dr hab. Henryk Wyrębek, prof. UPH[a)*], dr Paweł Szmitkowski[a)]

[a)]*Wydział Humanistyczny, Uniwersytet Przyrodniczo-Humanistyczy w Siedlcach / Faculty of Humanities, Siedlce University of National Sciences and Humanities*
**Autor korespondencyjny/Corresponding author: henryk.wyrebek@uph.edu.pl*

Koncepcja interaktywnego systemu ostrzegania i alarmowania ludności o zagrożeniach

A Concept of an Interactive Threat Warning System

Концепция интерактивной системы предупреждения и сигнализации о угрозах для людей

ABSTRAKT

Cel: Celem artykułu jest przedstawienie wyników badań wstępnych mających na celu poznanie opinii ludności cywilnej na temat potrzeby i możliwości wprowadzenia do powszechnego użytku aplikacji na smartfony oraz komputery stacjonarne pozwalającej przekazywać informacje o zagrożeniach w czasie rzeczywistym. Uzyskane dane, po uprzedniej weryfikacji i autoryzacji przez właściwe centrum dyspozycyjne, będą elementem systemu monitorowania zagrożeń oraz ostrzegania i alarmowania o zagrożeniach.
Projekt i metody: W badaniach posłużono się metodą sondażu diagnostycznego. Przy wykorzystaniu odpowiedniej techniki pozwala ona stosunkowo szybko i rzetelnie przeprowadzić badania w licznej grupie respondentów. W tym przypadku techniką była ankieta. Opracowane dla niej narzędzie składało się z siedmiu pytań merytorycznych, które posłużyły do zbadania opinii ludności cywilnej na temat potrzeby zaprojektowania aplikacji pozwalającej obywatelom aktywnie uczestniczyć w przekazywaniu informacji o zagrożeniach.
Wyniki: Uzyskane wyniki świadczą o zainteresowaniu respondentów projektowanym narzędziem oraz na względne zrozumienie istoty jego działania. Co oczywiste, pojawiają się rozbieżności w zakresie jego ostatecznego kształtu i przeznaczenia. Pewien niepokój budzą odpowiedzi wskazujące na to, że narzędzie będzie wykorzystywane przede wszystkim przez służby, inspekcje i straże, ale wydaje się, że te odpowiedzi wynikają z pewnej niewiedzy i nieświadomości badanych. Kampania społeczna oraz stosowne instrukcje będące elementem aplikacji powinny to zmienić.
Wnioski: Analizując wyniki przeprowadzonych badań, można wysnuć następujące wnioski:
– Istnieje bezsporna potrzeba opracowania interaktywnej aplikacji pozwalającej ludności cywilnej na czynny udział w procesie monitorowania zagrożeń.
– Niezbędne wydaje się powołanie komórek, które na szczeblach lokalnych, tj. w powiatach, będą weryfikować napływające informacje o zagrożeniach.
– Niezwykle ważne jest merytoryczne oraz wolicjonalne i etyczne przygotowanie ludności cywilnej do korzystania z aplikacji.
– Aplikacja musi mieć jasno zredagowaną instrukcję i samouczek. Zalecane jest opracowanie analogicznych i w pełni kompatybilnych wersji aplikacji na urządzenia przenośne oraz stacjonarne.
– Konieczne jest zaszczepienie w ludności cywilnej przekonania o potrzebie i celowości użycia aplikacji.
Słowa kluczowe: monitorowanie zagrożeń, zagrożenie, ostrzeganie, alarmowanie, system zarządzania kryzysowego
Typ artykułu: studium przypadku

Przyjęty: 19.02.2018; Zrecenzowany: 26.06.2018; Zatwierdzony: 05.07.2018;
Autorzy wnieśli równy wkład merytoryczny w opracowanie artykułu;
Identyfikatory ORCID autorów: H. Wyrębek – 0000-0001-9801-6905; P. Szmitkowski – 0000-0001-9288-9182;
Proszę cytować: BiTP Vol. 50 Issue 2, 2018, pp. 142–156, doi: 10.12845/bitp.50.2.2018.11;

ABSTRACT

Aim: The aim of this article is to present the results of the initial research aiming at gathering civilian population's opinions on whether it is necessary and possible to introduce into common use smart-phone and desktop applications for real-time threat warning. The data collected, following their verification and authorisation by the relevant dispatch centre, will become part of the system of monitoring, warning and alarming about possible threats.
Project and methods: In the research use was made of the diagnostic survey method for the collection of data. With an appropriate technique, this method makes it possible to survey a large group of respondents relatively fast and reliably. In this case, the technique employed was the questionnaire. The tool developed for this questionnaire consisted of seven content-related questions designed to investigate into people's opinions on whether there was a need for designing an app to provide a greater level of citizen involvement in disseminating information on threats.
Results: The results suggest that the respondents showed interest in the tool's being designed, and a relatively good understanding of how it should essentially work. Obviously, there were some discrepancies in the responses with regard to its final form and function. The responses indicating that this

tool will primarily be used by the services, inspections, brigades and guards might be a cause for concern, although it seems that these answers result from a lack of knowledge and awareness on the part of the respondents. A public awareness campaign and in-app instructions should be sufficient to change this perception.

Conclusions: An analysis of the survey results has led to the following conclusions:

- There is a need to develop an interactive app which would allow civilians to become actively involved in the process of monitoring threats;
- It seems necessary to establish units (dispatch centres), to verify the information received at the local level, i.e. in districts (powiat).
- An extremely important element in the process of implementing the application for general use is to prepare the public in terms of the relevant knowledge, and volitional and ethical aspects;
- The application should have a clear manual and tutorial. It is recommended to develop analogous and fully compatible versions of the app for mobile and stationary devices;
- It is also necessary to convince the public of the need and purposefulness of using the application.

Keywords: monitoring of threats, threat, warning, alarm, crisis management system

Type of article: case study

Received: 19.02.2018; Reviewed: 26.06.2018; Accepted: 05.07.2018;
The authors contributed equally to this article;
Authors' ORCID IDs: H. Wyrębek – 0000-0001-9801-6905; P. Szmitkowski – 0000-0001-9288-9182;
Please cite as: BiTP Vol. 50 Issue 2, 2018, pp.142–156, doi: 10.12845/bitp.50.2.2018.11;

АННОТАЦИЯ

Цель: Цель статьи – представить результаты предварительных исследований, направленных на ознакомление с мнениями гражданского населения о необходимости и возможности внедрения широко распространенных приложений для смартфонов и настольных компьютеров, позволяющих передавать информацию об угрозах в реальном времени. Данные, полученные после предварительной проверки и авторизации соответствующим располагаемым центром, будут частью системы мониторинга опасности, а также предупреждения и предупреждения об угрозах.

Дизайн и методы: В исследовании использовался метод диагностической съемки. Используя соответствующий метод, он позволяет относительно быстрые и надежные исследования у большой группы респондентов. В этом случае эта методика была анкетами. Разработанный для нее инструмент состоял из семи основных вопросов, которые были использованы для исследования гражданского мнения о необходимости разработки приложения, которое позволяет гражданам активно участвовать в передаче информации об угрозах.

Результаты: полученные результаты указывают на интерес респондентов в разработанном инструменте и относительное понимание сущности его функционирования. Очевидно, что есть расхождения в его окончательной форме и цели. Некоторое беспокойство вызвано ответами, свидетельствующими о том, что этот инструмент будет использоваться в первую очередь службами, инспекциями и охранниками, но, похоже, эти ответы являются результатом определенного невежества и незнания респондентов. Социальная кампания и соответствующие инструкции, которые являются частью приложения, должны изменить это.

Выводы. Анализируя результаты проведенных исследований, можно сделать следующие выводы:

- Существует неоспоримая необходимость в разработке интерактивного приложения, которое позволяет гражданским лицам активно участвовать в процессе мониторинга рисков.
- Кажется необходимым настроить ячейки, которые на местном уровне, то есть в повятах, будут проверять входящую информацию об угрозах.
- Существенная и волевая и этическая подготовка гражданского населения к использованию заявки чрезвычайно важна.
- Приложение должно иметь четко определенные инструкции и учебник. Рекомендуется разрабатывать аналогичные и полностью совместимые версии приложений для мобильных и стационарных устройств.
- Необходимо привить гражданскому населению убеждение в необходимости и желательности использования заявки.

Ключевые слова: мониторинг угроз, угроза, предупреждение, тревога, система управления кризисом

Вид статьи: исследование случая

Принята: 19.02.2018; Рецензирована: 26.06.2018; Одобрена: 05.07.2018;
Авторы внесли одинаковый вклад в создание этой статьи;
Идентификаторы ORCID авторов: H. Wyrębek – 0000-0001-9801-6905; P. Szmitkowski – 0000-0001-9288-9182;
Просим ссылаться на статью следующим образом: BiTP Vol. 50 Issue 2, 2018, pp. 142–156, doi: 10.12845/bitp.50.2.2018.11;

Wprowadzenie

Jednym z kluczowych elementów systemu zarządzania kryzysowego w Polsce w zakresie ochrony ludności cywilnej pozostaje ostrzeganie i alarmowanie społeczeństwa o zagrożeniach. Sposoby i algorytmy umożliwiające te przedsięwzięcia ewoluują wraz ze zmianami środków technicznych pozwalających na coraz peł-

Introduction

Public warning and alarm methods designed to protect civilians continue to be one of the key elements of the crisis management system in Poland. The approaches and algorithms underlying these efforts are evolving along with the technologies that allow us to issue communications and alarm signals in a more

niejsze i dokładniejsze przekazywanie komunikatów i sygnałów alarmowych. Analizując te sposoby, można zauważyć pewną prawidłowość. Dotyczą one zagrożeń noszących znamiona sytuacji nadzwyczajnych, a w pewnym okresie także sytuacji wojennych. Możliwości ostrzegania i alarmowania obywateli o zagrożeniach stają się coraz większe ze względu na niemal nieograniczony potencjał techniczny oraz wielorakość środków alarmowania. Aby jednak proces ten był skuteczny, niezbędne jest zebranie informacji o potencjalnych zagrożeniach. Odbywa się to według algorytmu: wykrycie zagrożenia, określenie jego skali i rodzaju oraz podjęcie ewentualnej decyzji o ostrzeganiu lub alarmowaniu.

