Mirosław BANASIK
Ministerstwo Obrony Narodowej

ATRYBUTOWY MODEL OCENY ZAGROŻEŃ

1. Wstęp

Projektowanie zdolności do zapewnienia bezpieczeństwa państwa zawsze powinno się opierać na wiedzy o zdolnościach, jakie przedstawiają sobą zagrożenia o charakterze kinetycznym i cybernetycznym. Jednak na podstawie obserwowanych trendów w środowisku bezpieczeństwa, można postawić tezę, że w przyszłości nie będziemy mieć do czynienia tylko z odrębnymi działaniami w jednej przestrzeni. Należy oczekiwać, że będą mieć miejsce zintegrowane działania, nazywane hybrydowymi, łączące w sobie uderzenia kinetyczne w cyberprzestrzeni i w innych wymiarach. Utechnicznienie społeczeństw i coraz łatwiejszy dostęp do informacji sprawiają, że uderzenia mogą mieć coraz bardziej kompleksowy charakter. Wraz ze stałym wzrostem liczby podmiotów stanowiących hipotetyczne zagrożenia oraz możliwych sposobów i rodzajów oddziaływania, praktycznie niemożliwe jest przygotowanie się do przeciwstawienia się im, na podstawie coraz większej ilości szczegółów informacyjnych. Ze względu na ogromną dynamikę zmian w środowisku bezpieczeństwa dużym wyzwaniem jest nawet katalogowanie zagrożeń. Problem jeszcze bardziej komplikuje się w odniesieniu do zapewnienia bezpieczeństwa infrastruktury krytycznej. Należy mieć świadomość, że jej operatorami są podmioty cywilne, a informacje o zagrożeniach najczęściej pochodzą z wywiadu i są opatrzone wysoką klauzulą niejawności.

W przeszłości bardzo szczegółowo i selektywnie identyfikowano pojedyncze, unikalne zagrożenia i ich konsekwencje, co stanowiło podstawę do opracowania i zastosowania mechanizmów obronnych. Obecnie, gdy liczba zagrożeń gwałtownie rośnie, wykorzystanie starych mechanizmów praktycznie nie jest możliwe. Konieczne okazało się opracowanie metody pozwalającej na obiektywne, jakościowe wartościowanie zdolności przypisanych do zagrożeń. Niezbędną też okazała się potrzeba przetransformowania wiedzy o zdolnościach hipotetycznych oponentów, na grunt jawnego języka zrozumiałego zarówno dla środowisk wojskowych, jak i cywilnych. Zatem problem oceny zagrożeń nie jest łatwy w swojej istocie i charakterze. Chcąc go rozwiązać, należy najpierw uporać się z kompleksowością zagrożeń. Zagrożenia należy sprowadzić do takiego poziomu, na którym możliwe będzie przeprowadzenie w prosty sposób prac analitycznych. Powyższy stan można osiągnąć, dzięki podzieleniu przestrzeni zagrożeń na mierzalne obszary, odpowiadające zdolnościom (taksonomii zdolności) i sprowadzenie ich do takiego poziomu szczegółowości (podzdolności), który będzie mógł być zbadany oddzielnie.

Obecnie stosowane metody oceny zagrożeń koncentrują się na ich źródłach, które mają swoje korzenie w uwarunkowaniach politycznych i społecznych. Nie są ukierunkowane na identyfikowanie obiektywnych przesłanek narastania i materializowania zagrożeń. Metoda oceny zagrożeń przedstawiona poniżej skoncentrowana jest na oszacowaniu zdolności i poziomu zmotywowania podmiotów kreujących zagrożenia do osiągnięcia zakładanych celów. Na

podstawie oceny atrybutów zdolności lub charakterystyk przypisanych do danej grupy zdolności, identyfikowane są generyczne modele zagrożeń. Stosownie do oceny poszczególnych zdolności i ich atrybutów, zagrożenia zostają zakwalifikowane do odpowiedniego poziomu. W ten sposób przedstawione informacje o zagrożeniach, pozwalają na ich wykorzystanie zarówno przez ekspertów wojskowych, jak i przez osoby cywilne odpowiedzialne za zapewnienie bezpieczeństwa, w tym infrastruktury krytycznej.

