Emilia Musiał
Uniwersytet Pedagogiczny w Krakowie

Trolling jako przykład zagrożeń informacyjnych w cyberprzestrzeni

Wstęp

Globalizacja, rozwój społeczeństwa informacyjnego, a także nowych technologii teleinformatycznych oraz Internetu zmieniły środowisko bezpieczeństwa państw, w tym także Polski. Tym nowym obszarem – środowiskiem bezpieczeństwa – staje się cyberprzestrzeń, umożliwiająca ludziom realizację swoich celów, choć nie zawsze zgodnych z zasadami życia społecznego, normami etycznymi i prawnymi.

Dlatego też poważnym niebezpieczenstwem wynikającym z funkcjonowania w tej przestrzeni stają się zagrożenia informacyjne tj. dezinformacja, trolling, wroga propaganda, manipulacja informacją. Szansą zaś w zapewnieniu bezpieczeństwa informacyjnego – zgodnie ze *Strategią Bezpieczeństwa Narodowego RP* – może być m.in. rozpoznawanie przestępstw dokonanych w cyberprzestrzeni, zapobieganie im oraz ściganie ich sprawców.

Trollowanie – charakterystyka zjawiska

Trollowanie (ang. *trolling*) to rodzaj antyspołecznego zachowania w cyfrowym świecie, polegający głównie na ośmieszaniu oraz obrażaniu użytkowników forów internetowych, portali społecznościowych oraz innych miejsc, w których toczy się dyskusję w Internecie (Olszewski 2014). Obecnie ma negatywne, wręcz chuligańskie znaczenie.

Pojęcie trollowanie (z ang. *trolling for fish*) ściśle wiąże się terminem wędkarskim określającym metodę połowu ryb przez ciągnięcie przynęty za łodzią, tzw. łowienie na haczyk. W odniesieniu do terminu internetowego przynęta przyjmuje postać napastliwej, kontrowersyjnej, często nieprawdziwej wiadomości najczęściej niezwiązanej z danym tematem. Tak więc internetowy troll zarzuca swoją „przynętę" – często w sposób bardzo nachalny i wulgarny – i robi to głównie po to, aby wywołać kłótnię.

Samo zjawisko trollowania nie podlega regulacjom prawnym – dopóki wypowiedź nie zawiera treści nielegalnych, np. grafik prezentujących pornografię dziecięcą. Karą dla regularnych trolli jest więc zwykłe wykluczenie z danego serwisu, ale jest to zależne wyłącznie od właścicieli serwisu (*„Trollowanie" i „flaming"…* 2012). Ponadto według art. 191 §1 Kodeksu Karnego wszystkie zachowania agresywne w Internecie, takie jak wulgaryzmy bądź groźby w komentarzach pod postami są wykroczeniem, a ich autorzy powinni ponosić konsekwencje w realnym świecie.

Osoba, która publikuje wiadomości podburzające, nieistotne i niezwiązane z tematem danej grupy dyskusyjnej, forum, czatu lub bloga w slangu internetowym nosi miano trolla. Za wszelką cenę dąży ona do dezorganizacji forum oraz irytacji pozostałych użytkowników. Im większa kłótnia i więcej osób uczestniczy w sporze, tym bardziej troll jest zadowolony, a zwycięstwem dla niego jest sytuacja, gdy administrator zamyka temat dyskusji (ang. *End Of Topic* – EOT) lub umieści go w tzw. *killfile'u* czyli na liście zablokowanych użytkowników, tematów lub słów.

Troll nie ma jednej twarzy. Portal *Smosh.com* (udostępniający m.in. humorystyczne memy internetowe) wyszczególnia aż kilkanaście typów internetowych „ujadaczy", wśród których znajduje się m.in. (*Sposób na internetowych*… 2016):

