Agnieszka Polończyk
Uniwersytet Pedagogiczny w Krakowie

Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa

Wstęp

Obserwowany od momentu przełomu XX i XXI wieku gwałtowny postęp dokonujący się w obszarze technologicznym oraz informatycznym, głównie w zakresie technologii mobilnych i teleinformatyki, w znaczący sposób wpłynął na wszystkie sfery życia ludzkiego. Dynamiczny rozwój mediów komunikacyjnych, a także coraz większa dostępność urządzeń elektronicznych umożliwiających korzystanie z Internetu, przyczyniły się do łatwego pozyskiwania informacji będącej obecnie jednym z najistotniejszych strategicznych zasobów współczesnych państw oraz organizacji.

Ze względu na stale rosnącą wartość i znaczenie informacji, stanowiącej czynnik przewagi, wiedzy oraz władzy poszczególnych podmiotów, a nawet niejednokrotnie decydujący o ich bezpieczeństwie (Liderman 2012, s. 11-12), coraz większą uwagę poświęca się zagadnieniom bezpieczeństwa informacji, ochrony systemów informacyjnych oraz bezpiecznego przetwarzania znajdujących się w nich danych. Problematyka ta wydaje się być o tyle doniosła i istotna, iż współcześnie każda niemalże płaszczyzna bezpieczeństwa narodowego – począwszy od politycznej, poprzez gospodarczą, militarną, czy ekologiczną, a na społecznej oraz kulturowej kończąc – staje się coraz bardziej zależna od bezpiecznego przepływu informacji oraz bezawaryjnej pracy systemów bazujących na obszernych zasobach informacyjnych. Zapewnienie bezpieczeństwa informacyjnego jest jednak bardzo złożonym przedsięwzięciem, a jego powodzenie zależy od wielu czynników, w tym od umiejętnego zarządzania bezpieczeństwem informacji, wypracowania szeregu procedur organizacyjnych i technicznych, wreszcie – poziomu świadomości osób dopuszczonych do przetwarzania informacji (Janczak, Nowak 2013, s. 7, 16).

W tym kontekście interesującym zagadnieniem jest częste udostępnianie w sieci przez podmioty państwowe (np. policję, urzędy, instytucje itp.) informacji oraz danych ważnych z punktu widzenia bezpieczeństwa państwa. Niejednokrotnie działania te wynikają z chęci włączania społeczeństwa w wybrane działania podmiotów (np. poprzez społeczny dialog, konsultacje, wdrażanie propozycji obywateli), co stanowi bez wątpienia pozytywny wymiar wzmacniający ideę społeczeństwa informacyjnego. Z drugiej strony, szerokie udostępnianie informacji i danych związane jest z licznymi zagrożeniami, których identyfikacja i zwalczanie staje się coraz większym wyzwaniem technicznym oraz organizacyjnym.

Na szczególną uwagę zasługują tu dane o charakterze przestrzennym, tj. dane odnoszące się bezpośrednio lub pośrednio do określonego położenia lub obszaru geograficznego. To właśnie informacja przestrzenna, uzyskiwana w procesie interpretacji danych przestrzennych, wydaje się być dziś jednym z najbardziej nośnych sposobów przekazu wiadomości o interesujących nas faktach, zdarzeniach, przedmiotach, zjawiskach czy procesach. Jej bezpieczeństwo powinno zatem znaleźć się w obszarze zainteresowania zarówno praktyków, jak i teoretyków z zakresu szeroko rozumianego bezpieczeństwa informacyjnego.

Jednym z narzędzi umożliwiających jasną i czytelną wizualizację danych o charakterze przestrzennym, jest Krajowa Mapa Zagrożeń Bezpieczeństwa (KMZB). Celem niniejszego artykułu jest przedstawienie głównych zagrożeń z obszaru bezpieczeństwa informacyjnego w odniesieniu do konkretnego narzędzia informatycznego udostępnianego przez Policję – wspomnianej wcześniej Krajowej Mapy Zagrożeń Bezpieczeństwa. W pierwszej części pracy zaprezentowano aparatorium pojęciowe oraz przedstawiono względnie zamknięty zbiór głównych zagrożeń identyfikowanych w obszarze bezpieczeństwa informacyjnego. Następnie, opisano działanie systemu KMZB oraz wyodrębniono rodzaje zagrożeń i sposoby włamań. Pracę wieńczą wnioski oraz autorskie propozycje wstępnych zmian, których zastosowanie przyczynić się może do zmniejszenia zagrożeń systemu bezpieczeństwa informacyjnego Policji.

Należy zaznaczyć, iż artykuł ma charakter przyczynkowy i stanowić może wstęp do dalszych, pogłębionych analiz na podjęty temat. Krajowa Mapa Zagrożeń Bezpieczeństwa jest narzędziem nowym, znajdującym się w fazie testowania i ulepszania, stąd pewne zawarte w niniejszej pracy spostrzeżenia i wnioski mogą w najbliższym czasie ulec częściowej dezaktualizacji.