Obecnie w Polsce funkcjonuje kilka systemów, których zadaniem jest zbieranie informacji o zagrożeniach. Jednym z pierwszych jest System Monitoringu i Osłony Kraju (SMOK), utworzony przez Instytut Meteorologii i Gospodarki Wodnej, a działający od 2005 roku. Powstał on w efekcie tragicznej powodzi w 1997 roku. SMOK ma za zadanie zbieranie informacji o zagrożeniach pogodowych. System ten składa się z:

- ośmiu radarów atmosferycznych POLRAD mających monitorować intensywność oraz rozmieszczenie chmur i opadów;
- systemu burzowego PERUN składającego się z dziewięciu czujników wykrywających i mierzących siłę wyładowań atmosferycznych docierających do ziemi oraz wewnątrz chmur;
- systemu blisko 1000 posterunków pomiarowych zbierających dane o: temperaturze powietrza, opadach, sile i kierunku wiatru oraz poziomie wody, i przekazujących te dane do 30 stacji meteorologiczno-hydrologicznych, a stamtąd – do sieci komputerowej IMGW.

SMOK jest uzupełniany i wspierany przez tworzony od 2010 roku Informatyczny System Osłony Kraju (ISOK), którego głównym zadaniem jest opracowanie map zagrożenia powodziowego i atmosferycznego na terenie Polski. Dzięki zastosowaniu mapowania satelitarnego system ten jest w stanie bardzo dokładnie odzwierciedlić wszelkie zagrożenia pogodowe. Uzyskane dane mogą być różnie wykorzystane przez wyspecjalizowane instytucje państwowe (np. Główny Urząd Geodezji i Kartografii – GUGiK), podmioty administracji publicznej wydające np. pozwolenia budowlane, a nawet zwykłych obywateli.

Scharakteryzowane pokrótce systemy sektorowe znacząco wspiera Krajowy System Wykrywania Skażeń i Alarmowania (KSWSiA). Powstał on na podstawie rozporządzenia Rady Ministrów z dnia 7 stycznia 2013 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach (Dz. U. poz. 96)[1]. Ten akt normatywny reguluje funkcjonowanie KSWSiA, który tworzą:

- System Wykrywania Skażeń Sił Zbrojnych RP – nadzorowany przez Ministra Obrony Narodowej;
- sieci i systemy nadzoru epidemiologicznego i kontroli chorób zakaźnych w kraju oraz krajowe punkty kontaktowe dla międzynarodowych systemów nadzoru nad zagrożeniami zdrowia lub życia dużych grup ludności – nadzorowane przez ministra właściwego do spraw zdrowia;

[1] Rozporządzeniem tym zastąpiono rozporządzenie Rady Ministrów z dnia 16 października 2006 r. w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach (Dz. U. Nr 191, poz. 1415).

comprehensive and detailed way. An analysis of these approaches and algorithms allows a certain pattern to be seen. Namely, they concern situations that can be at least partly viewed as emergencies, and also, at certain times, war situations. The ability to warn and alarm civilians about threats is expanding continuously due to the almost inexhaustible technological potential and the great diversity of alarm measures. However, in order for this process to be effective, it is necessary to collect information on potential threats. This is done according to the following algorithm – detect the threat, determine its scale and type, and make a decision on warming or alarming the population, if required.

Currently, Poland has several systems in place to collect information on threats. One of the oldest is the National Monitoring and Protection System (in Polish: System Monitoringu i Osłony Kraju – SMOK), developed by the Institute of Meteorology and Water Management and launched in 2005. It was established in response to the tragic flood of 1997. SMOK is aimed at collecting information on weather threats. It comprises:

- eight POLRAD weather radars designed to monitor the intensity and distribution of clouds and rainfall;
- the PERUN storm surveillance system which includes nine detectors for identifying and measuring the power of cloud-to-ground and cloud-to-cloud lightning;
- a system of almost 1,000 measurement stations collecting data on temperature, rainfall, strength and direction of wind and water levels, and providing these data to 30 weather and water monitoring stations, from where they are fed to the computer network of the Institute of Meteorology and Water Management.

SMOK is complemented and supported by the Computerised National Protection System (in Polish: System Osłony Kraju – ISOK), whose main task is to lay out flood-risk and weather-threat maps for the whole territory of Poland. Utilising satellite mapping, the system reflects all kinds of weather threats with high precision. The data collected with these systems can be used by specialised state institutions (e.g. the Central Office for Cartography and Geodesy – Główny Urząd Geodezji i Kartografii, GUGiK), public administration bodies issuing building permits and even by private individuals.

These sector-specific systems are substantially supported by the National Contamination Detection and Alarm System (in Polish: Krajowy System Wykrywania Skażeń i Alarmowania – KSWSiA). KSWSiA was developed under the Regulation of the Council of Ministers of 7 January 2013 on threat detection and warning systems, and the responsibility of authorities with regard thereto (Journal of Laws, item 96)[1]. This piece of legislation governs the functioning of KSWSiA, which comprises:

- the Contamination Detection System of the Armed Forces of the Republic of Poland, supervised by the Minister of National Defence;
- domestic epidemiological supervision and infectious disease management systems networks, as well as

[1] This Regulation replaced the Regulation of the Council of Ministers of 16 October 2006 on contamination detection systems and responsibility of authorities with regard thereto (Journal of Laws No. 191, item 1415).

- system stacji wczesnego wykrywania skażeń promieniotwórczych i placówek prowadzących pomiary skażeń promieniotwórczych, których działania koordynuje Prezes Państwowej Agencji Atomistyki;
- nadzorowane przez wojewodów wojewódzkie systemy wykrywania i alarmowania oraz wojewódzkie systemy wczesnego ostrzegania o zagrożeniach, o których mowa w art. 16 ust. 2 pkt 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590, z późn. zm.) i w § 3 pkt 6 rozporządzenia Rady Ministrów z dnia 25 czerwca 2002 r. w sprawie szczegółowego zakresu działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin (Dz. U. Nr 96, poz. 850), w części dotyczącej skażeń;
- systemy nadzoru epizootycznego, fitosanitarnego, nadzoru nad bezpieczeństwem produktów pochodzenia zwierzęcego i nadzoru nad paszami oraz nadzoru nad produktami rolno-spożywczymi – nadzorowane przez ministrów właściwych do spraw rolnictwa i rynków rolnych oraz zdrowia [3].
- Rozporządzenie zawiera także opis obowiązujących na terytorium Rzeczpospolitej Polskiej sygnałów i komunikatów alarmowych. Są one przekazywane w postaci słownej oraz akustycznej przez stacjonarne syreny alarmowe, które dziś swoim zasięgiem obejmują około 76,6% powierzchni kraju [4].

KSWSiA nadaje sygnał alarmowy informujący o niebezpieczeństwie oraz trzy komunikaty alarmowe (uprzedzenia): o zagrożeniu skażeniami, o zagrożeniu zakażeniami oraz o klęskach żywiołowych i zagrożeniu środowiska. Regulacje zawarte w rozporządzeniu w znacznym stopniu ograniczają zakres zagrożeń, o których system może informować. Ponadto jego parametry techniczne sprawiają, że ma on charakter bierny – system przesyła informację w kierunku osoby zagrożonej, ale sam nie odbiera komunikatu od tej osoby.

Obecnie oprócz wyżej opisanego systemu istnieją inne, niemal nieograniczone możliwości techniczne alternatywnego informowania społeczeństwa o zagrożeniach. Jednym z nich jest Regionalny System Ostrzegania (RSO), który jest usługą umożliwiającą powiadamianie ludności cywilnej o zagrożeniach lokalnych. System ten działa wielotorowo. Informowanie odbywa się przede wszystkim za pomocą stron internetowych urzędów wojewódzkich. Ponadto, na podstawie umowy podpisanej 14 października 2013 roku pomiędzy Telewizją Polską S.A. a Ministerstwem Administracji i Cyfryzacji [5], możliwe jest wyświetlenie informacji o zagrożeniu w postaci tzw. paska w naziemnej telewizji cyfrowej, w naziemnym multipleksie cyfrowym MUX-3 (w programach regionalnych): w standardzie HbbTV, w telegazecie, z wykorzystaniem napisów DVB. Usługa dostępna jest także w postaci aplikacji na smartfon lub tablet [6]. Od 1 lipca 2015 roku ostrzeżenia przed najważniejszymi zagrożeniami otrzymujemy również SMS-em [6]. Za pomocą RSO rozpowszechniane są także poradniki postępowania w sytuacjach kryzysowych. Wszystkie komunikaty przygotowywane są przez właściwe terytorialnie wojewódzkie centrum zarządzania kryzysowego.