1. Podpalacz („miotacz płomieni") – jego celem jest umyślne wywołanie burzy w dyskusji na temat nieznaczącego nic zagadnienia.
2. Pedantyczny gramatyk („gramatyczny nazista") – kompletnie nie interesuje go dyskusja, lecz zdania i słowa, które w niej padają. Wytyka użytkownikom to, że nie potrafią korzystać ze słownika.
3. Wojownik – nigdy nie odpuszcza dyskusji i walczy do końca, ponieważ „ktoś w Internecie nie ma racji".
4. Ekspert (człowiek-encyklopedia) – fachowiec. Wie wszystko – na wszystkim zna się najlepiej, wszystko widział i rozumie.
5. Złodziejaszek – wysyła wiadomości prywatne do użytkowników, podając się za organa ścigania, wymusza na innych użytkownikach zdradzenie ich faktycznej tożsamości, adresu, numeru telefonu itp.
6. Prześladowca – po upatrzeniu sobie celu (użytkownika) będzie go śledził i ścigał po każdym forum, starając się maksymalnie mu dokuczyć. Nie przestanie, dopóki ofiara ataków go nie przeprosi lub nie ukorzy się publicznie.
7. Troll-dawca – wyszuka wrażliwe informacje o tożsamości osoby po drugiej stronie internetowego łącza i dla zabawy upubliczni je na forach.

Na uwagę zasługuje fakt, iż – według badań Erina Buckelsa z Uniwersytetu Manitoba – osoby lubujące się w obrażaniu i agresywnej postawie wobec innych internautów wykazują się cechami psychopatycznymi. U ponad 50% trolli stwierdzono objawy makiawelizmu, czyli traktowania ludzi z wyższością, w sposób instrumentalny. Największy związek znaleziono jednak pomiędzy trollowaniem a sadyzmem. Zarówno jedni, jak i drudzy czerpią przyjemność z niepokojenia innych (Jachyra 2011, s. 259).

Trolle, czyli cyber-frustraci, którzy karmią się możliwością uprzykrzania komuś życia, są święcie przekonani, że nic im nie grozi i nikt ich nie namierzy. Wierzą, że są nieuchwytnymi, anonimowymi „bogami" w cyfrowej przestrzeni. Jednak nic bardziej mylnego. Otóż badacze danych (*Big Data*) oraz naukowcy z Cornell University oraz Stanford University, wspierani finansowo przez Google

opracowali algorytm, który – wyciągając wnioski z treści 10 postów opublikowanych przez internautę – jest w stanie ocenić, czy można uznać go za internetowego trolla. Przez półtora roku trwania eksperymentu okazało się, że trolle wyraźnie wyróżniają się na tle standardowego użytkownika sieci (*Sposób na internetowych…*, 2016):

1. generują znacznie więcej treści (nawet do 12 razy więcej niż typowy internauta),
2. częściej sięgają po wyrazy potoczne i wulgaryzmy,
3. mają tendencję do odpowiadania niemal na każdy komentarz, w którym ktoś inny odnosi się do ich słów.

Warto także wspomnieć o nowym projekcie Google, czyli *Perspective*. To program, który ma przeglądać komentarze i oceniać je w oparciu o to, jak bardzo podobne są do komentarzy określanych jako toksyczne albo takie, które sprawią, że ktoś opuści daną rozmowę. Póki co system, który uczy się coraz lepiej rozpoznawać i wyczuwać nastroje we wpisach, na razie jest w powijakach i jak to z uczeniem maszynowym, będzie ulepszał się z czasem oraz intensywnością użytkowania (Snoch 2017).

Wbrew pozorom trolling nie jest wcale domeną garstki młodych chuliganów. Trollowanie to pokusa, której ulega wielu internautów. Według badań przeprowadzonych przez Brytyjski Instytut YouGov na 1125 internautach ze Stanów Zjednoczonych, aż 28% dorosłych Amerykanów korzystających z zasobów sieci przyznało, że zdarzało im się celowo podejmować „szkodliwą działalność online", czyli działania wymierzone w urażenie innego internauty. Wśród najczęściej przewijających się zachowań dominowały: zażarte kłótnie z nieznajomymi na forach, przeradzające się w internetowe pyskówki (23%) oraz celowe stawianie kontrowersyjnych tez, których broni się do samego końca, mimo braku jakichkolwiek racjonalnych argumentów na ich korzyść (12%) (*Over a quarter*… 2014).