Bezpieczeństwo informacyjne i jego zagrożenia

W bogatej literaturze przedmiotu z obszaru nauk o bezpieczeństwie, dotyczącej typologii bezpieczeństwa, bezpieczeństwo informacyjne sytuuje się w ramach kryterium przedmiotowego obok bezpieczeństwa politycznego, militarnego, gospodarczego, społecznego, kulturowego, ekologicznego czy ideologicznego. Najczęściej jest ono definiowane jako *zbiór działań, metod oraz procedur podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem* (Potejko 2009, s. 194). W innym ujęciu, odnosi się ono do *wszelkiego rodzaju wysiłków, służących ochronie posiadanych informacji, istotnych w kontekście bezpieczeństwa (a więc mających wpływ na sprawne funkcjonowanie struktur państwowych i społeczeństwa), jak i zapewnieniu przewagi informacyjnej przez zdobywanie*

nowych lub bardziej aktualnych danych oraz akcje dezinformacyjne wobec ewentualnych przeciwników (państw lub innych podmiotów) (Madej 2009, s. 18-19). W szerszym rozumieniu, bezpieczeństwo informacyjne *obejmuje wszystkie procesy technologiczne – od pozyskiwania, poprzez transmisję, przetwarzanie, do przechowywania informacji w systemach informacyjnych, stanowiąc kompleks przedsięwzięć zapewniający bezpieczeństwo środowiska informacyjnego* (Janczak, Nowak 2013, s. 17). Bezpieczeństwo informacyjne jest pojęciem szerokim, dotyczy bowiem nie tylko bezpieczeństwa samej informacji w każdej postaci (również tej nieuświadomionej przez sam podmiot), ale również bezpieczeństwa systemów, w których jest ona generowana, przetwarzana, przechowywana i przekazywana, środowiska, w którym działają te systemy, a także personelu, który z tych systemów korzysta. Wynika z powyższego, iż w bezpieczeństwie informacyjnym zawiera się pojęcie bezpieczeństwa informacji, które oznacza *ochronę wszystkich form wymiany, przechowywania i przetwarzania danych* (Janczak, Nowak 2013, s. 20), innymi słowy – *zachowanie poufności, integralności i dostępności informacji* (norma PN-ISO/IEC 27001:2014-12), a także jej *ochronę przed wszelkimi zagrożeniami w celu zapewnienia ciągłości działań oraz minimalizacji ryzyka* […] (norma PN-ISO/IEC 27002:2014-12). E. Nowak i M. Nowak proponują szeroką definicję bezpieczeństwa informacyjnego, które określają jako *stan warunków wewnętrznych i zewnętrznych, który pozwala państwu na posiadanie, przetrwanie i swobodę rozwoju społeczeństwa informacyjnego* (E. Nowak, M. Nowak 2011, s. 103).

Co istotne, badania bezpieczeństwa informacyjnego nie należy odnosić jedynie do obszaru cyberprzestrzeni oraz teleinformatyki, a tym samym mylić go z bezpieczeństwem teleinformatycznym, które określa się również jako „bezpieczeństwo w sieci", „bezpieczeństwo sieciowe", „bezpieczeństwo komputerowe" czy „bezpieczeństwo telekomunikacyjne". Pojęcie bezpieczeństwa teleinformatycznego jest – podobnie, jak pojęcie bezpieczeństwa informacji – węższe od bezpieczeństwa informacyjnego, dotyczy bowiem uzyskiwania, przechowywania, przetwarzania oraz przekazywaniem informacji w formie elektronicznej poprzez systemy komputerowe, systemy teleinformatyczne oraz sieci teleinformatyczne. W pojęciu tym nie zawierają się zatem chociażby wszelkiego rodzaju dane występujące w innych niż cyfrowa postaciach, znajdujące się w zasobach instytucji (tj. w zbiorach bibliotecznych, muzealnych, archiwalnych, urzędowych itp.), a także w zasobach osób prywatnych (tj. w prywatnych zbiorach, kolekcjach itp.) (Ura, Pieprzny 2015, s. 35-36).

Bezpieczeństwo informacyjne niejednokrotnie definiuje się jako stan wolny od zagrożeń. Właściwe zidentyfikowanie zagrożeń stanowi obecnie podstawę określania właściwej strategii nie tylko przetrwania, ale i rozwoju każdego podmiotu organizacyjnego.

Z bogatego piśmiennictwa przedmiotu dotyczącego zagrożeń bezpieczeństwa (Wrzosek 2013; Liderman 2012; Łuczak 2004; Janczak 2001; Żebrowski, Kwiatkowski 2000), na potrzeby niniejszego artykułu wybrano klasyfikację proponowaną przez P. Bączka (Bączek 2006, s. 72-73). Dzieli on zagrożenia bezpieczeństwa informacyjnego wedle następujących kryteriów:

- zagrożenia losowe – klęski żywiołowe, katastrofy, wypadki, które wpływają na stan bezpieczeństwa informacyjnego organizacji (np. pożar budynku, w którym przechowywane są nośniki informacji);
- tradycyjne zagrożenia informacyjne – szpiegostwo, działalność dywersyjna lub sabotażowa (ukierunkowane na zdobycie informacji lub ofensywną dezinformację prowadzoną przez inne osoby, podmioty i organizacje);
- zagrożenia technologiczne – zagrożenia związane z gromadzeniem, przechowywaniem i przetwarzaniem informacji w sieciach teleinformatycznych (np. przestępstwa komputerowe, cyberterroryzm, walka informacyjna);
- zagrożenia odnoszące się do praw obywatelskich osób lub grup społecznych (np. sprzedaż informacji, przekazywanie informacji podmiotom nieuprawnionym, naruszanie przez władze prywatności, bezprawne ingerencje służb specjalnych, ograniczenie jawności życia publicznego).