Ocena zagrożeń powinna być wieloaspektowa i kompleksowa, a jej rezultaty przedstawione w postaci matrycy zagrożeń. W matrycy powinny być odzwierciedlone posiadane przez oponentów zdolności, a zagrożenia uszeregowane, stosownie do ich priorytetów. Generyczne modele pozwalają na identyfikowanie i opisywanie zagrożeń, o różnym charakterze i intensywności oddziaływania, bez konieczności wskazywania konkretnego podmiotu, który je kreuje. Takie podejście pozwala również na jawność informacji, a z drugiej strony na zebranie i pogrupowanie zdolności w stosowne obszary, odpowiadające całemu spektrum zagrożeń. Na tej podstawie możliwe jest dokonanie analizy i oceny poszczególnych grup zdolności. Wnioski wyciągnięte z tych ocen pozwalają na określenie do jakiego poziomu dane zagrożenie powinno być zakwalifikowane. Przyjęcie powyższego sposobu postępowania, sprowadzającego się do zdolnościowej oceny zagrożeń, służy do prognozowania sposobów przeprowadzenia uderzeń (wariantów użycia zdolności). Na tej podstawie możliwe jest identyfikowanie przyszłych misji i zadań, a następnie wymaganych zdolności w drodze procesu planowania obronnego. Tak zaprojektowane własne zdolności, pozwolą na przeciwstawienie się przyszłym zagrożeniom, bądź łagodzenie ich skutków

2. Atrybutowy model oceny zagrożeń[1]

2.1 Atrybuty zagrożeń

Atrybuty stanowią sobą wybrane cechy, bądź odrębne właściwości zagrożeń, na podstawie których określany jest poziom determinacji podmiotów kreujących zagrożenia do osiągnięcia swoich celów. Do każdego zagrożenia przypisane są odrębne atrybuty. Niemniej jednak należy wiedzieć, że pomiędzy atrybutami nie występują żadne, wzajemne zależności.

Wyodrębnić można dwie oddzielne grupy atrybutów:

1) Atrybuty odnoszące się do realnej możliwości wystąpienia danego zagrożenia, charakteryzują determinację do działania. Zaliczyć do nich należy: intensywność, skrytość i czas wystąpienia zagrożenia.
2) Atrybuty odnoszące się do zasobów, wyrażają realne możliwości osiągnięcia celów przez podmioty kreujące zagrożenia.

Na podstawie oceny atrybutów zagrożeń opracowywany jest generyczny model zagrożeń nazywany też matrycą zagrożeń.

[1] Przedstawia amerykańskie podejście do oceny zdolności, które posiadają zagrożenia. Por. D.P. Dugan, S. R Thomas, C.K. Veitch and L. Woodard, *Categorizing Threat, Building and Using a Generic Threat Matrix*. Albuquerque 2007, s. 19-27

2.1.1 Atrybuty wyróżniające determinacje do działania

Ta grupa atrybutów wartościuje skalę zagrożeń i wyraża poziom determinacji do osiągnięcia celów działania. Charakterystyki atrybutów odzwierciedlają zdolności podmiotów kreujących zagrożenia do egzemplifikacji własnych zamiarów. Czym wartość danego atrybutu jest większa, tym większa jest determinacja do osiągania założonych celów. Wyróżniamy trzy grupy atrybutów zagrożeń: intensywność zagrożeń, poziom ich skrytości i możliwy czas ich wystąpienia.

Intensywność jest atrybutem zagrożenia wyrażającym pośpiech lub wytrwałość w osiąganiu wcześniej nakreślonych celów. Określa poziom determinacji do działania i skłonność do podejmowania ryzyka w osiąganiu tych celów. Zagrożenia o większej intensywności są bardziej niebezpieczne, gdyż odzwierciedlają wyższe ambicje podmiotów kreujących zagrożenia. Intensywność zagrożeń może być zakwalifikowana do jednej z trzech wartości:

1) Wysoki poziom. Podmioty kreujące zagrożenia są bardzo wysoce zmotywowane do osiągania swoich celów i są skłonne zaakceptować wysokie ryzyko w ich osiąganiu. Akceptowalne konsekwencje własnego działania mogą obejmować między innymi śmierć lub dostanie się do niewoli członków organizacji oponentów lub osób postronnych.
2) Średni poziom. Podmioty kreujące zagrożenia średnio są zmotywowane do osiągania swoich celów i są skłonne zaakceptować wybrane, negatywne konsekwencje własnego działania w ich osiąganiu. Akceptowane konsekwencje własnego działania mogą obejmować między innymi dostanie się do niewoli, ale nie są akceptowalne straty bezpowrotne w stanie osobowym organizacji oponentów lub osób postronnych.
3) Niski poziom. Podmiot kreujący zagrożenia chce osiągnąć własne cele, ale nie akceptuje negatywnych konsekwencji własnego działania, takich jak śmierć czy dostanie się do niewoli.