Jak walczyć z tym zjawiskiem. Wszyscy znawcy tematu i netykiety podają tylko jedną, uniwersalną receptę na obchodzenie się z nimi. Brzmi ona: nie karmić trolla. Nie ma bowiem sensu wdawać się w dyskusję z kimś, kto swoim zachowaniem podważa elementarne zasady dyskusji i nie respektuje samego rozmówcy. Z trollem nie wygrasz. Trolla możesz tylko ignorować. Choć należy pamiętać, że ignorowany troll zniechęci się pisaniem tylko do siebie i najprawdopodobniej przeniesie się, poszukując nowych słuchaczy i ofiar.

Trolling w kontekście zagrożeń informacyjnych

Internet, który stał się synonimem wolności słowa i nieskrępowanego przepływu informacji, a także narzędziem rewolucji i zmian społecznych sprawił, że coraz więcej podmiotów (rządów, instytucji i firm), a także indywidualnych

osób decyduje się przenosić różne elementy swojej codziennej aktywności do cyberprzestrzeni.

Niestety przenikają do niej również negatywne formy ludzkiej działalności. Konstrukcja sieci internetowej dająca duże poczucie anonimowości, wykorzystywana jest przez przestępców, terrorystów, a także niektóre państwa, do prowadzenia nielegalnej działalności lub agresji wobec innych podmiotów (Grzelak i in. 2012, s. 126). Wzrost bowiem roli informacji we współczesnym świecie, powoduje wzrost zagrożeń jej bezpieczeństwa.

Ochrona cyberprzestrzeni stała się współcześnie jednym z najczęściej podejmowanych tematów związanych z bezpieczeństwem, w tym bezpieczeństwem informacyjnym państwa. Ten rodzaj bezpieczeństwa wraz z jego integralną częścią jaką jest cyberbezpieczeństwo, odnosi się do środowiska informacyjnego państwa, a jego celem jest *zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze* (*Projekt Doktryny*… 2015, s. 3).

K. Liderman bezpieczeństwo informacyjne określa jako uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej i wykorzystywanej informacji, pojęcie bezpieczeństwa informacyjnego dotyczy zatem podmiotu (człowieka, organizacji), który może być zagrożony utratą zasobów informacyjnych albo otrzymaniem informacji o nieodpowiedniej jakości (z czym właśnie w przypadku trollowania mamy do czynienia – E. M.) (Liderman 2012, s. 13).

Bezpieczeństwo informacyjne staje się zatem gwarantem bezpieczeństwa militarnego, finansowego, gospodarczego zarówno w skali lokalnej pojedynczego państwa, jak i na arenie międzynarodowej, co znajduje odpowiedź w opracowanych i wdrażanych przez państwo polskie strategiach oraz programach rządowych w zakresie bezpieczeństwa informacyjnego. Treści podkreślające wagę tej problematyki odnajdujemy m.in. w *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* oraz w *Rządowym programie ochrony cyberprzestrzeni RP na lata 2009-2011*. Należy podkreślić również, iż tematyka bezpieczeństwa informacyjnego jest regulowana przez polski system prawny, w tym Konstytucję RP.

Tu warto za K. Lidermanem przypomnieć, że jako źródła zagrożeń bezpieczeństwa informacyjnego możemy przyjąć: siły natury (pożar, powódź, huragan, trzęsienie ziemi, epidemie), błędy ludzi i ich działania wg. błędnych lub niewłaściwych procedur, celowe, szkodliwe działanie ludzi oraz awarie sprzętu komputerowego, oprogramowania, infrastruktury usługowej (zasilanie, klimatyzacja, woda, ogrzewanie) (Liderman 2012, s. 155).

Ponadto należy uwzględnić fakt, iż zagrożenie bezpieczeństwa informacyjnego może mieć swe źródło w działalności człowieka lub organizacji i wyrażać się (Bączek 2006, s. 86-87): nieuprawnionym ujawnieniem informacji;

naruszeniem przez władze praw obywatelskich; asymetrią w międzynarodowej wymianie informacji; niekontrolowanym rozwojem nowoczesnych technologii bioinformatycznych; przestępstwami komputerowymi; cyberterroryzmem; walką informacyjną; zagrożeniami asymetrycznymi; szpiegostwem; ale – co zasługuje na uwagę w kontekście wspomnianego trollingu [komentarz E. M.] – działalnością grup o antyspołecznym zachowaniu świadomie manipulujących przekazem informacji.