Ponadto, zagrożenia można podzielić ze względu na lokalizację ich źródła na:

- wewnętrzne (powstające wewnątrz organizacji), które obejmują zagrożenie utratą, uszkodzeniem lub modyfikacją danych z powodu niezamierzonego (błędnego lub przypadkowego) bądź celowego działania nieuczciwych użytkowników (pracowników);
- zewnętrzne (generowane poza organizacją), które obejmują zagrożenie utratą, uszkodzeniem danych lub pozbawieniem możliwości obsługi przez przypadkowe bądź celowe działania ze strony osób trzecich;
- fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi następuje w wyniku wypadku, awarii, katastrofy lub innego nieprzewidzianego zdarzenia wpływającego na system informacyjny bądź urządzenie sieciowe (Żebrowski, Kwiatkowski 2000, s. 65).

Uzupełnieniem powyższych rozważań jest stanowisko A. Żebrowskiego (Żebrowski, Kwiatkowski 2000, s. 63-64, 73), który wskazuje, iż największe zagrożenie bezpieczeństwa informacyjnego stanowi działalność człowieka. Celowe zagrażanie systemowi bezpieczeństwa informacyjnego jest wynikiem kumulacji trzech elementów: motywu, środka realizacji włamania do owego systemu oraz okazji, czyli uzyskania dostępu do dysku komputerowego lub sieci. Człowiek może wykorzystywać różnorakie sposoby włamań do systemów informacyjnych, jak np.:

- zmowę kilku sprawców,
- celowe inicjowanie awarii,

- wywoływanie fałszywych alarmów (uśpienie czujności),
- szantaż, korupcję,
- rozsyłanie do firm ankiet, zapytań, propozycji,
- rozkodowywanie hasła dostępu,
- atak słownikowy,
- podsłuch sieciowy,
- wirusy, bakterie, robaki, konie trojańskie, bomby logiczne oraz inne groźne aplikacje destabilizujące sprawność sytemu,
- wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego,
- techniki obchodzenia zabezpieczeń, np. programy wykorzystujące błędy w systemach operacyjnych i oprogramowaniu użytkowym,
- przechwytywanie otwartych połączeń sieciowych.

Należy podkreślić, iż przedstawiona powyżej lista nie jest listą zamkniętą – prognozuje się, iż będzie ona z pewnością ulegała rozszerzeniu o nowe zagrożenia oraz wykorzystywane sposoby włamań do systemów informacyjnych. W związku z tym, ważnym zadaniem każdej organizacji jest ciągłe monitorowanie zagrożeń w jej otoczeniu zewnętrznym, szczególnie, gdy upowszechniane dane oraz informacje mogą zostać potencjalnie wykorzystane w celu zachwiania jej bezpieczeństwem.

Wydaje się to być szczególne istotne w sytuacji, gdy tworzone są nowe programy oraz narzędzia informatyczne, znajdujące się jeszcze w początkowej fazie ich użytkowania. Szybka identyfikacja potencjalnych zagrożeń pozwoli na modyfikację oraz ulepszenie istniejącego oprogramowania tak, aby wyeliminować bądź zmniejszyć prawdopodobieństwo wystąpienia któregoś z nich w przyszłości, a tym samym wzmocnić system bezpieczeństwa całej organizacji.

Poniżej zaprezentowano jedno z nowoczesnych narzędzi informatycznych udostępnionych przez Policję – Krajową Mapę Zagrożeń Bezpieczeństwa, a następnie odniesiono się do potencjalnych zagrożeń bezpieczeństwa informacji związanych z jej utworzeniem i prowadzeniem.

Krajowa Mapa Zagrożeń Bezpieczeństwa

Celem wdrożenia Krajowej Mapy Zagrożeń Bezpieczeństwa (KMZB) stało się *rzetelne i czytelne zidentyfikowanie i przedstawienie, w tym społecznościom lokalnym, skali i rodzaju zagrożeń oraz instytucji współodpowiedzialnych za zapewnienie bezpieczeństwa i porządku publicznego* (http://www.policja.pl/pol/mapa-zagrozen-bezpiecze/33880,dok.html). Narzędzie to, traktowane jako istotny element procesu zarządzania bezpieczeństwem publicznym i jednocześnie platforma wymiany informacji o zagrożeniach, realizowana w partnerstwie międzyinstytucjonalnym i społecznym, służyć ma *poprawie bezpieczeństwa i porządku publicznego poprzez włączenie obywateli w wybrane działania Policji*

oraz dostosowaniu struktur organizacyjnych i działań Policji do zagrożeń wskazywanych przez społeczeństwo (https://www.mswia.gov.pl/download/1/27720/prezentacja1708MSWiA.pdf).

Pilotaż KMZB miał miejsce w dniach 1 lipca – 31 sierpnia 2016 r. i objął obszar województwa pomorskiego, podlaskiego oraz garnizonu stołecznego. Po tym okresie, program wdrażany był stopniowo na terenie poszczególnych województw (od 9 września województwa: lubuskie i kujawsko-pomorskie; od 14 września województwa: śląskie, małopolskie, lubelskie, łódzkie i warmińsko-mazurskie; od 20 września województwa: wielkopolskie, podkarpackie, mazowieckie, opolskie i zachodniopomorskie; od 5 października województwa: dolnośląskie i świętokrzyskie).