Dokonana charakterystyka systemów monitorowania zagrożeń oraz ostrzegania i alarmowania o zagrożeniach pozwala zauważyć ich pewien istotny mankament. Wszystkie one mają

- domestic contact points for international systems monitoring health and life threats for large groups of population, supervised by the Minister of Health;
- an early warning system for the detection of radioactive contamination, including facilities conducting measurements of radioactive contamination, coordinated by the National Atomic Energy Agency;
- provincial detection and alarm systems, and provincial early warning systems, supervised by provincial governors, as referred to in Article 16 (2) (3) of the Act of 26 April 2007 on crisis management (Journal of Laws No. 89, item 590, as amended) and § 3 (6) of the Regulation of the Council of Ministers of 25 June 2002 on the detailed scope of operations of the Chief of National Civil Defence, provincial, district and communal chiefs of civil defence (Journal of Laws No. 96, item 850), with regard to contamination;
- episootic, phytosanitary, animal product safety, fodder and agri-food product monitoring systems, supervised by ministers in charge of agriculture, agricultural markets and health [3].

The Regulation also contains a description of the alarm signals and communications applicable on the territory of Poland. They are issued in verbal and acoustic forms by stationary alarm sirens, whose current range covers about 76.6 percent of the country's area [4].

KSWSiA issues alarm signals to warn against a threat, and three alarm communications (warnings) to warn against contamination threats, natural disasters and environmental threats. The provisions of the Regulation substantially restrict the scope of threats against which the system may warn the population. Moreover, due to its technical characteristics, this is a passive system – that is, one which sends information to people exposed to the threat, but does not receive communications from the people.

Currently, in addition to the system described above, there are almost limitless technological possibilities for alternative solutions to notify the public about pending threats. One of them is the Regional Warning System (in Polish: Regionalny System Ostrzegania – RSO) – a solution designed to notify civilian population of local threats. The system operates on a multi-pronged basis. Notifications are sent primarily through the websites of provincial offices. Furthermore, under the Agreement of 14 October 2013, concluded between Telewizja Polska S.A. (Polish national television) and the Ministry of Administration and Digitisation [5], threat notifications may be displayed as "strips" on digital terrestrial television, on the MUX-3 digital terrestrial multiplex (on regional programmes): in the HbbTV standard, on tele-text and using DVB subtitles. This service is also available as an app for smartphones or tablets [6]. Starting from 1 July 2015, key warnings have also been issued by text messages [6]. RSO also disseminates emergency guides. All communications are prepared by the relevant provincial crisis management centres.

Notably, all the threat monitoring, warning and alarm systems described above have a major drawback. Namely, they send information to people exposed to the threat, but do not

charakter bierny, tzn. przesyłają informację w kierunku osoby zagrożonej, ale same nie odbierają komunikatu od tej osoby. A przecież przekazywane przez obywateli informacje o zaobserwowanych zagrożeniach mogłyby, po odpowiedniej weryfikacji i autoryzacji (np. przez powołane w tym celu stosowne centra weryfikacji danych będące elementem centrów zarządzania kryzysowego), znacząco zwiększyć sprawność i skuteczność działania systemów. W związku z powyższym należy rozważyć rozszerzenie działania istniejących lub opracowanie nowych aplikacji multimedialnych pozwalających na aktywny kontakt obywateli z podmiotami pozyskującymi informacje o niebezpieczeństwach. Oczywiście znacznie wygodniejsze i łatwiejsze do wprowadzenia byłyby rozwiązania będące swego rodzaju „wtyczkami" do rozwiązań już funkcjonujących. Nie wymagałoby to dokonywania daleko idących reform, lecz jedynie zwiększenia istniejących możliwości systemów wykrywania zagrożeń oraz ostrzegania i alarmowania o zagrożeniach.

Warto podkreślić, że podobne aplikacje funkcjonują już w innych krajach, a ich kształt i zastosowanie są bardzo zróżnicowane. Przykładem mogą być narzędzia: Rapid SOS [7], Rescuer [8] czy Emergency Plus [9]. Umożliwiają one kontakt ze służbami ratunkowymi i przekazywanie informacji o właściwych dla danej służby zagrożeniach lub też uzyskanie informacji o sposobie właściwego zachowania się. Projektowana aplikacja idzie o krok dalej i pozwala na przekazywanie większego zakresu danych do centrum dyspozycyjnego, które po weryfikacji i zakwalifikowaniu zgłoszenia może zadysponować nawet kilka służb, inspekcji lub straży.

Hipoteza

Powyższe spostrzeżenia pozwalają sformułować problem badawczy dla przedmiotowych badań w postaci pytania: Czy potrzebne jest zwiększenie interaktywności istniejących systemów monitorowania zagrożeń oraz ostrzegania i alarmowania o zagrożeniach tak, aby w systemach tych mogli brać czynny udział obywatele, oraz na czym powinna polegać ewentualna ich modernizacja zmierzająca w tym kierunku?

Wskazany problem badawczy pozwala na wysunięcie hipotezy będącej punktem wyjścia do dalszych badań. Należy przypuszczać, że można, a wręcz trzeba zwiększyć interaktywność systemów monitorowania zagrożeń oraz ostrzegania i alarmowania o zagrożeniach tak, aby w systemach tych mogli brać czynny udział obywatele. Niezbędna modernizacja powinna polegać na: powołaniu podmiotów weryfikujących i klasyfikujących napływające zgłoszenia, opracowaniu narzędzi (w postaci aplikacji na komputery i urządzenia przenośne) umożliwiających interaktywny kontakt w czasie rzeczywistym z danym podmiotem oraz wyrobieniu w społeczeństwie postawy odpowiedzialnego i racjonalnego korzystania z tych narzędzi.

Metodologia badań

Na potrzeby badań przyjęto, że projektowana aplikacja powinna umożliwiać: zgłaszanie zagrożeń bezpieczeństwa

receive communications from them. This is disadvantageous, as civilian information on observed threats, once verified and authorised (e.g. by dedicated data verification centres operating within crisis management centres), could make the systems work much more effectively and efficiently. Therefore, consideration should be given to expanding the existing, or developing new, multimedia apps which would allow civilians to actively communicate with the institutions that collect threat information. Obviously, the most convenient and easiest way to do this would be by introducing some sort of "plug-ins" to the existing solutions. Such a solution would not require extensive reforms – it would only expand the existing possibilities of threat detection, warning and alarm systems.

It should be mentioned that such apps – representing a great variety of uses and designs – are already in place in other countries. For example, these include such tools as Rapid SOS [7], Rescuer [8] and Emergency Plus [9]. They allow people to contact emergency services and provide information on threats relevant to these services, or to obtain information on what to do in emergency situations. The app being designed goes a step further, allowing people to provide a broader range of information to dispatch centres, which, following verification and qualification, may dispatch even several services, inspections, brigades or guards.

Hypothesis

Based on the above conclusions, a research problem can be formulated for the study, in the form of the following question: Is it necessary to make the existing threat monitoring, warning and alarm systems more interactive so that they could actively involve citizens, and what should such modernisation, if any, involve in order to achieve a greater level of interaction?

This research problem leads to a hypothesis which serves as the starting point for further study. It seems reasonable, if not necessary, to make threat monitoring, warning and alarm systems more interactive, in order to make citizens actively involved in these systems. The following should be done to modernise these systems: establishing authorities that would verify and classify incoming reports, developing tools (as apps for desktop computers or mobile devices) for real-time interaction with these authorities, and helping citizens become responsible and reasonable users of these tools.

Survey methodology

For the purposes of the survey, we assumed that the designed application should allow for reporting threats as texts

 ISSN 1895-8443

w formie tekst ze zdjęciem i lokalizacją na mapie, automatyczną lokalizację zgłaszającego za pomocą GPS, inteligentne rozpoznawanie rodzajów naruszeń bezpieczeństwa, wysyłanie użytkownikom alertów dotyczących zagrożeń w ich najbliższym otoczeniu, szacunkową ocenę ryzyka na wybranym terenie, generowanie lokalnych map ryzyka na podstawie przyjętych kryteriów, korzystanie z niej osobom niepełnosprawnym, oraz obsługę w wielu językach.

W celu przeprowadzenia badań terenowych umożliwiających poznanie opinii obywateli na temat potrzeby stworzenia oraz kształtu ewentualnego narzędzia pozwalającego zwiększyć możliwość uczestnictwa obywateli w procesie zbierania informacji o zagrożeniach oraz ostrzegania i alarmowania o nich posłużono się metodą sondażu diagnostycznego. Przy wykorzystaniu odpowiedniej techniki pozwala ona stosunkowo szybko i rzetelnie przeprowadzić badania w licznej grupie respondentów. W tym przypadku techniką była ankieta. Opracowane dla niej narzędzie składało się z siedmiu pytań merytorycznych, które posłużyły do zbadania opinii ludności cywilnej na temat potrzeby zaprojektowania aplikacji pozwalającej obywatelom aktywnie uczestniczyć w przekazywaniu informacji o zagrożeniach. W sześciu pytaniach zastosowano kafeterię zamkniętą, w jednym pytaniu – kafeterię otwartą.

Badaniami objęto 60 kobiet oraz 50 mężczyzn, pełnoletnich, podzielonych na grupy wiekowe: do 25 lat, 26–35 lat, 36–45 lat, 46–55 lat i powyżej 56 lat. Liczebność próby badawczej wynosząca 110 osób wynika z wielkości populacji generalnej (57 tysięcy) oraz przyjętego błędu maksymalnego (9%) [1]. Badani byli mieszkańcami Siedlec. Przyjęcie tak szerokiego spektrum badań wynika z tego, że obecnie dostęp do środków komunikacji elektronicznej jest powszechny.