Zagrożenie dla bezpieczeństwa informacyjnego buduje także aktywność grup, środowisk, firm, koncernów, które w swojej działalności świadomie manipulują przekazem informacji, maskując swoje prawdziwe cele, dane dotyczące oferowanych wyrobów, usług, wykorzystując techniki manipulacji, perswazji, dezinformacji, propagandy (Więcaszek-Kuczyńska 2014, s. 222).

Projekt *Doktryny Bezpieczeństwa Informacyjnego RP* zwraca uwagę, że zagrożeniem płynącym z funkcjonowania w środowisku informacyjnym może być rozpowszechnianie i powielanie treści propagandowych mające na celu ukazanie polskiej racji stanu w negatywnym świetle (stosowanie prowokacji, celowe manipulowanie przekazem poprzez wyrywanie z kontekstu fragmentów wypowiedzi polityków RP, nadawanie im kontrowersyjnego charakteru). Zaś wśród zagrożeń informacyjnych związanych z funkcjonowaniem w cyberprzestrzeni wymienia (*Doktryna…* 2015, s. 6):

1. ataki powodujące zakłócenia funkcjonowania sieci teleinformatycznych w sektorach i instytucjach o podwyższonym stopniu wrażliwości, w tym tworzących infrastrukturę krytyczną;
2. istnienie technologicznych luk, które dają szansę, także niezauważonej, ingerencji w treści portali internetowych oraz wpływania na zdolności do działania w cyberprzestrzeni;
3. dezinformację, trolling, wrogą propagandę, zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego.

W kontekście wspomnianych wyżej zagrożeń na uwagę zasługuje fakt, iż wśród głównych pojęć przyjętych w *Doktrynie bezpieczeństwa informacyjnego RP* znalazło się trollowanie interpretowane jako *antyspołeczne zachowanie charakterystyczne dla internetowych grup, forów dyskusyjnych, czatów i sieci społecznościowych, polegające na zamierzonym wpływaniu na innych użytkowników w celu ich ośmieszenia lub obrażenia poprzez wysyłanie napastliwych, kontrowersyjnych, często nieprawdziwych przekazów* (*Doktryna…* 2015, s. 4).

Większość z nas nie zdaje sobie sprawy z faktu, iż mentalność ludzka jest łatwym celem dla oddziaływania informacyjnego, bowiem wszechobecne środki masowego przekazu, a także nieograniczony dostęp do nich powoduje, iż dostarczane informacje mogą być swobodnie kształtowane i przekazywane masowo. Zatem rozpowszechnianiu zmanipulowanych lub nieprawdziwych

informacji w celu wywarcia wpływu na odbiorców i skłonienia ich do określonych zachowań na korzyść dezinformującego, możemy przeciwdziałać świadomie konsumując treści informacyjne, analizując je (identyfikując ataki propagandowe i dezinformacyjne), a także podnosząc swoją świadomość o zagrożeniach.

Z dużym prawdopodobieństwem można przyjąć także, że skuteczne radzenie sobie z tego typu sytuacjami kryzysami wymaga wysokiego poziomu kultury informacyjnej, stanowiącej jeden z podstawowych elementów kultury bezpieczeństwa (zob. Cieślarczyk 2015; Batorowska 2013; Babik 2016). Różny bowiem poziom kultury informacyjnej będzie miał istotne znaczenie dla sposobów konstruowania informacji, jej przekazywania, przechowywania i odbierania docierających oznajmień – oceny dostępnych informacji pod względem jej prawdziwości, ważności, rzetelności, a także zrozumienia i użycia jej zgodnie z prawem i etyką.