KMZB opiera się o informacje skatalogowane w trzech płaszczyznach:

- informacje gromadzone w policyjnych systemach informatycznych,
- informacje pozyskiwane od społeczeństwa w trakcie bezpośrednich kontaktów z obywatelami, z przedstawicielami samorządu terytorialnego, organizacji pozarządowych itp., a także w trakcie realizowanych debat społecznych poświęconych bezpieczeństwu publicznemu,
- informacje pozyskiwane od obywateli (internautów) z wykorzystaniem platformy wymiany informacji (http://www.policja.pl/pol/mapa-zagrozen-bezpiecze/33880,dok.html).

Każdy mieszkaniec może zgłosić na interaktywnej mapie (rys. 1) zagrożone miejsce, które podlega sprawdzeniu przez Policję. Jednocześnie należy pamiętać, iż strona nie służy do zgłaszania potrzeby pilnej interwencji Policji (w tego typu przypadkach należy korzystać z numerów alarmowych 112, 997), stąd apel o odpowiedzialne korzystanie z aplikacji.

Rys. 1. Krajowa Mapa Zagrożeń Bezpieczeństwa

Źródło: https://mapy.geoportal.gov.pl/iMapLite/KMZBPublic.html.

Aby obywatel mógł skorzystać z możliwości zgłoszenia zagrożenia bezpieczeństwa publicznego na mapie, po wpisaniu adresu URL w przeglądarce internetowej musi zaakceptować zapisy regulaminu serwisu internetowego.

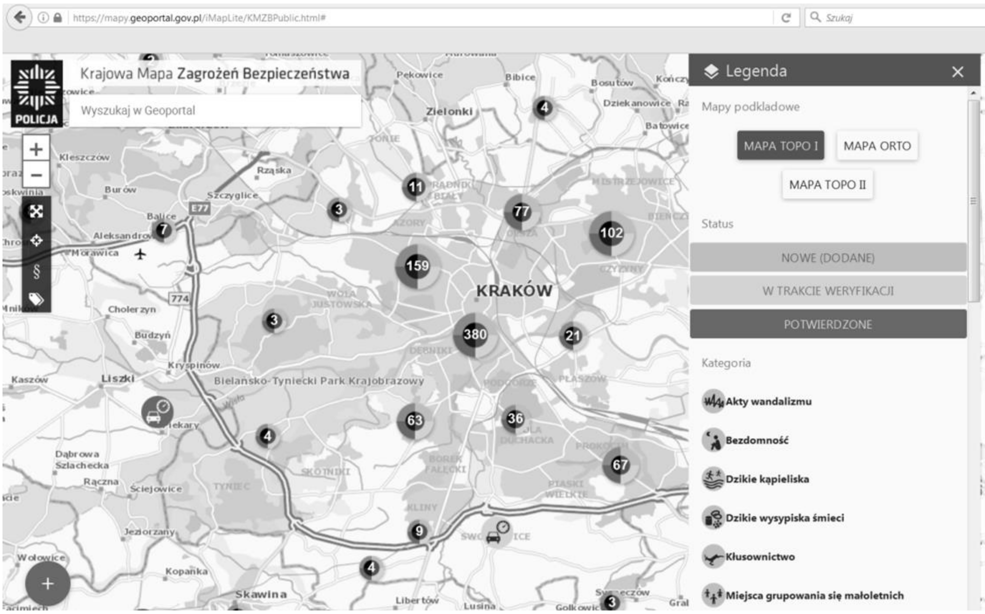
W regulaminie podkreśla się, iż użytkownik korzystający ze zbiorów i usług danych KMZB zobowiązany jest do przestrzegania obowiązującego prawa, norm społecznych i obyczajowych oraz postanowień regulaminu. Administrator danych, którym jest Komendant Główny Policji, może – ze względów bezpieczeństwa oraz z powodu innych przyczyn od niego niezależnych – czasowo zawiesić dostęp do serwisu. Zaznacza się, iż KMZB ma charakter wyłącznie poglądowy. Zasoby tego serwisu i generowane przez użytkownika mapy nie mogą być traktowane jako dokumenty oficjalne oraz nie mogą być podstawą jakichkolwiek czynności sądowych czy administracyjnych.

Należy zwrócić uwagę, iż korzystanie ze zbiorów danych przestrzennych KMZB odbywa się za pomocą usług przeglądania i wyszukiwania danych przestrzennych opublikowanych w infrastrukturze systemu Geoportal (www.geoportal.gov.pl), co jest równoznaczne z akceptacją jego regulaminu. Precyzuje on rodzaje i zakres świadczonych usług, a także warunki i zasady korzystania z danych i usług przez usługobiorców, tj. osoby fizyczne, prawne, organy administracji lub jednostki organizacyjne nieposiadające osobowości prawnej, które korzystają z zasobów Geoportalu.

Co istotne, użytkownik może dokonać zgłoszenia za pomocą serwisu z tego samego adresu IP jedynie raz na dobę. Ponadto, podczas korzystania z serwisu KMZB zabrania się wykorzystywania wirusów, botów, robaków oraz innych kodów komputerowych, skryptów lub programów, które przerywają, niszczą bądź ograniczają działanie KMZB lub jej infrastruktury technicznej, albo w inny sposób umożliwiają nieuprawnione korzystanie lub dostęp do infrastruktury technicznej systemu. Zakazuje się także wykorzystywania kodów komputerowych, skryptów lub programów automatyzujących korzystanie z usług udostępnionych przez KMZB. W regulaminie pojawia się również informacja, iż strona używa tzw. „cookies”, które identyfikują dane komputera i przeglądarki używanych do przeszukiwania stron internetowych. „Ciasteczka” nie służą jednak identyfikacji użytkowników i na ich podstawie w żaden sposób nie jest ustalana czyjakolwiek tożsamość.