Poziom skrytości jest atrybutem zagrożenia wyrażającym utrzymanie wymaganego poziomu poufności zdefiniowanych wcześniej celów. Aby to osiągnąć, niezbędne jest utrzymanie w tajemnicy szczegółowych informacji dotyczących organizacji podmiotów kreujących zagrożenia, struktury i sposobu działania. Na wyższych poziomach organizacyjnych powinno się dążyć do ukrycia przed światem prawdziwych zamiarów przyszłego działania. Pozyskanie powyższych, zazwyczaj dobrze ukrywanych informacji, może pozwolić na wykonanie uderzenia wyprzedzającego lub przygotowanie się do odparcia niespodziewanego uderzenia oponentów. Wyróżnić można trzy poziomy skrytości:

1) Wysoki. Podmioty kreujące zagrożenia są zdolne do utrzymania na wysokim poziomie w tajemnicy swoich celów i zamiarów działania.
2) Średni. Podmioty kreujące zagrożenia są zdolne do utrzymania na średnim poziomie tajemnicy swoich celów i zamiarów działania. Nie są w stanie ukryć szczegółów dotyczących organizacji, do których przynależą i działalności wewnątrz tej organizacji.
3) Niski. Podmioty kreujące zagrożenia nie są zdolne do utrzymania w tajemnicy niezbędnego poziomu tajemnicy swoich celów i zamiarów działania oraz działalności organizacji, do których przynależą.

Czas jest atrybutem zagrożenia wyrażającym perspektywę, w której podmioty kreujące zagrożenia są w stanie zaplanować i wdrożyć w życie takie sposoby

działania, które zagwarantują osiągnięcie zaplanowanych celów szczegółowych. W przypadku uderzenia w cyberprzestrzeni lub wykonania ataku kinetycznego, czas ten jest liczony do chwili jego przeprowadzenia. Im więcej czasu podmioty kreujące zagrożenia są w stanie poświęcić na przygotowanie się do ataku, tym większe będą dewastujące skutki jego przeprowadzenia. Wyróżnia się cztery poziomy odnoszące się do atrybutu czasu:

1) Od kilku lat do kilku dekad. Podmioty kreujące zagrożenia są w stanie poświęcić wiele lat na zaplanowanie i przygotowanie sposobów działania zmierzających do osiągnięcia własnych celów.
2) Od kilku miesięcy do kilku lat. Podmioty kreujące zagrożenia są w stanie poświęcić kilka lat na zaplanowanie i przygotowania sposobów działania zmierzających do osiągnięcia własnych celów.
3) Od kilku tygodni do kilku miesięcy. Podmioty kreujące zagrożenia są w stanie poświęcić kilka miesięcy na zaplanowanie i przygotowania sposobów działania zmierzających do osiągnięcia własnych celów.
4) Od kilku dni do kilku tygodni. Podmioty kreujące zagrożenia są w stanie poświęcić kilka tygodni na zaplanowanie i przygotowania sposobów działania zmierzających do osiągnięcia własnych celów.

2.1.2 Atrybuty wyrażające zasoby

Atrybuty zasobów charakteryzują zdolności podmiotów kreujących zagrożenia i wyrażane są przez wskaźniki ilościowe odnoszące się do ludzi, dostępu i wiedzy. Atrybuty te zapewniają możliwości podjęcia działań dla osiągnięcia z góry zaplanowanych celów. Wyróżnia się atrybuty odnoszące się do personelu, wiedzy i dostępu.