Ponieważ w ankiecie znalazły się głównie pytania z kafeterią zamkniętą, więc można było pokusić się przede wszystkim o analizę ilościową zgromadzonego materiału empirycznego.

Jako kluczowe zmienne zależne przyjęto płeć oraz wiek badanych. Uznano bowiem, że mają one zasadnicze znaczenie w kontekście nie tyle sprawnego korzystania z aplikacji, ile odczuwania potrzeby pozyskiwania informacji o zagrożeniach, ich rzetelności i aktualności, a także chęci brania czynnego udziału w przekazywaniu danych o pojawiających się niebezpieczeństwach. Wzięto tutaj pod uwagę również zjawisko tzw. bariery technologicznej polegające na tym, że osoby starsze nie chcą lub boją się korzystać zarówno ze stacjonarnych, jak i mobilnych urządzeń komunikacji elektronicznej.

Na uwagę może zasługiwać także zmienna w postaci miejsca zamieszkania respondentów. Jednakże w metryczce badani zaznaczyli jednolicie miasto od 30 do 100 tys. mieszkańców, co w kontekście interpretacji wyników badań przestaje mieć znaczenie jako punkt odniesienia.

Na podstawie analizy materiału empirycznego uznano, że w kontekście prowadzony badań przedstawianie korelacji między innymi zmiennymi zależnymi, takimi jak miejsce zamieszkania i wykształcenie respondentów, nie rzutuje znacząco na uzyskane wyniki.

Poniżej zaprezentowano główne wyniki badań i wnioski płynące z analizy zgromadzonego materiału badawczego.

with pictures and map locations, automated GPS geolocation, smart threat-type recognition, sending alerts to users on threats in their area, risk estimation for an area, generating local risk maps based on predefined criteria, use by the disabled people, and use in multiple languages.

The diagnostic survey method was employed to conduct field surveys, in order to gather peoples' opinions on whether a tool providing greater citizen involvement in threat monitoring, warning and alarming processes is needed, and what it should possibly involve. With an appropriate technique, this method makes it possible to survey a large group of respondents relatively fast and reliably. In this case, the technique employed was the questionnaire. The tool developed for this questionnaire consisted of seven content-related questions designed to investigate into people's opinions on whether there was a need for designing an app to provide a greater level of citizen involvement in disseminating information on threats. The multiple-choice format was used in six questions, and one question had an open-ended format.

The survey covered 60 adult women and 50 adult men, grouped by age into the following categories: up to 25, 26–35, 36–45, 46–55 and over 56. The sample size of 110 is linked to the general population size (57,000) and the assumed maximum error (9%) [1]. The respondents were all citizens of Siedlce. This broad spectrum of the study is attributable to the current common availability of means of electronic communication.

Since the questionnaire contained mainly multiple-choice questions, the empirical material it provided was appropriate primarily for qualitative analysis.

The age and gender of the respondents were taken as dependent variables, due to their key significance not so much for the app-use efficiency, but for the perceived need to collect information on threats, the reliability and timeliness of such information, as well as the willingness to become actively involved in sharing data on pending threats. For the purposes of the survey, we took account of the "technological-barrier" phenomenon in which elderly people are reluctant or afraid to use both desktops and mobile devices for communication purposes.

Another notable variable involves respondents' place of residence. However, in the demographic information section, the respondents uniformly indicated a city of 30,000 to 100,000 inhabitants, which makes this variable irrelevant as a point of reference for the purposes of interpreting the results.

An analysis of the empirical material led to the conclusion that, in the context of the survey in question, the demonstration of correlations between other dependent variables, such as the place of residence and educational attainment of the respondents, would have little impact on the results.

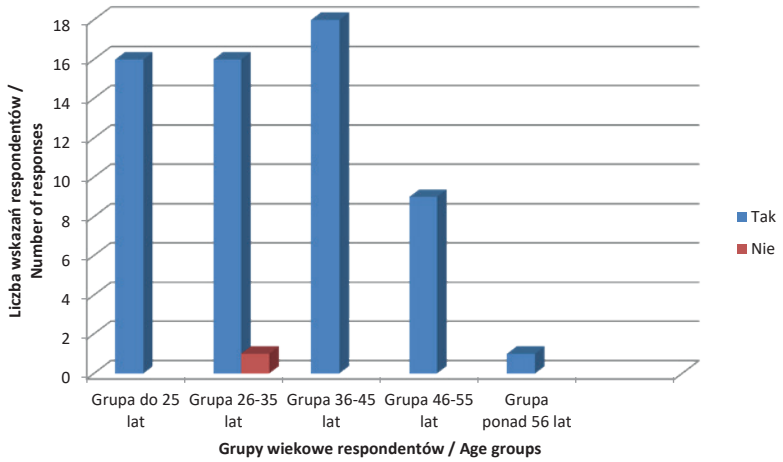
Below are the main results of our surveys and the conclusions drawn from the analysis of the empirical material collected.

Wyniki badań

Większość mężczyzn, niezależnie od grupy wiekowej, na pytanie 1: „Czy chcieliby Państwo być poinformowani o aktualnych zagrożeniach w okolicy?", odpowiedziała twierdząco. Przeczący odpowiedział tylko jeden respondent z grupy wiekowej 26–35 lat. Wydaje się to oczywiste w kontekście licznych kategorii i coraz większego zakresu pojawiających się zagrożeń.

Survey results

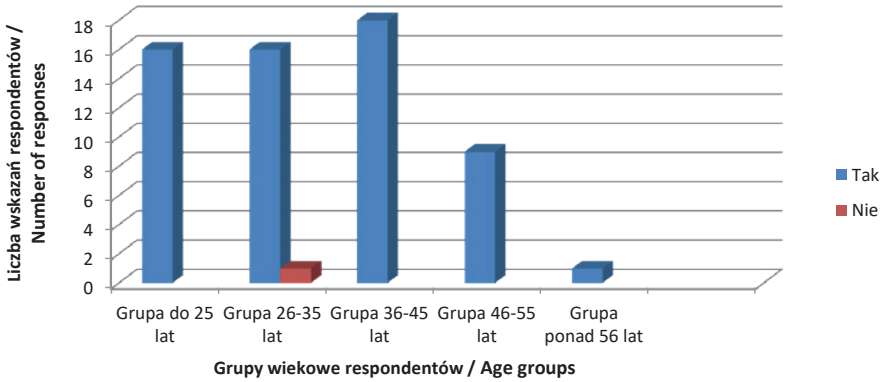
In Question 1: "Would you like to be updated on current threats in your area?", most men, regardless of the age group, gave an affirmative answer. Only one respondent from the group of 26–35-year-olds gave a negative answer to this question. This is hardly surprising, given the broad spectrum of threat categories and their growing range.



Rycina 1. Opinia respondentów na temat chęci bycia informowanym o zagrożeniach
Figure 1. Male respondents' opinion on whether they wished to be notified of threats
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds
Źródło: Opracowanie własne.
Source: Own elaboration.

Na pytanie 2: „Czy aplikacja mająca poniższe cechy będzie dla Państwa interesująca?" (Jako cechy aplikacji wskazano: prostotę i intuicyjność obsługi, powszechną dostępność oraz jasno określony katalog zagrożeń, które mogą być zgłaszane przez użytkownika), większość ankietowanych mężczyzn odpowiedziała twierdząco. Tylko jeden respondent z grupy wiekowej 26–35 lat wyraził dezaprobatę dla kształtu aplikacji.

In Question 2: "Would an app with the following characteristics be of interest to you?" (the app characteristics included simplicity and intuitiveness, common accessibility and a clearly defined catalogue of threats which could be reported), the majority of the male respondents answered "Yes". Only one respondent from the age group of 26–35-year-olds gave a "No" answer to this question.

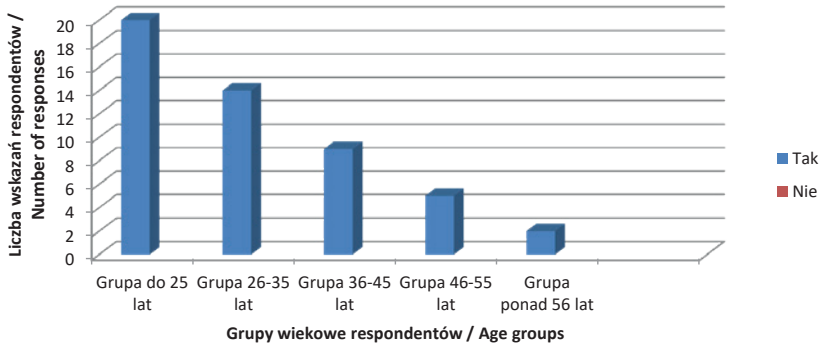


Rycina 2. Opinia respondentów na temat zainteresowania aplikacją
Figure 2. Male respondents' opinion on whether the app was of interest to them
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds
Źródło: Opracowanie własne.
Source: Own elaboration.

ISSN 1895-8443

Z kolei na pytanie 3: „Czy aplikacja powinna udostępniać informacje na temat najbardziej aktualnych zagrożeń?", wszyscy ankietowani mężczyźni odpowiedzieli twierdząco. Biorąc pod uwagę kształt i przeznaczenie aplikacji, trzeba stwierdzić, że jest to najbardziej logiczne i poprawne podejście do zagadnienia.