Po zatwierdzeniu regulaminu, na stronie pojawia się okno mapy zawierające wszystkie zgłoszenia dodane przez użytkowników serwisu. Informacje prezentowane na mapach uwzględniają zarówno wybrane kategorie przestępstw i wykroczeń, jak i zagrożenia, które w subiektywnym odczuciu mieszkańców negatywnie wpływają na ich poczucie bezpieczeństwa. Narzędzia umieszczone w serwisie umożliwiają przybliżenie bądź oddalenie mapy oraz wyszukanie dowolnego miejsca. Poniżej (rys. 2) zaprezentowano mapę ze zgłoszeniami dokonanymi w Krakowie (stan na dzień 4.01.2017).

Rys. 2. Zgłoszenia dokonane w Krakowie w ramach Krajowej Mapy Zagrożeń Bezpieczeństwa



Źródło: https://mapy.geoportal.gov.pl/iMapLite/KMZBPublic.html.

Jak widać, istnieją trzy kategorie zgłoszeń: zgłoszenia nowe (dodane), w trakcie weryfikacji oraz potwierdzone. Użytkownik korzystać może z różnych podkładów map, tj. dwóch rodzajów map topograficznych oraz ortofotomapy.

W celu dodania zgłoszenia na mapie, należy wybrać ikonę „+" znajdującą się w lewym dolnym rogu serwisu. Następnie, pojawi się 25 uporządkowanych alfabetycznie kategorii zgłoszeń, spośród których należy wybrać jedną (są to m.in. akty wandalizmu, bezdomność, miejsca grupowania się nieletnich, nieprawidłowe oznakowanie drogi, nieprawidłowe parkowanie, niszczenie zieleni, żebractwo i in.). Kolejną czynnością jest dodanie szczegółów zgłoszenia, tj. wskazanie miejsca na mapie oraz daty zaistniałego zdarzenia. Po zatwierdzeniu, pojawia się informacja o przyjęciu zgłoszenia. Dodanie zgłoszenia odbywa się w sposób anonimowy.

Eksperyment przeprowadzony przez autorkę w dniu 27 grudnia 2016 r. dotyczył zgłoszenia nieprawidłowego parkowania na ul. Krupniczej w Krakowie i wykazał, że reakcja na zgłoszenie wynosi ok. godziny, natomiast weryfikacja jego statusu na mapie – do około 8-10 godzin od momentu zatwierdzenia zgłoszenia (czas reakcji uzależniony jest m.in. od liczby zgłoszeń, pilnych interwencji telefonicznych w danym dniu, dostępności funkcjonariuszy w danym czasie i in.).

Zagrożenia bezpieczeństwa informacyjnego na przykładzie KMZB

Krajowa Mapa Zagrożeń Bezpieczeństwa jest interesującym interaktywnym narzędziem, jednak należy zwrócić uwagę na szereg luk oraz niedociągnięć, które przyczynić się mogą do zaistnienia sytuacji nadużywania owego narzędzia oraz spowodowania sytuacji stworzenia zagrożenia bezpieczeństwa systemu informacyjnego Policji.

W kontekście wcześniejszych rozważań dotyczących zagrożeń bezpieczeństwa informacyjnego, w poniższej tabeli (tab. 1) zestawiono, a następnie opisano, możliwe rodzaje zagrożeń wraz z odpowiadającymi im sposobami włamań do systemów informacyjnych, odnosząc je do Krajowej Mapy Zagrożeń Bezpieczeństwa. W analizie skupiono się na tradycyjnych zagrożeniach informacyjnych oraz zagrożeniach technologicznych, pomijając zagrożenia losowe oraz te odnoszące się do praw obywatelskich osób lub grup społecznych, jako iż w opinii autorki przede wszystkim dwa pierwsze rodzaje stanowią główne źródło zagrożeń w przypadku tego konkretnego narzędzia informatycznego. Ponadto, analizę ograniczono do zagrożeń jedynie zewnętrznych, nie uwzględniając zagrożeń pojawiających się w wyniku wypadku, awarii, katastrofy lub innego nieprzewidzianego zdarzenia, a także ewentualności generowania owych zagrożeń wewnątrz samej organizacji (w tym przypadku Policji).

Tab. 1. Rodzaje zagrożeń bezpieczeństwa informacyjnego i sposoby włamań na przykładzie KMZB

	Rodzaj zagrożenia	**Sposoby włamań do systemu informacyjnego**	**Przykład KMZB**
1a.	Tradycyjne zagrożenia informacyjne	Zmowa kilku sprawców Celowe inicjowanie awarii Wywoływanie fałszywych alarmów	Celowe, wielokrotne zgłaszanie fałszywych przestępstw i wykroczeń przez pojedyncze osoby lub zorganizowane większe grupy
2a.		Przypadkowe inicjowanie awarii Wywoływanie fałszywych alarmów	Przypadkowe zgłaszanie fałszywych przestępstw i wykroczeń przez pojedyncze osoby, wynikające m.in. z niedostatecznej znajomości obsługi systemu/programu
3a.		Szantaż	Notoryczne zgłaszanie drobnych wykroczeń w celu zaszantażowania danej osoby lub grupy osób
1b.	Zagrożenia technologiczne	Zmowa kilku sprawców Celowe inicjowanie awarii Wywoływanie fałszywych alarmów Wpuszczanie wirusów, bakterii, robaków, koni trojańskich, bomb logicznych oraz innych groźnych aplikacji destabilizujących sprawność sytemu Wykorzystywanie luk w zabezpieczeniach dostępu do serwisu informacyjnego Techniki obchodzenia zabezpieczeń	Celowe inicjowanie awarii w całym systemie KMZB powodujące jego ogólną destabilizację

Źródło: opracowanie własne.