Personel techniczny jest atrybutem zagrożenia wyrażającym ilość osób, które są zdolne do budowania technicznych zdolności potrzebnych do osiągnięcia celów, założonych przez podmioty kreujące zagrożenia. Personel techniczny ogranicza się tylko do takich grup ludzi, którzy posiadają wiedzę i umiejętności wykonywania uderzeń w cyberprzestrzeni, bądź przeprowadzenia uderzeń kinetycznych, a także takich, którzy potrafią wyprodukować systemy, zapewniające pozyskanie nowych zdolność. Podmioty posiadające większą ilość personelu technicznego, mają większy potencjał do rozwijania nowych metod i technik wykonywania takich uderzeń, z którymi nie mieliśmy do czynienia w przeszłości. Ponadto wyższy personel techniczny jest bardzo pomocny przy opracowywaniu planów przeprowadzenia uderzeń. Wyróżnia się cztery poziomy wartości odnoszące się do ilości personelu technicznego:

1) Tysiące. Podmioty kreujące zagrożenia są w stanie dedykować kilka tysięcy osób posiadających techniczne zdolności do budowy nowych rodzajów broni. Osoby te mogą bez ograniczeń komunikować się między sobą we wszystkich fazach pozyskiwania nowych środków rażenia.
2) Setki. Podmioty kreujące zagrożenia są w stanie dedykować małe grupy personelu posiadającego techniczne zdolności do budowy nowych rodzajów broni. Grupy te mają ograniczoną możliwość komunikowania się pomiędzy sobą, ale bez ograniczeń mogą komunikować się z innymi członkami danej grupy.
3) Dziesiątki. Podmioty kreujące zagrożenia są w stanie dedykować małe, niezależne grupy posiadające techniczne zdolności do budowy nowych

rodzajów broni. Osoby te mogą bez ograniczeń komunikować się między sobą we wszystkich fazach pozyskiwania nowych środków rażenia.

4) Kilka osób. Podmioty kreujące zagrożenia są w stanie dedykować do kilku osób posiadających techniczne zdolności do budowy nowych rodzajów broni. Osoby te mogą bez ograniczeń komunikować się między sobą we wszystkich fazach pozyskiwania nowych środków rażenia.

Szacunkowe liczby osób przypisane do danego poziomu, stanowią jedynie wartość kalkulacyjną i nie ograniczają fizycznej liczby osób aktualnie będących członkami organizacji generujących zagrożenia. Dla przykładu wrogo nastawione organizacje skupiające w swych szeregach tysiąc członków, mogą posiadać jedynie kilka osób zdolnych do budowy nowych środków rażenia. Tak więc w zależności od struktury organizacyjnej, personel techniczny zazwyczaj może liczyć dziesiątki lub setki osób.

Wiedza jest atrybutem zagrożenia, wyraża teoretyczny i praktyczny poziom posiadania kompetencji oraz do wykorzystania tych kompetencji, dla użycia posiadanych zdolności i osiągnięcia własnych celów. Wiedza powinna obejmować między innymi takie obszary jak prowadzenie badań naukowych i prac rozwojowych, a także treningów i ćwiczeń. Z wiedzą ściśle związane są możliwości dzielenia się informacjami. Atrybut ten odnosi się do wiedzy na temat zdolności zarówno ofensywnych, jak i defensywnych. Im większa jest wiedza, tym większe zdolności posiadają podmioty i tym mniejsze potrzebne są zasoby, a tym samym szybciej mogą być osiągnięte własne cele. Oczywiście potrzebna jest wiedza stosowna do charakteru kreowanego zagrożenia, tj. cybernetycznego, kinetycznego czy hybrydowego. Wyróżnia się dwie kategorie wiedzy, to jest dotyczącej cyberprzestrzeni i działań kinetycznych. W każdej z powyższej kategorii wyróżnia się trzy poziomy wiedzy:

1) Wysoka. Podmioty kreujące zagrożenia posiadają możliwości wykorzystania teoretycznej i praktycznej wiedzy oraz kompetencji ekspertów dla osiągnięcia własnych celów. Podmioty kreujące zagrożenia posiadają wiedzę i możliwości dzielenia się informacjami, dotyczącymi programów szkolenia, prowadzenia badań naukowych i prac rozwojowych.
2) Średnia. Podmioty kreujące zagrożenia posiadają możliwości wykorzystania średnich kompetencji ekspertów dla osiągnięcia własnych celów. Średnie kompetencje należy rozumieć jako posiadanie na wysokim poziomie wiedzy praktycznej, wspartej wiedzą teoretyczną na niskim lub średnim poziomie. Podmioty kreujące zagrożenia, posiadają ograniczoną wiedzę i możliwości dzielenia się informacjami, dotyczącymi programów szkolenia, prowadzenia badań naukowych i prac rozwojowych.
3) Niska. Podmioty kreujące zagrożenia posiadają możliwości wykorzystania niewielkich kompetencji ekspertów dla osiągnięcia własnych celów. Niewielkie kompetencje należy rozumieć jako posiadanie na niskim lub średnim poziomie wiedzy praktycznej i niewielkiej lub nie posiadanie w ogóle wiedzy teoretycznej. Podmioty kreujące zagrożenia, nie posiadają wiedzy i możliwości dzielenia się informacjami, dotyczącymi programów szkolenia, prowadzenia badań naukowych i prac rozwojowych.

Dostęp jest atrybutem zagrożenia wyrażającym możliwość dostania się do restrykcyjnie chronionych systemów w celu osiągnięcia własnych celów, poprzez oddziaływanie kinetyczne i w cyberprzestrzeni. Charakterystyki tego atrybutu

odnoszą się do zdolności infiltrowania systemów ochranianych elektronicznie, bądź fizycznie, poprzez szantaż, wymuszanie, korupcję osób uprawnionych, bądź poprzez oddziaływanie w cyberprzestrzeni. Dzięki infiltracji można uzyskać szereg pozytywnych efektów. Zaliczyć do nich między innymi można: potrzebę posiadania mniejszych zasobów niezbędnych do osiągnięcia zakładanych celów, podniesienie poziomu wiedzy o potencjalnych obiektach ataków, czy wreszcie przyjęcie długoterminowych schematów postępowania dla odniesienia innych korzyści. Wyróżnia się trzy poziomy dostępu:

1) Wysoki. Podmioty kreujące zagrożenia są w stanie, poprzez określone grupy osób, posiadać nieograniczony dostęp do wybranych, ochranianych systemów.
2) Średni. Podmioty kreujące zagrożenia są w stanie, poprzez określone grupy osób, posiadać ograniczony dostęp do wybranych, ochranianych systemów.
3) Niski. Podmioty kreujące zagrożenia nie są w stanie, poprzez określone grupy osób, dotrzeć do wybranych, ochranianych systemów.

2.2 Model oceny zagrożeń

Na podstawie powyżej zdefiniowanych atrybutów, można zidentyfikować generyczny model zagrożeń. W modelu generycznym (tabela 2), każdy rodzaj zagrożenia, jest scharakteryzowany i oceniony oddzielnie, a następnie dane zagrożenie zakwalifikowane jest do odpowiedniego poziomu, odzwierciedlającego możliwość wystąpienia sytuacji niebezpiecznej (zdarzenia).

Scharakteryzowany na podstawie zdolności profil zagrożenia, stanowi źródło informacji do predykcji sposobów działania przeciwnika. Na tej podstawie definiowana jest własna misja, której celem jest przeciwstawienie się zagrożeniom. W ramach tej misji określa się sposoby własnego działania, a następnie zadania, które muszą być wykonane, aby osiągnąć cele misji. Powyższe informacje są niezbędne do zdefiniowania własnych, przyszłych zdolności, które są potrzebne do przeciwstawienia się przyszłym zagrożeniom. Tak więc modele zagrożeń służą do identyfikowania przyszłych, własnych zdolności, na podstawie których dokonuje się rozwój sił zbrojnych. Podmioty cywilne, do których zaliczamy między innymi właścicieli (operatorów) infrastruktury krytycznej, na podstawie profilu zagrożeń, opracowują strategie przeciwdziałania, a w ramach nich budują plany ochrony i przyjmują systemowe rozwiązania, w których określają wymaganą architekturę zdolności niezbędną do przeciwstawienia się przyszłym zagrożeniom i łagodzenia skutków możliwych uderzeń.

