunki Międzynarodowe". Doktorant na Wydziale Studiów Międzynarodowych i Politologicznych UŁ. W kręgu jego zainteresowań znajdują się cyberbezpieczeństwo, region Kaukazu Południowego oraz polityka bezpieczeństwa i zagraniczna USA.

Nadrzędną misją **Fundacji AMICUS EUROPAE** jest popieranie integracji europejskiej, a także wspieranie procesów dialogu i pojednania, mających na celu rozwiązanie politycznych i regionalnych konfliktów w Europie.

Do najważniejszych celów Fundacji należą:

- Wspieranie wysiłków na rzecz budowy społeczeństwa obywatelskiego, państwa prawa i umocnienia wartości demokratycznych;
- Propagowanie dorobku politycznego i konstytucyjnego Rzeczypospolitej Polskiej;
- Propagowanie idei wspólnej Europy i upowszechnianie wiedzy o Unii Europejskiej;
- Rozwój Nowej Polityki Sąsiedztwa Unii Europejskiej, ze szczególnym uwzględnieniem Ukrainy i Białorusi;
- Wsparcie dla krajów aspirujących do członkostwa w organizacjach europejskich i euroatlantyckich;
- Promowanie współpracy ze Stanami Zjednoczonymi Ameryki, szczególnie w dziedzinie bezpieczeństwa międzynarodowego i rozwoju gospodarki światowej;
- Integracja mniejszości narodowych i religijnych w społeczności lokalne;
- Propagowanie wiedzy na temat wielonarodowej i kulturowej różnorodności oraz historii naszego kraju i regionu;
- Popularyzowanie idei olimpijskiej i sportu.