Rozpoczynając od tradycyjnych zagrożeń informacyjnych, należy zauważyć, iż użytkownicy korzystający z serwisu KMZB mogą pojedynczo lub też w większych grupach wielokrotnie zgłaszać fałszywe przestępstwa i wykroczenia, które w rzeczywistości nie miały miejsca. Jest to ułatwione dzięki możliwości anonimowego zgłaszania danego incydentu. Oznacza to, iż korzystać z serwisu może każdy bez wyjątku – bez konieczności podawania jakichkolwiek danych weryfikujących tożsamość (np. imienia i nazwiska, daty urodzenia, loginu i in.). Jedynym obostrzeniem jest dodawanie zgłoszenia z tego samego adresu IP raz na dobę, co w żaden sposób nie ogranicza użytkownika, ponieważ może on korzystać z różnych komputerów w tym samym czasie lub niedługim odstępie czasowym (komputery innych domowników, komputery w kawiarni internetowej i in.). W związku z tym, iż Policja zareagować musi na każde zgłoszenie, takie działanie może prowadzić do chaosu informacyjnego.

Wielokrotnie zgłaszane w danym rejonie zdarzenie, które w rzeczywistości nie miało miejsca (np. nielegalna wycinka drzew, picie alkoholu w miejscu niedozwolonym czy przekraczanie dozwolonej prędkości) spowodować może „uśpienie czujności" Policji, która podczas otrzymywania prawdziwych powiadomień reagować będzie w sposób opieszały, kierując się wcześniejszymi doświadczeniami w związku z pojawiającymi się fałszywymi zgłoszeniami. Istnieje zatem prawdopodobieństwo, iż potrzebujący pomocy mieszkaniec nie otrzyma wsparcia na czas – nawet, jeśli zgłoszenie nie jest na tyle pilne, aby dzwonić pod numer alarmowy, przez opieszałość i „uśpienie czujności" może minąć czas, w którym uda się Policji potwierdzić zasadność zgłoszonego wydarzenia.

Tego typu działania wiążą się ponadto z angażowaniem sił i środków Policji, co pociąga za sobą generowane w sposób nieuzasadniony koszty. Jednocześnie sytuacje wywoływania fałszywych alarmów zajmują czas (identyfikacja przyjmowanych zgłoszeń, czas dojazdu funkcjonariuszy na miejsce, czas powrotu), co jest szczególnie niepożądane i niebezpieczne wtedy, gdy w tym samym czasie mają miejsce inne, pilne i wymagające rzeczywistej interwencji Policji incydenty.

Celem tego typu działań może być nie tylko szeroko rozumiana ofensywna dezinformacja, ale również chęć pozyskania ważnych informacji, np. szybkości czasu reakcji Policji w danym rejonie, ogólnej reakcji funkcjonariuszy na fałszywe zgłoszenia (czy i jak reagują na dane doniesienie) czy też sposobu reakcji na poszczególne typy przestępstw i wykroczeń. Takie obserwacje posłużyć mogą potencjalnemu sprawcy do lepszego przygotowania się do ewentualnych przestępstw na mniejszą lub większą skalę. Warto zwrócić uwagę na to, iż wizualizacja danych przestrzennych na mapie również przyczynić się może do lepszego rozpoznania danego obszaru przez potencjalnego obywatela chcącego popełnić wykroczenie lub przestępstwo, np. poprzez dostarczenie informacji o rejonach, w których aktywność mieszkańców zgłaszających potwierdzone już zgłoszenia jest wysoka (a zatem mieszkańcy są uważni i chętnie współpracują

z Policją) lub rejony, które zwracają uwagę dużą liczbą potwierdzonych zgłoszeń o jednym, konkretnym typie (np. duża liczba potwierdzonych incydentów związanych z nieprawidłowym parkowaniem powinna sugerować, iż należy uważać na popełnianie tego typu wykroczenia na danym obszarze).

Poza działaniami celowymi, istnieje również możliwość wywołania chaosu informacyjnego na skutek przypadkowego, nieuświadomionego przez użytkownika działania. Może być to konsekwencją kilku czynników. Jednym z nich jest niedostateczna znajomość procedur lub przepisów, w tym przypadku regulaminu KMZB. Mimowolne zaakceptowanie regulaminu, w którym znajdują się istotne dla użytkownika informacje, sprawić może, iż użytkownik nie zrozumie warunków i ograniczeń wynikających z korzystania z systemu. Na przykład w sytuacji dokonania niewłaściwego zgłoszenia (przypadkowe zaznaczenie i potwierdzenie miejsca wystąpienia zagrożenia), użytkownik nie będzie miał możliwości dokonania kolejnego zgłoszenia, które faktycznie miało miejsce. Twórcy KMZB przygotowali się na sytuację występowania nieświadomych zachowań użytkownika w postaci przypadkowych „kliknięć" na mapę – każde zgłoszenie należy potwierdzić ponownie, wprowadzając datę zdarzenia. Mimo to, należy liczyć się z sytuacjami przypadkowych zgłoszeń w następstwie zabawy lub sprawdzania, czy KMZB faktycznie działa itp. (zarówno ze strony dzieci, jak i dorosłych).