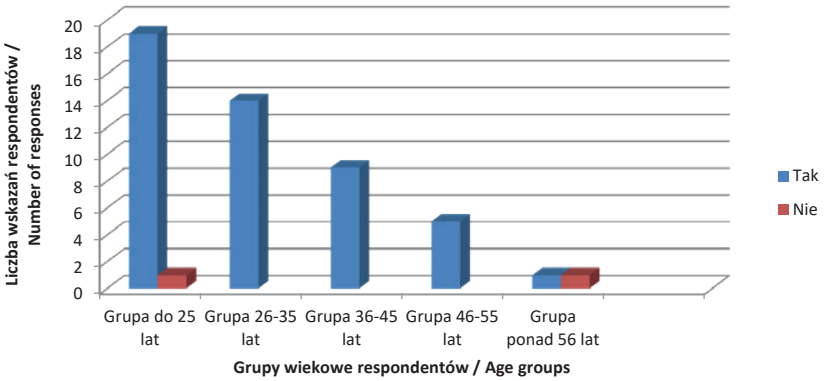
In Question 3: "Should the app provide information on the latest threats?", all the male respondents answered "Yes". Given the design and purpose of the app, this was clearly the most logical and appropriate answer.



Rycina 3. Opinia respondentów na temat udostępniania przez aplikację informacji o najbardziej aktualnych zagrożeniach
Figure 3. Male respondents' opinion on whether they wished to be notified of the latest threats
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds
Źródło: Opracowanie własne.
Source: Own elaboration.

Na pytanie 4: „Czy w aplikacji powinny być zamieszczone komunikaty, instrukcje oraz scenariusze reagowania na poszczególne zagrożenia?", większość badanej grupy mężczyzn odpowiedziała „Tak". Tylko dwie osoby: jedna z grupy wiekowej do 25 lat, a druga z grupy wiekowej powyżej 56 lat, odpowiedziały „Nie".

In Question 4: "Should the app provide communications, instructions and response scenarios for individual threats?", the majority of the male respondents answered "Yes". Only two respondents, one from the group of up-to-25-year-olds, the other from the over-56-year-olds, answered "No" to this question.



Rycina 4. Opinia respondentów na temat elementów aplikacji
Figure 4. Male respondents' opinion on what features the app should have
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds
Źródło: Opracowanie własne.
Source: Own elaboration.

Interpretacja takiego podejścia, ze względu na wielofunkcyjność aplikacji, pozostaje problematyczna. Podejście to może jednak wynikać z traktowania aplikacji wyłącznie jako informatora, nie zaś jako poradnika i narzędzia przydatnego wtedy, gdy zaistnieje konieczność samoochrony i samoobrony.

W przypadku pytania 5: „Kto powinien mieć dostęp do takiej aplikacji?", liczba i zakres odpowiedzi były zróżnicowane, co

Given the multi-functional character of the app, it is problematic to interpret these negative answers. One possible explanation for them would be that the app was viewed exclusively as a means of notification, rather than a guide and tool which could be useful for self-defence and self-protection.

In Question 5: "Who should have access to the app?", the answers and response rates varied, due to the multiple-response

wynika z zastosowania kafeterii z możliwością wielokrotnego wyboru. W pierwszej grupie wiekowej rozkład odpowiedzi był bardzo podobny. Według 12 respondentów dostęp do aplikacji powinna mieć administracja samorządowa, zdaniem 15 osób dostęp do niej powinny mieć służby, inspekcje i straże, a według 17 badanych dostęp ten powinni mieć cywile.

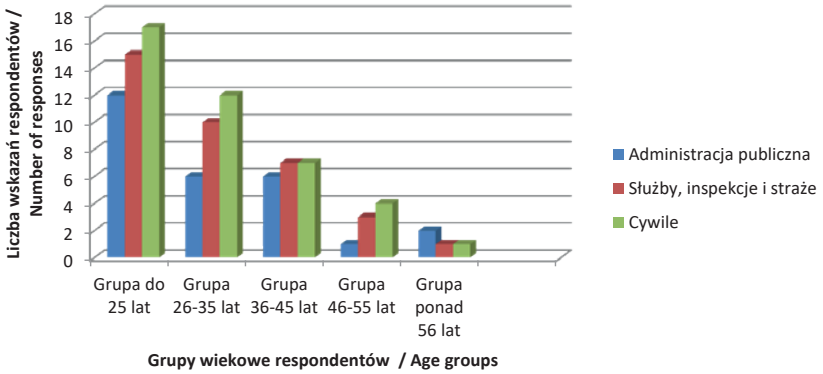
W grupie wiekowej 26–35 lat układ odpowiedzi jest, proporcjonalnie do liczby badanych, podobny. Na administrację publiczną wskazało 6 respondentów, na służby, inspekcje i straże – 10, a na cywilów – 12.

W przypadku grupy wiekowej 36–45 lat wyniki były nieco inne. Proporcjonalnie do próby badawczej na administrację publiczną wskazało 6 osób, a na służby, inspekcje i straże oraz na cywilów – po 7 osób.

format. The first age group had a very consistent distribution of answers. According to 12 respondents, the app should be available to government administration; 15 respondents said it should be available to services, inspections, brigades and guards while 17 respondents said the app should be available to civilians.

In the group of 26–35-year-olds, the answers were, proportionately to the number of the respondents, similar. Government administration was indicated by 6 respondents, services, inspections, brigades and guards were chosen by 10 respondents and civilians were mentioned by 12 respondents.

The results were slightly different for the group of 36–45-year-olds. Proportionately to the survey sample, government administration was indicated by 6 respondents, and services, inspections, brigades and guards and civilians were mentioned by 7 respondents, respectively.



Rycina 5. Opinia respondentów na temat tego, które podmioty powinny mieć dostęp do aplikacji
Figure 5. Male respondents' opinion on who should have access to the app
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds; Administracja publiczna – government administration;Służby, inspekcje i straże – services, inspections, brigades and guards
Źródło: Opracowanie własne.
Source: Own elaboration.

W grupie wiekowej 46–55 lat 1 respondent wskazał na administrację publiczną, 3 badanych wskazało na służby, inspekcje i straże, a 4 badanych – na cywilów.

Mężczyźni z najstarszej i jednocześnie najmniej licznej grupy wiekowej udzielili odpowiedzi podobnie jak mężczyźni z grupy wiekowej 36–45 lat. Na administrację publiczną wskazały 2 osoby, a zarówno na służby, inspekcje i straże, jak i na cywilów wskazała 1 osoba.

Na przykładzie pytania 6: „Na jakich urządzeniach aplikacja powinna być dostępna?", wyraźnie widać, że urządzenia mobilne są preferowane przez osoby młodsze, a komputery stacjonarne – przez osoby starsze. W trzech pierwszych grupach wiekowych udzielano odpowiednio odpowiedzi: 20:8, 14:6 oraz 9:6 na korzyść smartfonów. W dwóch najstarszych grupach odpowiedzi układały się odpowiednio 4:4 oraz 1:2 na korzyść komputerów stacjonarnych.

Można tu oczywiście zastanawiać się nad celowością opracowywania aplikacji na sprzęt stacjonarny, skoro aby mieć do niego dostęp, potrzebne jest stanowisko pracy, podczas gdy z urządzeniami mobilnymi kontakt jest w zasadzie permanentny. Jednak nawiązując do zasygnalizowanej wcześniej „barierą technologiczną", trzeba zauważyć, że osoby w starszym wieku mniej sprawnie korzystają ze smartfonów, preferując komputery stacjonarne, zwłaszcza w celu pozyskiwania różnego rodzaju informacji.

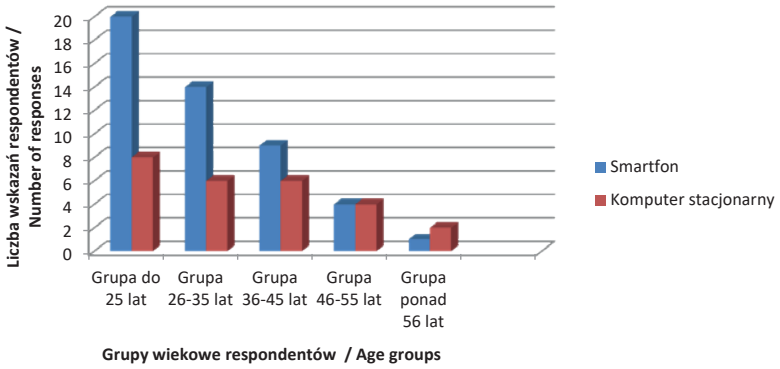
In the group of 46–55-year-olds, 1 respondent indicated government administration, 3 respondents mentioned services, inspections, brigades and guards and 4 respondents indicated civilians.

The answers of male respondents from the oldest and smallest age group were similar to the answers of the group of 36–45-year olds. Government administration was indicated by 2 respondents, and services, inspections, brigades and guards, and civilians were chosen by 1 respondent.

As shown by Question 6: "What kind of devices should the app be accessible on?", it was clear that mobile devices were preferred by younger respondents, while desktops were preferred by the older respondents. In the first three age groups, the answers were: 20:8, 14:6 and 9:6 in favour of smartphones. In the two oldest age groups, the responses to this question were 4:4 and 1:2, respectively, in favour of desktops.

It might be legitimately argued that there is no point in developing the app for desktops, since its use would be limited to the location where the desktop is installed, while mobile devices provide permanent access to the app. Hover, due the previously mentioned "technological barrier", older people are less apt at using smartphones, so they prefer desktops, especially as a means of obtaining various information.