Tabela nr 1: Generyczna matryca oceny zagrożeń

Poziom zagrożenia	**Profile zagrożeń**						
	Atrybuty determinacji do działania			**Atrybuty zapewniające działanie (zasoby)**			
					Wiedza		
	Intensywność	Skrytość	Czas	Personel techniczny	O działaniach w cyberprzestrzeni	O działaniach kinetycznych	Dostępność
1	W	W	Od kilku lat do kilku dekad	Tysiące	W	W	W
2	W	W	Od kilku lat do kilku dekad	Setki	Ś	W	Ś

3	W	W	Od kilku miesięcy do kilku lat	Setki	W	Ś	Ś
4	Ś	W	Od kilku tygodni do kilku miesięcy	Dziesiątki	W	Ś	Ś
5	W	Ś	Od kilku tygodni do kilku miesięcy	Dziesiątki	Ś	Ś	Ś
6	Ś	Ś	Od kilku tygodni do kilku miesięcy	Kilku	Ś	Ś	N
7	Ś	Ś	Od kilku miesięcy do kilku lat	Dziesiątki	N	N	N
8	N	N	Od kilku dni do kilku tygodni	Kilku	N	N	N

Źródło: D.P. Duggan, S.R. Thomas, C.K Veitch. and L. Woodard, *Categorizing Threat, Building and Using a Generic Threat Matrix*. Albuquerque 2007, s. 23

Zagrożenia zakwalifikowane do poziomu pierwszego, zawsze będą posiadały największe zdolności do osiągnięcia własnych celów, a do poziomu ósmego najmniejsze. Zaszeregowanie do odpowiedniego poziomu zagrożenia odbywa się na podstawie oceny atrybutów zagrożeń, a te z kolei ocenia się na podstawie taksonomii (architektury) zdolności. Generalnie można stwierdzić, że zagrożenia narastają od poziomu ósmego do poziomu pierwszego. Tak więc największe niebezpieczeństwo odzwierciedla poziom pierwszy. Niekiedy zagrożenia zakwalifikowane do poziomu najniższego mogą osiągnąć te same cele, co zagrożenia zakwalifikowane do poziomu pierwszego, ale będzie to zapewne rezultatem przypadku, braku ochrony obiektu na który wykonano uderzenia, czy niedogodnego czasu do przeciwstawienia się uderzeniom, niż rezultatem realnie posiadanych zdolności przez podmioty kreujące zagrożenia.

W praktyce jest też bardzo prawdopodobne, że przykładowe zagrożenie nie będzie odpowiadało wszystkim parametrom opisanym w matrycy generycznej. W takiej sytuacji zagrożenie powinno być zakwalifikowane do poziomu, który najbardziej odzwierciedla dany profil zagrożenia. Należy rozumieć, że model generyczny służy głównie do tego, aby można było zidentyfikować różnice pomiędzy zagrożeniami, a więc dać pewność, że nie są to te same zagrożenia i na tej podstawie zakwalifikować je do odpowiedniego poziomu.

Dokonując oceny generycznej matrycy zagrożeń, można wyciągnąć następujące wnioski:

1) Należy wyodrębnić dwie granice uwarunkowań, które są niezbędne do zidentyfikowania realnego profilu zagrożeń:
   a) Zagrożenie zakwalifikowane do pierwszego poziomu, zawsze będzie charakteryzowało się najwyższymi zdolnościami przypisanymi do wszystkich atrybutów;
   b) Zagrożenie zakwalifikowane do poziomu ósmego zawsze będzie charakteryzowało się najniższymi zdolnościami przypisanymi do wszystkich atrybutów.
2) Poziom technicznego personelu, może być pomocny w zrozumieniu innych atrybutów zagrożeń:

a) Zagrożenia charakteryzujące się większą ilością technicznego personelu, niewątpliwie zawsze będą posiadały wyższe wartości intensywności, wiedzy i akcesu;
b) Zagrożenia charakteryzujące się kilkuosobowym personelem technicznym, nie będą posiadały wysokiej wiedzy, gdyż będzie ona niewystarczająca do prowadzenia badań, projektów rozwojowych i dzielenia się nowymi informacjami;
c) Zagrożenia charakteryzujące się kilkuosobowym personelem technicznym, będą posiadały niską wartość intensywności, gdyż zagrożenia nie biorą się same z siebie, a muszą je wykreować ludzie z odpowiednią wiedzą, umiejętnościami i doświadczeniem.