Kolejnym sposobem związanym z tradycyjnymi zagrożeniami informacyjnymi jest szantaż. Użytkownicy mogą w sposób nieskrępowany zgłaszać każde, nawet najmniejsze zauważone wykroczenie, kierując się chęcią zaszantażowania danej osoby bądź grupy osób. Działania takie mogą być powodowane również pobudkami psychologicznymi (np. konfliktami sąsiedzkimi, kłopotami emocjonalnymi lub nawet chorobami psychicznymi). Prowadzić to może do nieprawidłowych motywacji używania narzędzia, jakim jest KMZB, czego dodatkowym skutkiem stanie się narastająca niechęć i frustracja ze strony obejmowanych notorycznymi karami użytkowników, którzy zdają sobie sprawę z pobudek kierujących osobami zgłaszającymi wobec nich konkretny incydent. W rezultacie, wpłynąć to może na ogólną negatywną ocenę Policji i używanych przez nią tego typu nowoczesnych narzędzi, powodując w przyszłości negatywne podejście do współpracy z tą służbą.

Istotne zagrożenia związane są ponadto z wszelkimi działaniami destabilizującymi funkcjonowanie systemu Krajowej Mapy Zagrożeń Bezpieczeństwa. Mimo, iż w regulaminie istnieje zapis o zakazie wykorzystywania wirusów, bakterii, botów i innych kodów komputerowych w czasie użytkowania serwisu, wiadomym jest, iż w dobie cyberterroryzmu i zaawansowanych metod włamań do komputerów czy całych systemów informatycznych, zaistnienie tego typu zagrożeń spowodowanych działaniami jednej bądź większej liczby osób nie jest niemożliwe. Skutkować to może istotnym zagrożeniem całości zasobów

informacyjnych Policji, nie tylko tych związanych z Krajową Mapą Zagrożeń Bezpieczeństwa, ale przede wszystkim istotnych danych i informacji mających realny wpływ na bezpieczeństwo całego państwa.

Propozycje i wnioski

Na podstawie powyższego, syntetycznego opracowania wybranych najważniejszych potencjalnych zagrożeń i sposobów włamań możliwych do stosowania przez użytkowników KMZB, zasadną wydaje się propozycja wprowadzenia zmian, które usprawnią działanie systemu oraz wyeliminują przynajmniej część potencjalnych zagrożeń wpływających na szeroko rozumiane bezpieczeństwo informacyjne Policji.

Jednym z sugerowanych przez autorkę rozwiązań mogłoby być wprowadzenie odpowiednich regulacji związanych z weryfikacją tożsamości użytkownika systemu. Obostrzenia te nie powinny dotyczyć przeglądania samej mapy, a jedynie sytuacji, w której obywatel chce dokonać konkretnego zgłoszenia. Należy zwrócić uwagę, iż obowiązek logowania się i wpisywania danych (np. imienia i nazwiska) budzić może opór tej części obywateli, którzy z jakichś względów chcą pozostać anonimowi. Warto pamiętać równocześnie, iż anonimowość zapewniają zgłoszenia telefoniczne – KMZB nie jest ostateczną i jedyną drogą informowania o wykroczeniach czy przestępstwach, a zatem użytkownicy chcący przekazać tą drogą informacje mogą i powinni liczyć się z obowiązkiem weryfikacji ich tożsamości.

Sugerowane rozwiązanie dotyczyć mogłoby zatem rejestracji w systemie za pomocą podawania loginu i hasła z ewentualną możliwością potwierdzenia logowania się do systemu poprzez istniejący adres e-mail. Tego typu regulacja mogłaby zniechęcać potencjalnych użytkowników chcących bez żadnych ograniczeń, w sposób celowy przekazywać fałszywe informacje. Inne sposoby weryfikacji tożsamości użytkownika, jak np. podawanie adresu zamieszkania, daty urodzenia czy numeru PESEL, są bezzasadne, gdyż stanowiłyby naruszenie m.in. prawa obywateli do prywatności.

Proponowanym rozwiązaniem mogłoby być również blokowanie możliwości wysyłania zgłoszeń z tych adresów IP, z których kilkukrotnie wysyłane były nieprawdziwe zgłoszenia. Blokowanie danego adresu IP mogłoby obowiązywać przez określony czas (np. przez miesiąc, dwa miesiące lub kwartał), w zależności od preferencji danego Komisariatu Policji. Pozwoliłoby to na uniknięcie fałszywych zgłoszeń, a jednocześnie umożliwiło mieszkańcom współpracę z Policją.

Należy również wskazać, iż ułatwieniem dla weryfikacji zgłoszenia mogłoby być umożliwienie użytkownikom załączania w formie plików informacji stanowiących dowód zaistniałego przestępstwa lub wykroczenia (np. zdjęć, filmów). Taka możliwość mogłaby przyczynić się do zmniejszenia chaosu informacyjnego wynikającego np. z pojawiania się zgłoszeń, które mogą wydać się

wątpliwe lub dyskusyjne ze względu chociażby na powiązanie określonego typu przestępstwa lub wykroczenia z danym miejscem, czasem jego wystąpienia i in.