ISSN 1895-8443



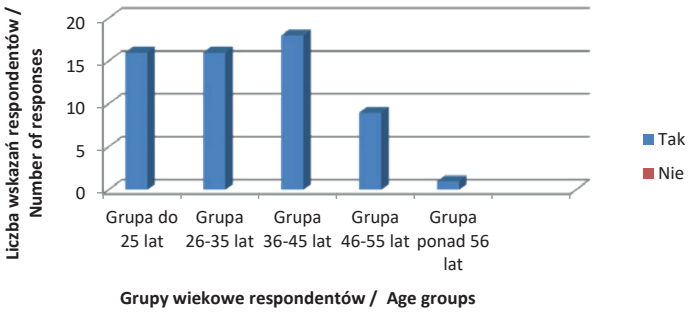
Rycina 6. Opinia respondentów na temat rodzajów urządzeń, na które aplikacja powinna być dostępna.
Figure 6. Male respondents' opinion on the types of devices the app should be accessible on.
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds; Smartfon – smartphone; Komputer stacjonarny – desktop
Źródło: Opracowanie własne.
Source: Own elaboration.

Ostatnie pytanie ankietowe: „Co by Państwa skłoniło do pobrania takiej aplikacji?", miało charakter otwarty, wymagało więc przeprowadzenia analizy zarówno ilościowej, jak jakościowej. Należy podkreślić, że odpowiedzi na to pytanie udzieliła stosunkowo niewielka grupa respondentów. Wśród pojawiających się komentarzy można zauważyć znaczny rozdźwięk tematyczny mogący wynikać z rozmaitych przesłanek, które skłoniłyby potencjalnych użytkowników do skorzystania z aplikacji. Są tutaj wskazania typu „darmowy dostęp" i „ciekawość", które sugerują brak należytego przygotowania merytorycznego do wykorzystania programu. Ale pojawiają się również odpowiedzi „informacja o zagrożeniach", „poczucie bezpieczeństwa swojego i bliskich", które wskazują na przeświadczenie o użyteczności potencjalnego produktu. Jednak znamienne wśród udzielonych odpowiedzi jest także, być może instynktowne i wynikające z dotychczasowych braków, wskazanie na wykorzystanie aplikacji jako „odbiornika" komunikatów, nie zaś jako narzędzia interaktywnego pozwalającego na aktywne informowanie o pojawiających się niebezpieczeństwach.

W grupie kobiet na pytanie 1: „Czy chcieliby Państwo być poinformowani o aktualnych zagrożeniach w okolicy?", wszystkie osoby odpowiedziały twierdząco. Żadna z osób nie wyraziła swojej dezaprobaty w tym zakresie.

The last question: "What would prompt you to download such an app?" had an open-ended format, thus requiring both qualitative and quantitative analysis. It should be stressed that the question was answered by a relatively small group of respondents. The comments made by the respondents span a broad range of subjects due to the diverse reasons which would prompt them to use the app. Answers like "free access" and "curiosity" suggest that the respondents were ill-prepared to use the software. But there were also answers such as "information on threats" or "a sense of safety of the family and close ones", which suggested a belief that the product could be useful. What was characteristic in the answers, however, was that the respondents viewed the app as being useful for receiving communications, rather than as an interactive tool designed to actively provide information on pending threats – this could be explained by the unavailability and, by extension, lack of experience with interactive tools.

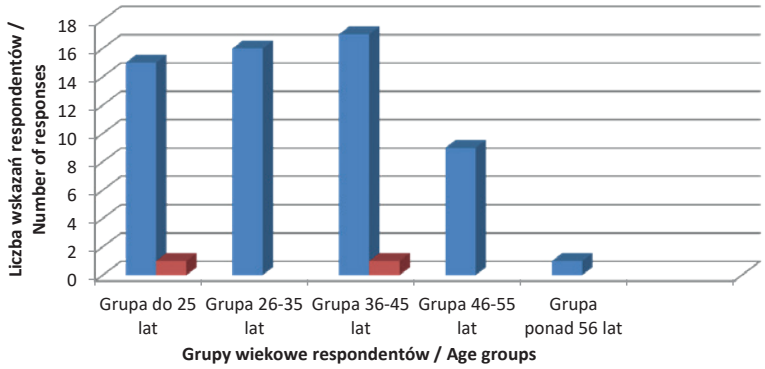
In the group of the female respondents, Question 1: "Would you like to be updated on current threats in your area?", all the respondents gave an affirmative answer.



Rycina 7. Opinia respondentów na temat chęci bycia informowanym o zagrożeniach
Figure 7. Female respondents' opinion on whether they wished to be notified of threats
Tak – Yes; Nie – No; Grupa do 25 lat.. – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds
Źródło: Opracowanie własne.
Source: Own elaboration.

W odpowiedziach na pytanie 2: „Czy aplikacja mająca poniższe cechy będzie dla Państwa interesująca?", można zaobserwować pewne rozbieżności. Mimo zasadniczej zgodności badanych i pozytywnego wyrażania się o aplikacji jedna kobieta z grupy wiekowej do 25 lat oraz jedna z grupy wiekowej 36–45 lat wyraziły się negatywnie na temat kształtu i możliwych opcji aplikacji.

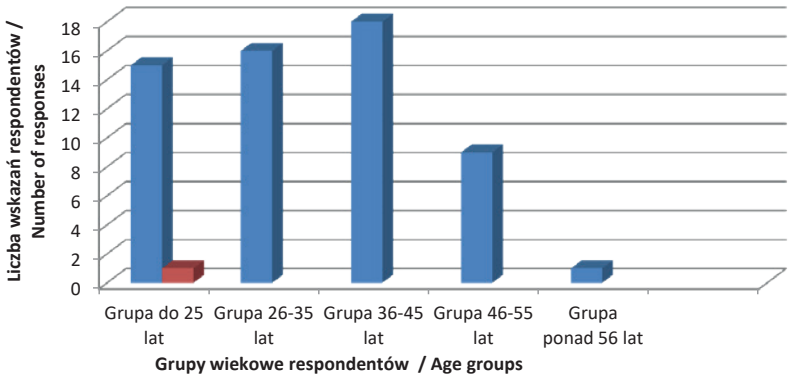
In Question 2: "Would an app with the following characteristics be of interest to you?" a certain discrepancy could be noticed. Although the female respondents were generally consistent in their positive answers regarding the app, one respondent from the group of up-to-25-year-olds and one respondent from the group of 36–45-year olds gave negative answers as to the design and possible options of the app.



Rycina 8. Opinia respondentów na temat zainteresowania aplikacją
Figure 8. Female respondents' opinion on whether the app was of interest to them
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds
Źródło: Opracowanie własne.
Source: Own elaboration.

W swoich odpowiedziach na pytanie 3: „Czy aplikacja powinna udostępniać informacje na temat najbardziej aktualnych zagrożeń?", kobiety były niemal w pełni zgodne – wyrażały aprobatę dla tego rozwiązania. Tylko jedna osoba z grupy najmłodszej odpowiedziała na pytanie przecząco.

In Question 3: "Should the app provide information on the latest threats?", almost all the female respondents answered "Yes". Only one respondent, from the youngest age group, answered "No" to this question.



Rycina 9. Opinia respondentów na temat udostępniania przez aplikację informacji o najbardziej aktualnych zagrożeniach
Figure 9. Female respondents' opinion on whether they wished to be notified of the latest threats
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds
Źródło: Opracowanie własne.
Source: Own elaboration.

W odniesieniu do planowanej struktury i przeznaczenia aplikacji odpowiedź ta wydaje się nielogiczna i może wynikać z niezrozumienia zagadnienia.

W przypadku pytania 4: „Czy w aplikacji powinny być zamieszczone komunikaty, instrukcje oraz scenariusze reagowania na poszczególne zagrożenia?", rozkład odpowiedzi pozostał zasadniczo podobny. Większość badanych odpowiedziała

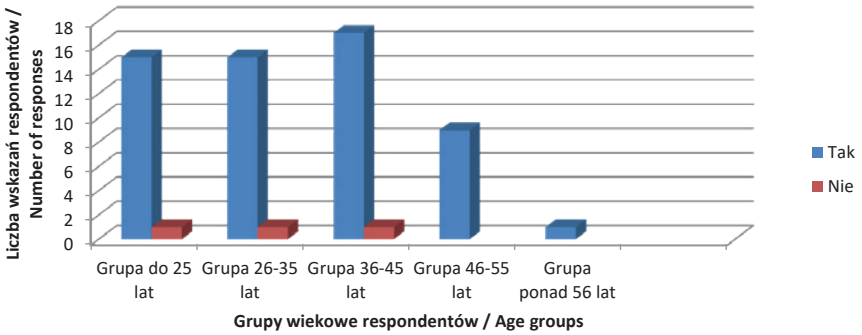
With regard to the planned design and purpose of the app, the negative answer seems to be illogical and might stem from a misunderstanding of the subject.

In Question 4: "Should the app provide communications, instructions and response scenarios for individual threats?", the majority of the female respondents answered "Yes". Only three respondents – from the first three age groups – said that

 ISSN 1895-8443

„Tak". Tylko trzy osoby: po jednej z trzech pierwszych grup wiekowych, stwierdziły, że publikowanie komunikatów, instrukcji i scenariuszy reagowania jest niecelowe. Wydaje się, że opinia ta wynika z braku pełnej wiedzy na temat działania tego typu oprogramowania.