Trollowanie w praktyce

Naukowcy z Beihang University dowiedli, że najbardziej znaczącą emocją (także w kontekście naszych aktywności w Sieci) jest gniew, który szybko się rozprzestrzenia (Maj 2013). Stąd też nierzadko zdarza się, że pisząc wyrażamy złość, która może narastać i przyjmować formę trollowania – podburzania innych do kłótni i bezsensownych dyskusji, wypowiadania się na tematy, o których nie mamy najmniejszego pojęcia. Bezspornie tematem numer jeden, który podejmujemy w licznych dyskusjach internetowych jest polityka, ale nie stronimy od innych równie kontrowersyjnych tematów tj.: aborcja, homoseksualizm, eutanazja, sport, czy też życie ludzi z pierwszych stron gazet.

Dane pozyskane przez naukowców z Uniwersytetu Stanforda oraz Cornella wskazują jasno – *każdy z nas może być internetowym trollem, o ile ma zły humor. Oczywiście, to zjawisko jest dużo bardziej złożone – każdy z nas może mieć zupełnie inny motyw w dokopywaniu komuś w sieci. Warto jednak wiedzieć, że od naszego samopoczucia może zależeć nasza skłonność do siania nienawiści w sieci, gdzie tak naprawdę nikt nie jest anonimowy* (Szczęsny 2017).

Trollowanie to także – o dziwo – pomysł na biznes. Wśród trolli bowiem mamy do czynienia z zaawansowanymi trollami płatnymi, których zadaniem jest pisanie kilkudziesięciu komentarzy dziennie, na forach, portalach newsowych, Facebooku oraz produkcja lajków lub „nie-lajków" (m.in. całą armię takich trolli wykorzystują służby rosyjskie, jak również partie polityczne w celu ośmieszenia swoich partyjnych przeciwników). Są oni najczęściej zatrudniani na krótkie umowy (według dziennika „Polska" ceny za komentarz liczący 100 do 350 znaków wahają się w przedziale 0,3 – 2 zł; najlepsi w tym fachu mogą liczyć nawet na 6 tys. złotych miesięcznie) i mają swoich opiekunów, którzy weryfikują ich pracę.

Taki płatny troll staje się wyrobnikiem, „lansującym" samochód, komputer, restaurację, celebrytę, partię itp. Może także być częścią akcji ograniczania szkody,

gdy celebrycie, politykowi, firmie lub produktowi powinie się noga i trzeba ratować jego reputację. Albo może też uczestniczyć w akcji popsucia czyjejś reputacji, np. konkurenta politycznego.

Stąd na stronach internetowych możemy natknąć się na ogłoszenia typu: *Agencja marketingu szeptanego poszukuje osób z doświadczeniem (warunek konieczny) w pisaniu postów politycznych w Internecie. Wymagania: kreatywność, dyskrecja, umiejętność logicznego myślenia. Atrakcyjne wynagrodzenie, umowa o dzieło. Proszę o wysyłanie CV wraz z listem motywacyjnym do …*

Czy także: *Zatrudnię trolla na dobrych warunkach do komentowania wpisów na temat katastrofy smoleńskiej. Wymagania: minimalna umiejętność pisania w języku polskim, błyskawiczne reakcje na pojawiające się wpisy na powyższy temat, własna inicjatywa w ich tworzeniu będzie mile widziana, umiejętność wyśmiewania i wyszydzania wszelkich faktów i teorii sugerujących jakąkolwiek winę rosyjską lub władz polskich, nienawiść do wszystkiego, co wiąże się z PiS i oboma Kaczyńskimi, brak jakichkolwiek zahamowań w oczernianiu ofiar katastrofy oraz ich rodzin. Dodatkowym atutem będzie umiejętność kwestionowania, gmatwania, komplikowania, rozdrabniania nawet najbardziej oczywistych prawd i faktów. Termin rozpoczęcia pracy: zaraz po ogłoszeniu wyników badania zapisów czarnych skrzynek rządowego TU-154M przez Krakowski Instytut im. J. Sehna. Wynagrodzenie do uzgodnienia.*

Na uwagę zasługuje także fakt, iż płatni trolle najczęściej przechodzą liczne szkolenia m.in. (*Byłam…* 2015):