Podsumowując powyższe rozważania, należy podkreślić, iż twórcy oraz koordynatorzy Krajowej Mapy Zagrożeń Bezpieczeństwa powinny liczyć się z możliwością występowania wielu różnych zagrożeń bezpieczeństwa systemu informacyjnego. Istotna w tym względzie jest zatem bieżąca identyfikacja potencjalnych zagrożeń oraz szybka, a jednocześnie przemyślana korekta wprowadzanych rozwiązań tak, aby system ten spełniał jak najlepiej swoje zadania, przyczyniając się do realnej poprawy bezpieczeństwa obywateli.

Mimo istnienia potencjalnych zagrożeń systemu oraz krótkiego okresu funkcjonowania, Krajową Mapę Zagrożeń Bezpieczeństwa ocenić można jako przydatne narzędzie potrzebne obywatelom. Świadczy o tym między innymi systematycznie rosnąca ilość dokonywanych na terenie całej Polski zgłoszeń, posiadających status zgłoszeń potwierdzonych. Warto jednak dodać, iż aby w pełni i w wymierny sposób korzystanie z KMZB wpływało na poczucie bezpieczeństwa obywateli, wymagana jest duża dojrzałość i świadomość społeczeństwa zarówno emocjonalna, jak i informacyjna.

Bibliografia

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

Geoportal. Dostęp: 4.01.2017. Tryb dostępu: www.geoportal.gov.pl.

Janczak, J. (2001) *Zakłócenia informacyjne*. Warszawa: Wydawnictwo AON.

Janczak, J., Nowak, A. (2013) *Bezpieczeństwo informacyjne. Wybrane problemy*. Warszawa: Wydawnictwo AON.

Krajowa Mapa Zagrożeń Bezpieczeństwa. Dostęp: 4.01.2017. Tryb dostępu: https://mapy.geoportal.gov.pl/iMapLite/KMZBPublic.html.

Krajowa Mapa Zagrożeń Bezpieczeństwa (portal Policji). Dostęp: 4.01.2017. Tryb dostępu: http://www.policja.pl/pol/mapa-zagrozen-bezpiecze/33880,dok.html.

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

Łuczak, J. (red.) (2004) *Zarządzanie bezpieczeństwem informacji*. Poznań: Oficyna Współczesna.

Madej, M. (2009) *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*. W: Madej,

M., Terlikowski, M. (red.), *Bezpieczeństwo teleinformatyczne państwa*. Warszawa: Wydawnictwo PISM, s. 17-40.

Nowak, E., Nowak, M. (2011) *Zarys teorii bezpieczeństwa narodowego*. Warszawa: Difin.

Potejko, P. (2009) *Bezpieczeństwo informacyjne*. W: Wojtaszczyk, K. A., Materska-Sosnowska, A. (red.), *Bezpieczeństwo państwa*. Warszawa: Oficyna Wydawnicza ASPRA-JR, s. 194.

Prezentacja pilotażu Krajowej Mapy Zagrożeń Bezpieczeństwa (MSWiA). Dostęp: 4.01.2017. Tryb dostępu: https://www.mswia.gov.pl/download/1/27720/prezentacja1708MSWiA.pdf.

Ura, E., Pieprzny, S. (2015) *Bezpieczeństwo wewnętrznego państwa*. Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego.

Wrzosek, M. (2013) *Współczesne zagrożenia w obszarze bezpieczeństwa europejskiego. Warszawa:* Wydawnictwo Menedżerskie PTM.

Żebrowski, A., Kwiatkowski, M. (2000) *Bezpieczeństwo informacji III Rzeczypospolitej*. Kraków: Oficyna Wydawnicza Abrys.

Streszczenie

Artykuł przedstawia główne zagrożenia identyfikowane w obszarze bezpieczeństwa informacyjnego oraz związane z nimi sposoby włamań do systemów informatycznych w odniesieniu do wybranego narzędzia informatycznego – Krajowej Mapy Zagrożeń Bezpieczeństwa (KMZB). W pierwszej części pracy zaprezentowano aparatorium pojęciowe oraz przedstawiono względnie zamknięty zbiór głównych zagrożeń identyfikowanych w obszarze bezpieczeństwa informacyjnego. Następnie, opisano działanie systemu KMZB oraz wyodrębniono rodzaje zagrożeń i sposoby włamań. Pracę wieńczą wnioski oraz autorskie propozycje wstępnych zmian, których zastosowanie przyczynić się może do zmniejszenia zagrożeń systemu bezpieczeństwa informacyjnego Policji.

Słowa kluczowe: bezpieczeństwo informacyjne, zagrożenia bezpieczeństwa informacyjnego, Krajowa Mapa Zagrożeń Bezpieczeństwa, Policja

Information security threats on the example of Polish National Map of Security Threats

Abstract

This paper presents main threats identified in the field of information security as well as various ways of breaks into information systems in regard to specific computer tool – Polish National Map of Security Threats (PNMST). In the first part, main definitions were explained. Then, the system of PNMST and different threats with ways of breaks on the example of PNMST were described. The last part presents conclusions and author's suggestions of changes, which can reduce threats of Police's information security system.

Keywords: information security, information security threats, Polish National Map of Security Threats, Police