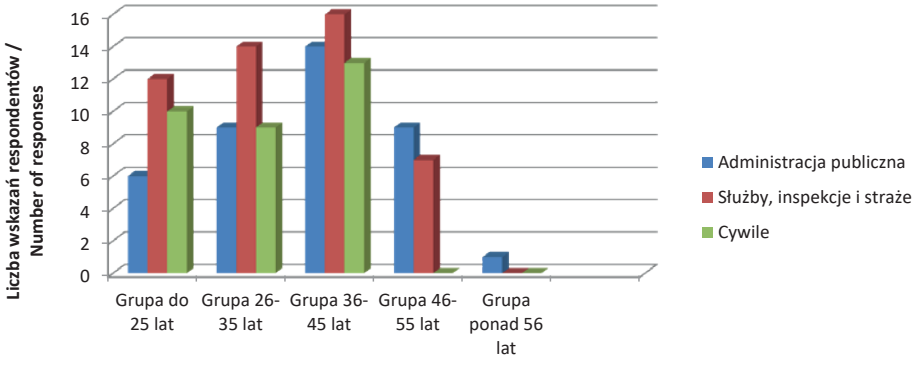
there was no point in issuing communications, instructions and response scenarios. It seems that this opinion resulted from insufficient knowledge of how this type of software works.



Rycina 10. Opinia respondentów na temat elementów aplikacji
Figure 10. Female respondents' opinion on what features the app should have
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds
Źródło: Opracowanie własne.
Source: Own elaboration.

Z kolei w odpowiedzi na pytanie 5: „Kto powinien mieć dostęp do takiej aplikacji?", większość kobiet wskazywała na służby, inspekcje i straże. Jeśli chodzi o pozostałe miejsca, rozkład odpowiedzi był bardzo różny. Na drugim miejscu na przemian pojawiała się administracja publiczna i ludność cywilna. W najmłodszej grupie wiekowej stosunek wskazań na ludność cywilną do wskazań na administrację publiczną wynosił 10:6. W grupie wiekowej 26–35 lat zaobserwowano równowagę w tym zakresie, a w grupie wiekowej powyżej 56 lat najczęściej wskazywanym podmiotem była administracja publiczna.

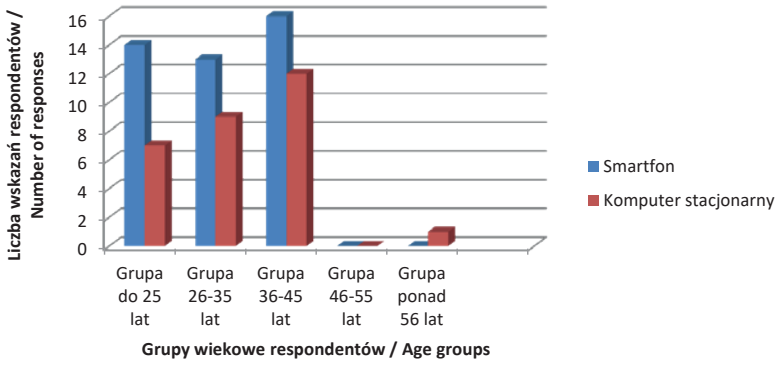
In Question 5: "Who should have access to the app?", most female respondents indicated services, inspections, brigades and guards. Other answers varied significantly. Second most-popular answers included, interchangeably, government administration and civilians. In the youngest age group, the relationship between answers involving civilians and answers involving government administration was 10:6. In the group of 26–35-year-olds, the answers on this subject were balanced, while in the group of over-56-year-olds, the most popular answer involved government administration.



Rycina 11. Opinia respondentów na temat tego, które podmioty powinny mieć dostęp do aplikacji
Figure 11. Female respondents' opinion on who should have access to the app
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds;
Administracja publiczna – government administration; Służby, inspekcje i straże – services, inspections, brigades and guards; Cywile – civilians
Źródło: Opracowanie własne.
Source: Own elaboration.

Odpowiedzi na pytanie 6: „Na jakich urządzeniach aplikacja powinna być dostępna?", pokazały, że wśród kobiet, podobnie jak wśród mężczyzn, urządzenia mobilne są wybierane przez osoby młodsze, a urządzenia stacjonarne – przez osoby starsze.

In Question 6: "What devices should the app be accessible on?", the answers showed that, as in the case of male respondents, mobile devices were preferred by younger respondents, while desktops were preferred by older respondents.



Rycina 12 Opinia respondentów na temat rodzajów urządzeń, na które aplikacja powinna być dostępna
Fig. 12 Female respondents' opinion on the types of devices the app should be accessible on.
Tak – Yes; Nie – No; Grupa do 25 lat – up-to-25-year olds, 26-35-year-olds, 36-45-year-olds, over-56-year olds; Smartfon – smartphone
Komputer stacjonarny – desktop
Źródło: Opracowanie własne.
Source: Own elaboration.

W pierwszych trzech grupach wiekowych wskazań na smartfony było więcej niż wskazań na urządzenia stacjonarne – odpowiednio: 14:7, 13:9 i 16:12. Interesujące jest to, że w grupie wiekowej 46–55 lat nikt nie udzielił odpowiedzi na pytanie. Z kolei najstarsi respondenci –zgodnie z zasygnalizowaną już tendencją – wskazali na urządzenia stacjonarne.

Pytanie 7: „Co by Państwa skłoniło do pobrania takiej aplikacji?", wymagało – ze względu na swój otwarty charakter – przeprowadzenia analizy jakościowej. Zaobserwowano wyraźną analogię między odpowiedziami kobiet a odpowiedziami mężczyzn. Pojawiło się bowiem bardzo mało wskazań różnych pod względem kategorii. Od odpowiedzi typu „ciekawość", „darmowy dostęp" możemy przejść do tych związanych z poczuciem bezpieczeństwa własnego i najbliższych, uzyskania rzetelnej i szybkiej informacji o zagrożeniach po „troskę o bezpieczeństwo".

In the first three age groups, answers involving smartphones were more frequent than answers involving desktops: 14:7, 13:9 and 16:12, respectively. What is interesting is that no respondents in the group of 46–55-year-olds gave an answer to this question. Older respondents, consistent with the mentioned tendency, indicated desktops.

Question 7: "What would prompt you to download such an app?", required a qualitative analysis due to the open-ended format of the question. A clear analogy was found between the answers of the female and male respondents. Namely, there were very little answers that differed in terms of category. These ranged from "curiosity" and "free access" to answers involving a sense of one's own and family's safety, and the need to obtain reliable and fast information on threats, to "concern for safety".

Dyskusja nad metodami i wynikami

Po przeanalizowaniu wyników przeprowadzonych badań można z 95-procentowym prawdopodobieństwem przyjąć, że dzięki metodzie, technice oraz narzędziu badawczemu, które zastosowano, uzyskano wyniki z założonym błędem w wysokości 0,09 umożliwiające falsyfikację postawionej hipotezy oraz wyciągnięcie wniosków mogących się przyczynić do opracowania interaktywnego narzędzia dającego społeczeństwu możliwość czynnego uczestniczenia w procesie monitorowania zagrożeń. Oczywiście przeprowadzona ankieta miała charakter badań wstępnych, których pozytywny rezultat umożliwi kontynuowanie programu badawczego przy użyciu innych technik, takich jak wywiad ekspercki, czy metod w postaci eksperymentu. Zastosowany algorytm analizy wyników według płci i wieku respondentów pozwolił uzyskać opinie na badany temat. Oczywiście można także prześledzić wyniki według – zawartych w metryczce narzędzia badawczego – wykształcenia i miejsca zamieszkania uczestników badania. Jednak ich wstępna analiza wykazała, że nie mają one większego wpływu na udzielone odpowiedzi. Obecnie bowiem dostęp do sprzętu elektronicznego oraz Internetu

Discussion of methods and results

Following an analysis of the surveys, it can be assumed with a 95-percent certainty that the methods, techniques and survey questionnaires which had been used yielded results with an assumed error of 0.09, allowing the falsification of the hypothesis and making it possible to draw conclusions that could contribute to the development of an interactive tool, in order to provide the public with an opportunity to become actively involved in the process of monitoring threats. Although the analysis conducted here only served as a preliminary study, its positive result will make it possible to continue the survey programme using other techniques, such as expert opinion surveys or experimental methods. The algorithm used for analysing the results by gender and age helped to obtain opinions on the studied subject. The results may also be plotted according to the educational attainment and place of residence of the respondents, which are included in the survey questionnaire demographic information section. However, a preliminary analysis showed that these factors had no significant influence on the answers given. It should be taken into account that electronic devices and the Internet

jest powszechny, a ich użytkowanie jest w znacznej mierze intuicyjne i nie wymaga specjalistycznych kwalifikacji.

Uzyskane wyniki wskazują natomiast niemal jednoznacznie na zainteresowanie respondentów projektowanym narzędziem oraz względne zrozumienie istoty jego działania. Oczywiście pojawiają się rozbieżności w zakresie jego ostatecznego kształtu i przeznaczenia. Pewien niepokój budzą odpowiedzi wskazujące na to, ze narzędzie będzie wykorzystywane przede wszystkim przez służby, inspekcje i straże, ale wydaje się, że te odpowiedzi wynikają z niewiedzy i nieświadomości badanych. Kampania społeczna oraz stosowne instrukcje będące elementem aplikacji powinny to zmienić.

Wnioski

Na podstawie uzyskanych wyników badań empirycznych można pozytywnie zweryfikować postawioną na początku artykułu hipotezę oraz wysnuć wniosek, że bezspornie potrzebne jest opracowanie interaktywnej aplikacji pozwalającej ludności cywilnej na czynny udział w procesie monitorowania zagrożeń. Jej projektowany kształt, jest w opinii badających właściwy. Aby oprogramowanie było w pełni funkcjonalne, powinno być interaktywne i umożliwiać przekazywanie oraz odbieranie informacji o zagrożeniach.

