Berta JURCZUK[1]

CYBERZAGROŻENIA WE WSPÓŁCZESNYM ŚRODOWISKU WOJSKOWYM

Rozwój technologii informacyjno-komunikacyjnych w istotny sposób wpłynął na funkcjonowanie współczesnych państw oraz struktur odpowiedzialnych za zapewnienie bezpieczeństwa. Cyberprzestrzeń stała się obszarem intensywnej aktywności administracyjnej, gospodarczej oraz militarnej, co spowodowało konieczność uwzględnienia jej w systemie bezpieczeństwa narodowego[2]. Wraz z postępującą cyfryzacją procesów zarządzania oraz dowodzenia wzrosła również podatność na różnego rodzaju zagrożenia o charakterze cybernetycznym.

Zjawiska te sprawiają, że cyberbezpieczeństwo należy obecnie postrzegać jako jeden z kluczowych elementów współczesnego środowiska bezpieczeństwa[3]. Analiza zagrożeń oraz mechanizmów ochrony informacji stanowi istotny punkt wyjścia do dalszych rozważań dotyczących roli czynnika ludzkiego w systemie bezpieczeństwa.

W niniejszym artykule przedstawiono pojęcie cyberprzestrzeni, charakterystykę cyberzagrożeń oraz znaczenie cyberbezpieczeństwa w kontekście funkcjonowania państwa i struktur obronnych.

POJĘCIE I ZNACZENIE CYBERPRZESTRZENI W SYSTEMIE BEZPIECZEŃSTWA PAŃSTWA

Rozwój technologii informacyjno-komunikacyjnych w ostatnich dekadach doprowadził do powstania nowej przestrzeni funkcjonowania państwa, społeczeństwa oraz sił zbrojnych – cyberprzestrzeni. Stała się ona środowiskiem, w którym realizowane są procesy komunikacyjne, wymiana informacji, zarządzanie danymi oraz działania o charakterze administracyjnym, gospodarczym i militarnym.

W literaturze przedmiotu cyberprzestrzeń definiowana jest jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne oraz powiązania między nimi. Obejmuje ona zarówno infrastrukturę techniczną, jak i użytkowników korzystających z sieci oraz urządzeń cyfrowych[4].

---

[1] ORCID: 0009-0009-8333-8368.

[2] M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.

[3] J. Andress, *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*, Helion, Gliwice 2022.

[4] P. W. Singer, A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, New York 2014.

W ujęciu doktrynalnym cyberprzestrzeń postrzegana jest jako środowisko wielowarstwowe, obejmujące warstwę fizyczną, logiczną oraz tożsamości cyfrowej. Warstwa fizyczna odnosi się do infrastruktury technicznej, takiej jak urządzenia, sieci i systemy transmisyjne. Warstwa logiczna obejmuje dane, oprogramowanie oraz procesy przetwarzania informacji, natomiast warstwa tożsamości cyfrowej obejmuje funkcjonowanie podmiotów w cyberprzestrzeni poprzez ich wirtualne reprezentacje, takie jak loginy, adresy e-mail, profile czy inne identyfikatory cyfrowe. Warstwa tożsamości cyfrowej ma charakter abstrakcyjny i nie musi być bezpośrednio powiązana z rzeczywistą tożsamością osoby lub organizacji. W konsekwencji jeden podmiot może posiadać wiele tożsamości cyfrowych, a jedna tożsamość może być współdzielona przez różne podmioty[5].

Istotną konsekwencją przedstawionego modelu jest fakt, że w przeciwieństwie do warstwy fizycznej, której elementy posiadają określone położenie geograficzne, warstwa logiczna oraz warstwa tożsamości cyfrowej mają charakter transgraniczny. Oznacza to brak jednoznacznego przypisania do określonego terytorium państwowego, co istotnie wpływa na trudności w zakresie regulacji prawnych oraz zapewnienia bezpieczeństwa. Jednocześnie warstwy te pozostają ze sobą w ścisłej zależności – warstwa logiczna nie może funkcjonować bez warstwy fizycznej, natomiast warstwa tożsamości cyfrowej opiera się na zasobach warstwy logicznej[6].

Model warstwowy cyberprzestrzeni pozwala na lepsze zrozumienie jej złożonej struktury oraz identyfikację potencjalnych obszarów podatności na zagrożenia. Każda z warstw może stanowić odrębny cel oddziaływania, przy czym skutki działań podejmowanych w jednej z nich mogą wpływać na pozostałe. W szczególności naruszenia warstwy tożsamości cyfrowej może skutkować uzyskaniem nieuprawnionego dostępu do zasobów warstwy logicznej, a w konsekwencji oddziaływaniem na elementy warstwy fizycznej.