1. prawnicze, podczas którego prawnik zapewnia, że to, co trolle mają robić jest w pełni legalne i nie grozi im za to żadna kara (każdy taki troll podpisuje oświadczenie o dochowaniu tajemnicy, zachowaniu anonimowości w sieci, zobowiązanie do usunięcia otrzymanych programów po skończeniu projektu, do niekopiowania instrukcji i nieudostępniania innym itp.);
2. techniczne pokazujące, jak zmieniać adresy IP (po to, aby mnożyć lajki dla wybranych wypowiedzi na stronie i aby umieszczać posty pod różnymi nikami), jak wygenerować losowy adres IP (tu nieoceniona jest wyszukiwarka TOR), gdzie można utworzyć bezpłatne konta e-mailowe bez potrzeby podawania numeru telefonu (potrzebne do rejestracji w różnych portalach i tworzenia ników), jak używać specjalnego programu-muszli, który czyści historię lajków i komentarzy, czy też jak zachować pełną anonimowość w sieci;
3. „ideologiczne", w trakcie których określona zostaje „misja", czyli kogo należy promować (lajkować i pomnażamy lajki), a kogo wprost przeciwnie – osłabiać (nie-lajkować).

Podsumowanie

Nienawiść w sieci jest zjawiskiem powszechnym i szkodliwym, jednak trudno jest ją zwalczyć. Eskalacja wrogości – także przejawiającej się

w internetowym trollingu – wynika z poczucia anonimowości i bezkarności piszącego, daje mu poczucie istnienia w świecie, w którym egzekwowanie prawa jest niemożliwe, a nawet nikomu niepotrzebne. Agresywne działania w przestrzeni informacyjnej skierowane mogą być nie tylko przeciwko przypadkowo napotkanym osobom w sieci, ale na całe społeczeństwo oraz jego świadomość, a także na aparat administracyjny, świat nauki i kultury oraz przemysł i ekonomikę danego państwa.

Warto pamiętać, że dziś polem walki są przede wszystkim umysł i mentalność człowieka, które w dobie społeczeństwa informacyjnego nie posiadają naturalnej bariery przed manipulacją, dezinformacją czy konsekwentną i zmasowaną propagandą. Według jednej z technik manipulacji ludźmi lub informacją nie ten jest skuteczny, kto ma dużą wydajność, lecz ten, kto potrafi użyć innych do swoich celów, a to zapewne potrafi troll internetowy.

I choć agresywni i podstępni komentujący nie opanują Internetu, to mogą popsuć niejedno dobre miejsce w cyberprzestrzeni celem chociażby realizacji interesów sprzecznych z interesem RP.

Bibliografia

„Trollowanie" i „flaming", czyli kłótnie internetowe stają się coraz większym utrapieniem (2012). Dostęp: 5.01.2017. Tryb dostępu: http://www.dziennikpolski24.pl/artykul/3105800,trollowanie-i-flaming-czyli-klotnie-internetowe-staja-sie-coraz-wiekszym-utrapieniem,id,t.html.

Babik, W. (2016) *Kultura informacyjna a ekologia informacji współczesnego człowieka.* W: Batorowska, H., Kwiasowski, Z. (red. nauk.), *Kultura informacyjna w ujęciu interdyscyplinarnym*. *Teoria i praktyka*. T. II. Kraków: UP, IBiEO, KKIiZI.

Batorowska, H. (2013) *Od alfabetyzacji informacyjnej do kultury informacyjnej. Rozważania o dojrzałości informacyjnej*. Warszawa: Wydaw. SBP.

Bączek, P. (2006) *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*. Toruń: Wydaw. Adam Marszałek.

Byłam bankowym trollem (2015). Dostęp: 5.01.2017. Tryb dostępu: https://bylambankowymtrolem.wordpress.com/2015/05/02/bylam-bankowym-trolem/.

Cieślarczyk, M. (2015) *Kultura informacyjno-komunikacyjna jako element kultury bezpieczeństwa.* W: Batorowska, H. (red. nauk.), *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka.* T. 1. Kraków: Wydaw. UP w Krakowie.

Doktryna Bezpieczeństwa Informacyjnego RP. Projekt (2015). Dostęp: 5.01.2017. Tryb dostępu:

https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf.