Jednakże w kontekście działania aplikacji niezbędne jest wprowadzenie zmian systemowych oraz zainicjowanie zmiany sposobu myślenia społeczeństwa. Jeśli chodzi o zmiany systemowe konieczne jest powołanie komórek (centrów dyspozycyjnych), które na szczeblach lokalnych, tj. w powiatach, będą weryfikować napływające informacje. Ogniwo powiatu wydaje się najwłaściwsze ze względu na optymalną liczbę pojawiających się zgłoszeń. W gminie może ich być zbyt mało, z kolei w województwie – zbyt wiele. Ponadto z perspektywy dyspozycji sił takie rozwiązanie powinno pozwolić na płynne funkcjonowanie centrum. Poza tym możliwości finansowe powiatu są większe niż możliwości finansowe gmin, w związku z czym powstanie tego typu podmiotów byłoby realne. Oczywiście powinny być one sprzężone z właściwym terenowo centrum powiadamiania ratunkowego (a nawet stanowić jego część) oraz centrum zarządzania kryzysowego. Pozwoliłoby to harmonijny obieg informacji o zagrożeniach.

Niezwykle ważnym elementem wdrażania aplikacji do powszechnego użytku jest ponadto merytoryczne oraz wolicjonalne i etyczne przygotowanie ludności cywilnej do korzystania z niej. Dlatego też wprowadzenie jej do użytku powinno być poprzedzone kampanią społeczną, na co wskazują niektóre odpowiedzi na pytania 3–5, a także wskazania w pytaniu 7. Aplikacja musi mieć jasno zredagowaną instrukcję i samouczek. Należy ponadto opracować analogiczne i w pełni kompatybilne jej wersje na urządzenia przenośne oraz stacjonarne.

Kolejną kwestią jest konieczność zaszczepienia w ludności cywilnej przekonania o potrzebie i celowości użycia aplikacji. Jeśli uda się zaangażować społeczności lokalne – bo na takim poziomie aplikacja ta będzie szczególnie przydatna – szybkość i dokładność wykrywania niebezpieczeństw się zwiększą. Korzystanie z aplikacji musi mieć jednak charakter odpowiedzialny. Zapewnić to powinien mechanizm lokalizacji

are widely available and highly intuitive, and their use does not require specialist knowledge.

The obtained survey results show a high degree of interest among respondents in the tool's being designed, and a relatively good understanding of how it should work. Still, there are some obvious discrepancies regarding its final form and function. The responses indicating that this tool will primarily be used by the services, inspections, brigades and guards might be a cause for concern, although it seems that these answers result from a lack of knowledge and awareness on the part of the respondents. A public awareness campaign and in-app instructions should be sufficient to change this perception.

Conclusions

The empirical study results confirm the hypothesis put forward at the beginning of this article and lead to the conclusion that there is a clear need to develop an interactive application to allow the public to become actively involved in the process of monitoring threats. The respondents positively assessed the current design of the application. To make it fully functional, it should be interactive and allow sending and receiving information about threats.

However, in the context of the application's functioning, it appears necessary to introduce system changes and raise public awareness. As for the system changes, it is necessary to establish units (dispatch centres) that would verify the information received at the local level, i.e. in districts (powiat). The district level seems to be the best solution in the context of processing an optimum number of notifications. A commune (gmina) might receive too few notifications, and an entire province (województwo) – too many. In addition, in terms of resource allocation, this should allow the smooth operation of the centres. In addition, the financial resources at the disposal of district units are greater than those available in the communes, which makes the establishment of such centres feasible. They should work closely with the relevant local emergency notification centres (or even become their part) and crisis management centres. This would facilitate the smooth flow of information about threats.

An extremely important element in the process of implementing the application for general use is to prepare the public in terms of the relevant knowledge, and volitional and ethical aspects needed to use it. Due to this, its introduction should be preceded by a public awareness campaign, which is suggested by some of the answers to questions 3–5 and 7. The application should have a clear manual and tutorial. Similar and fully compatible versions for mobile and desktop devices should also be developed.

It is also necessary to convince the public of the need and purposefulness of using the application. If we succeed in involving local communities, as it is at this level that the application will be particularly useful, the speed and precision of detecting threats will improve. However, the application must be used responsibly. This should be ensured by a solution designed to

zgłaszającego i jego identyfikacja. Powinien on wyeliminować wszelkie nieodpowiedzialne bądź złośliwe użycia tego narzędzia.

Jeśli powyższe wnioski zostaną wykorzystane w procesie wdrażania aplikacji do użytku, to można przypuszczać, że system zarządzania kryzysowego w Polsce zyska bardzo skuteczny i silnie zintegrowany ze strukturą społeczną kraju mechanizm, który pozwoli wykrywać zagrożenia oraz informować o nich i będzie uzupełnieniem obecnie istniejących rozwiązań.

gather information on the location and identity of the notifier. This should eliminate all cases of irresponsible and malicious use of this tool.

If the above conclusions are taken into consideration in the process of implementing the application, it can be assumed that the emergency management system in Poland will receive a highly effective mechanism that is tightly integrated with the country's social structure and facilitates the detection and notification of threats in addition to the existing solutions.

Wykaz skrótów

SMOK – System Monitoringu i Osłony Kraju
IMGW – Instytut Meteorologii i Gospodarki Wodnej
ISOK – Informatyczny System Osłony Kraju
GUGiK – Główny Urząd Geodezji i Kartografii
KSWSiA – Krajowy System Wykrywania Skażeń i Alarmowania

List of abbreviations

SMOK – the National Monitoring and Protection System
IMGW – the Institute of Meteorology and Water Management
ISOK – the Computerised National Protection System
GUGiK – the Central Office for Cartography and Geodesy
KSWSiA – the National Contamination Detection and Alarm System

Literatura

[1] Sobczyk M., *Statystyka*, Wydawnictwo Naukowe PWN, Warszawa 2018.
[2] Rozporządzenie Rady Ministrów z dnia 16 października 2006 r. w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach (Dz. U. Nr 191, poz. 1415).
[3] Rozporządzenia Rady Ministrów z dnia 7 stycznia 2013 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach (Dz. U. poz. 96), § 4, pkt 1.
[4] *Ocena przygotowań w zakresie ochrony ludności i obrony cywilnej w Polsce za 2015 r.*, Biuro ds. Ochrony Ludności i Obrony Cywilnej Komendy Głównej Państwowej Straży Pożarnej, Warszawa 2016, 8.
[5] http://www.zabieram.pl.mediafm.net/art/40701/regionalny-system-ostrzegania-w-caej-polsce.html [dostęp: 1.02.2018].
[6] http://www.lublin.uw.gov.pl/regionalny-system-ostrzegania [dostęp: 31.01.2018].
[7] http://www.dailymail.co.uk/sciencetech/article-3023155/The-app-save-LIFE-Emergency-service-tells-rescuers-save-touch-button.html [dostęp: 7.02.2017].
[8] https://play.google.com/store/apps/details?id=com.curlybrace-apps.ruchir.rescuer [dostęp: 7.02.2017].
[9] https://play.google.com/store/apps/details?id=com.threesixtyen-tertainment.nesn [dostęp: 7.02.2017].

DR HAB. HENRYK WYRĘBEK, PROF. UPH – doktor hab. nauk społecznych (dyscyplina: nauki o obronności). Profesor nadzwyczajny w Instytucie Nauk Społecznych i Bezpieczeństwa Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, kierownik Zakładu Bezpieczeństwa Państwa. W swoich zainteresowaniach naukowo-badawczych skupia się na problemach interdyscyplinarnych: naukach o zarządzaniu oraz naukach o bezpieczeństwie i obronności. Autor ponad 100 publikacji naukowych.

DR PAWEŁ SZMITKOWSKI – adiunkt w Zakładzie Bezpieczeństwa Państwa Instytutu Nauk Społecznych Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Od 2014 roku kierownik Pracowni Zarządzania Kryzysowego. Autor i redaktor monografii, artykułów naukowych i popularno-naukowych z zakresu zarządzania kryzysowego, ochrony ludności i obrony cywilnej oraz edukacji dla bezpieczeństwa.

HENRYK WYRĘBEK, PROF. UPH, doctor in social sciences (discipline: defence science). Associate Professor at the Social Science and Security Institute of the Faculty of Humanities of the Siedlce University of Natural Sciences and Humanities, Head of the Department of State Security. His scientific research interests include interdisciplinary problems of management sciences, and security and defence sciences. He has authored over 100 scientific publications.

PAWEŁ SZMITKOWSKI, PH.D. – assistant professor at the Department of State Security of the Social Science and Security Institute of the Siedlce University of National Sciences and Humanities. Since 2014 he has been Head of the Crisis Management Unit at the Department. He has published and edited a number of monographs, scientific and popular science articles in crisis management, population protection and civil defence, as well as safety education.

Ministerstwo Nauki i Szkolnictwa Wyższego

Stworzenie anglojęzycznych wersji oryginalnych artykułów naukowych wydawanych w kwartalniku „BITP. Bezpieczeństwo i Technika Pożarnicza" – zadanie finansowane w ramach umowy 658/P- DUN/2018 ze środków Ministra Nauki i Szkolnictwa Wyższego przeznaczonych na działalność upowszechniającą naukę.