3) Wysoki poziom wiedzy organizacji kreującej zagrożenia w cyberprzestrzeni, nie będzie skutkował niskim poziomem wiedzy w wymiarze kinetycznym i na odwrót, zazwyczaj ze względu na doświadczenie ekspertów w teorii i praktyce.
4) Zagrożenia charakteryzujące się wysoką wiedzą (w cyberprzestrzeni i wymiarze kinetycznym), będą posiadały wartość akcesu co najmniej na średnim poziomie, gdyż z założenia, ekspertów jest trudniej wykryć, a tym samym łatwiej jest im niepostrzeżenie włamać się do ochranianych systemów.

Istnieją pewne właściwości zagrożeń, które pomimo tego że nie posiadają wyróżniających się charakterystyk, mogą wpływać na jeden lub kilka atrybutów. Nazywamy je multiplikatorami. Mogą one wpływać na zwiększenie zdolności, ale nie mają wpływu na profil zagrożeń. Do multiplikatorów możemy zaliczyć środki finansowe, środki trwałe, technologie itp.

Środki finansowe wspierają kreowanie zagrożeń. Historycznie finanse były utożsamiane ze zdolnościami, jakkolwiek czynnik inflacji sprawił, że wszelkie kalkulacje stają się coraz bardziej niejasne i nieobiektywne, dlatego trudne jest odnoszenie się do obecnie posiadanych zdolności przez pryzmat finansów. Finanse mogą podnosić wartości niektórych atrybutów, na przykład wiedzy lub akcesu. Z drugiej strony mogą redukować poziom wartości innych, na przykład skrytości. Pozyskiwanie bowiem wiedzy lub zwiększenie możliwości do pokonania ochranianych systemów może narazić wrogą organizację na szybsze wykrycie, ze względu na wykorzystanie zewnętrznych zasobów.

Środki trwałe są podobnym multiplikatorem do środków finansowych. Mogą ułatwić możliwości przeprowadzenia misji, ale ciężko jest je przetransformować na aktualne zdolności. Definiowane są jak możliwości zagrożeń do budowania lub pozyskania wyposażenia, sprzętu, narzędzi i materiałów, niezbędnych do osiągnięcia własnych celów.

Niektóre technologie wykorzystywane do pozyskania zdolności i osiągania zakładanych celów, mogą być czynnikiem ograniczającym niektóre atrybuty zagrożeń, na przykład czas i wiedzę. Dynamicznie rozwijające się technologie wymagają zawsze aktualizacji wiedzy i szybkiego zastosowania.

3. Zakończenie

Permanentnie wzrastająca liczba zagrożeń stwarza sytuację, w której z jednej strony bardzo trudno jest posiadać wiedzę o nowych podmiotach stwarzających zagrożenia i wszystkich szczegółach ich dotyczących, a z drugiej strony obecnie

niewyobrażalne jest budowanie zdolności do zapewnienia bezpieczeństwa na podstawie szczegółowo przeanalizowanych, jedynie pojedynczych, wyselekcjonowanych zagrożeń, które wydają się być najbardziej odpowiednie w danym czasie. Przyjęcie takich założeń nie daje gwarancji zbudowania struktury organizacyjnej, która posiadałaby zdolności pozwalające na przeciwstawienie się przyszłym zagrożeniom. Potrzebne jest inne podejście oparte na modelu zdolnościowej oceny zagrożeń. Dokonać tego można poprzez zredukowanie kompleksowości przestrzeni zagrożeń, polegające na jej podziale na mniejsze części, odpowiadające mierzalnym wartościom zdolności posiadanych przez podmioty kreujące zagrożenia i na tej podstawie zakwalifikowanie ich do stosownego poziomu. Zaproponowany, atrybutowy model oceny zagrożeń, jest przykładem podziału przestrzeni na osiem odrębnych poziomów zagrożeń. Każdy z nich charakteryzuje się specyficznym profilem, skonstruowanym w oparciu o ilościowe wartości atrybutów zagrożeń, oszacowane na podstawie oceny zdolności, do których zaliczamy intensywność, skrytość, czas, personel techniczny, wiedzę o działaniach kinetycznych i w cyberprzestrzeni oraz dostęp. Różnice w wartościach zagrożeń przypisanych danemu poziomowi w matrycy generycznej, zapewniają to, że każde unikalne zagrożenie może być skatalogowane, gdyż odzwierciedla zdolności zagrożeń do przeprowadzenia uderzenia, odpowiadające modelowi teoretycznemu (oczekiwanego przez ekspertów). Generyczne modele zagrożeń, stanowiące sobą rezultat kompleksowej oceny zagrożeń, pozwalają podmiotom państwowym odpowiadającym za bezpieczeństwo, w tym siłom zbrojnym i operatorom infrastruktury krytycznej w szczególności, na podstawie profilu zdolnościowego zagrożeń, zidentyfikować sposób przeprowadzenia uderzenia. Na tej podstawie możliwe jest budowanie własnych, przyszłych zdolności i strategii, które pozwolą na przeciwstawienie się przyszłym zagrożeniom i minimalizowanie skutków ich oddziaływania. Dzielenie się informacjami o zagrożeniach w skali państwa zapewni wyeliminowanie najbardziej wrażliwych obszarów, podatnych na uderzenia infrastruktury krytycznej i innych wrażliwych obiektów, a także na przygotowanie wszystkich podmiotów odpowiedzialnych za bezpieczeństwo, w tym sił zbrojnych, do odparcia niespodziewanego uderzenia.