Grzelak, M., Liedel, K. (2012) *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*. „Bezpieczeństwo Narodowe", nr 22, s. 125-139. Dostęp: 5.01.2017. Tryb dostępu: https://www.bbn.gov.pl/download/1/11469/str125-139MichalGrzelakKrzysztofLiedel.pdf.

Jachyra, D. (2011) *Trollowanie – antyspołeczne zachowania w Internecie, sposoby wykrywania i obrony*. Dostęp: 5.01.2017. Tryb dostępu: http://www.wneiz.pl/nauka_wneiz/studia_inf/28-2011/si-28-253.pdf.

Liderman, K. (2012) *Bezpieczeństwo informacyjne*. Warszawa: Wydawnictwo Naukowe PWN.

Maj, M. (2013) *W sieci nie panuje głupota tylko złość – uważają naukowcy*. Dostęp: 5.01.2017. Tryb dostępu: http://di.com.pl/w-sieci-nie-panuje-glupota-tylko-zlosc-uwazaja-naukowcy-48829.

Olszewski, R. (2014) *Trollowanie – antyspołeczne zachowanie czy świetny pomysł na biznes*. Dostęp: 5.01.2017. Tryb dostępu: http://artelis.pl/artykuly/61821/Trollowanie---antyspoleczne-zachowanie-czy-swietny-pomysl-na-biznes.

Over a quarter of Americans have made malicious online comments (2014). Dostęp: 5.01.2017. Tryb dostępu: https://today.yougov.com/news/2014/10/20/over-quarter-americans-admit-malicious-online-comm/.

Snoch, J. (2017) *Google Perspective – uczenie maszynowe w walce z trollingiem*. Dostęp: 25.02.2017. Tryb dostępu: http://www.komputerswiat.pl/nowosci/aplikacje/2017/08/google-perspective-uczenie-maszynowe-w-walce-z-trollingiem.aspx.

Sposób na internetowych trolli i hejterów (2016). Dostęp 5.01.2017. Tryb dostępu: http://tech.wp.pl/sposob-na-internetowych-trolli-i-hejterow-6034811830030977a.

Szczęsny, J. (2017) *Każdy może stać się internetowym trollem. Wystarczy, że ma „zły humor"*. Dostęp: 8.02.2017. Tryb dostępu: http://antyweb.pl/internetowy-troll-badanie/.

Więcaszek-Kuczyńska, L. (2014) *Zagrożenia bezpieczeństwa informacyjnego*. „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej", nr 2(10), s. 210-233. Dostęp: 5.01.2017. Tryb dostępu:

http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-7c4c89d0-10ba-4930-a714-19c2da0b93b5/c/Wiecaszek-Kuczynska.pdf.

Streszczenie

W dobie społeczeństwa informacyjnego, a także wszechobecnego Internetu nowym środowiskiem bezpieczeństwa staje się cyberprzestrzeń, umożliwiająca ludziom realizację swoich celów, choć nie zawsze zgodnych z zasadami życia społecznego, normami etycznymi i prawnymi.

Dlatego też poważnym zagrożeniem wynikającym z funkcjonowania w tej przestrzeni stają się zagrożenia informacyjne tj. dezinformacja, trolling, wroga propaganda, manipulacja informacją. Szansą zaś w zapewnieniu bezpieczeństwa informacyjnego może być m.in. rozpoznawanie przestępstw dokonanych w cyberprzestrzeni, zapobieganie im oraz ściganie ich sprawców.

Słowa kluczowe: trollowanie, troll, cyberprzestrzeń, zagrożenia informacyjne, bezpieczeństwo informacji

Trolling as an example of the information risk in cyberspace

Summary

In the era of the information society, new technologies and the Internet, new security environment becomes a cyberspace that enables people to the realization of its objectives, although not always compatible with the principles of social life, ethical standards and legal framework.

That is why a serious threat resulting from the operation of the in this space become threats: misinformation, trolling, enemy propaganda, manipulation of information. Chance in ensuring information security may be recognition of crimes committed in cyberspace, the prevention and prosecution of their perpetrators.

Keywords: trolling, troll, cyberspace, information risk, information security