Streszczenie

Atrybutowy model oceny zagrożeń, polega na redukowaniu kompleksowości przestrzeni zagrożeń, poprzez podział jej na mniejsze części, odpowiadające mierzalnym wartościom zdolności, jakie posiadają podmioty kreujące zagrożenia. Profil zagrożenia przypisany do stosownego poziomu, oszacowany jest na podstawie oceny atrybutów zdolności, do których zaliczamy: intensywność, skrytość, czas, personel techniczny, wiedza o działaniach kinetycznych i w cyberprzestrzeni oraz dostęp. Generyczne modele zagrożeń, stanowiące sobą rezultat kompleksowej oceny zagrożeń, pozwalają podmiotom państwowym odpowiadającym za bezpieczeństwo, w tym siłom zbrojnym i operatorom infrastruktury krytycznej, zidentyfikować efekty i sposób przeprowadzenia uderzenia. Na tej podstawie możliwe jest budowanie własnych, przyszłych zdolności i strategii, które pozwolą na przeciwstawienie się przyszłym zagrożeniom bądź minimalizowanie ich skutków.

Słowa klucze: zagrożenia, zdolności, ocena

Summary

Attribute model for threats assessment is based on reducing the complexity of the space of threats by dividing it into smaller parts, corresponding to measurable values of capabilities of entities which create threats. Threats profile assigned to an appropriate level, is estimated on the basis of attributes ability assessment including: intensity, stealth, time, technical personnel, knowledge of kinetic and cyber operations and access. Generic models of threats, which are the result of a comprehensive risk assessment allow entities responsible for the security of the state, including the armed forces and operators of critical infrastructure to identify the effects and manner of conducting the strike. On that basis it is possible to build individual, future capabilities and strategies that will allow the opposition to future threats or mitigation of their impact.

Key words: threats, capable, assessment

Bibliografia

1. Ackerman G., A*ssessing Terrorist Motivations for Attacking Critical Infrastructure.* strona *www.e-reports-ext.llnl.gov/pdf/341566.pdf* (pobrano 15.11.2014 r.)
2. A military guide to terrorism in the twenty-first century. strona *www.fas.org/irp/threat/terrorism/guide.pdf* (pobrano 25.11.2014 r.)
3. Duggan D.P., Thomas S.R., Veitch C.K. and Woodard L., Categorizing Threat, Building and Using a Generic Threat Matrix. Albuquerque 2007
4. Duggan D. P., & Michalski J. T., *Threat analysis framework report*. Albuquerque 2007
5. Duggan D.P., *Generic threat profiles*. Albuquerque 2005
6. Durling R.L., Jr., Price D.E. & Spero K.K., *Vulnerability and risk assessment using the Homeland-Defense Operational Planning System (HOPS).* San Francisco 2005
7. Harmonized Threat and Risk Assessment (TRA), Methodology,TRA-1. Ottawa 2007
8. Luiijf E.A.M., *Energy sector threats and vulnerabilities. Proc. of 3rd EAPC/PfP Workshop on Critical Infrastructure Protection and Civil Emergency Planning*. Zurich 2005
9. Merkle P.B., *Extended defense systems: I. Adversary-defender modeling grammar for vulnerability analysis and threat assessment*. Albuquerque 2006
10. Olson D.T., *The path to terrorist violence: A threat assessment model for radical groups at risk of escalation to acts of terrorism.* Monterey 2005