Takie ujęcie wskazuje, że cyberprzestrzeń nie ogranicza się wyłącznie do aspektów technologicznych, lecz stanowi złożone środowisko funkcjonowania, w którym istotną rolę odgrywa zarówno infrastruktura, jak i czynnik ludzki oraz procesy informacyjne.

Wraz ze wzrostem uzależnienia instytucji publicznych i struktur wojskowych od systemów teleinformatycznych, cyberprzestrzeń zaczęła odgrywać istotną rolę w systemie bezpieczeństwa państwa. Zakłócenie jej funkcjonowania może prowadzić do ograniczenia zdolności operacyjnych, utraty poufności informacji oraz destabilizacji procesów

[5] *Operacje w cyberprzestrzeni DD-3.20*, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2020.
[6] Tamże.

decyzyjnych[7]. Z tego względu zagadnienia związane z ochroną cyberprzestrzeni stały się jednym z istotnych elementów współczesnej polityki bezpieczeństwa.

W dokumentach strategicznych wielu państw oraz organizacji międzynarodowych podkreśla się, że cyberprzestrzeń stanowi obecnie jeden z kluczowych obszarów oddziaływania zarówno w czasie pokoju, jak i w sytuacjach kryzysowych czy konfliktach zbrojnych[8]. Wskazuje się, że zagrożenia pojawiające się w tej domenie mogą mieć charakter transgraniczny, a ich skutki mogą oddziaływać równocześnie na strefę militarną, gospodarczą czy społeczną. Z tego względu ochrona cyberprzestrzeni została włączona do katalogu priorytetowych zadań państwa w zakresie zapewnienia bezpieczeństwa narodowego.

W polskich dokumentach strategicznych dotyczących bezpieczeństwa podkreśla się konieczność budowy i utrzymywania zdolności do zapobiegania, wykrywania oraz reagowania na incydenty w cyberprzestrzeni[9]. Zwraca się uwagę nie tylko na ochronę infrastruktury krytycznej i systemów administracji publicznej, ale również na zapewnienie ciągłości funkcjonowania struktur odpowiedzialnych za obronność. Oznacza to, że cyberbezpieczeństwo nie jest już traktowane jako zagadnienie wyłącznie techniczne, lecz jako element szerszej polityki bezpieczeństwa państwa.

Istotnym krokiem w postrzeganiu cyberprzestrzeni jako obszaru o znaczeniu strategicznym było uznanie jej za domenę operacyjną. W praktyce oznacza to, że cyberprzestrzeń jest traktowana na równi z takimi domenami jak ląd, morze, powietrze czy przestrzeń kosmiczna[10]. Działania prowadzone w tym środowisku mogą wspierać operacje wojskowe, ale także mogą stanowić narzędzie oddziaływania przeciwnika, ukierunkowane na osłabienie zdolności obronnych państwa bez konieczności użycia klasycznych środków militarnych.

Wraz z rozwojem technologii oraz rosnącą cyfryzacją procesów dowodzenia i zarządzania, znaczenie cyberprzestrzeni w funkcjonowaniu sił zbrojnych systematycznie wzrasta. Systemy teleinformatyczne wspierają planowanie operacyjne, łączność, logistykę oraz obieg informacji. W konsekwencji ich zakłócenie może wpływać na sprawność podejmowania

---

[7] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024*, Warszawa 2019.
M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.
[8] NATO, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20)*, Brussels 2020.
European Commission, *The EU Cybersecurity Strategy for the Digital Decade*, Brussels 2020.
The White House, *National Cyber Strategy of the United States of America*, Washington, D.C. 2018.
[9] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, Warszawa 2019.
Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.
[10] M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.

decyzji oraz skuteczność realizowanych zadań. Z tego powodu zapewnienie odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni stanowi obecnie jeden z warunków utrzymania zdolności obronnych państwa.

W kontekście funkcjonowania sił zbrojnych szczególnego znaczenia nabiera zapewnienie ciągłości wymiany informacji. System dowodzenia wymaga nieprzerwanego przepływu danych na potrzeby kierowania podległymi siłami i środkami, realizowanego w ramach sieci łączności gwarantującej dostępność, integralność oraz poufność przesyłanych informacji[11]. Zakłócenie tego procesu może prowadzić do ograniczenia zdolności dowodzenia oraz obniżenia efektywności realizowanych zadań.

W literaturze podkreśla się, że cyberbezpieczeństwo należy postrzegać nie tylko jako zbiór narzędzi technicznych, lecz jako proces obejmujący działania organizacyjne, prawne oraz edukacyjne. Zwraca się uwagę, że skuteczna ochrona systemów teleinformatycznych wymaga podejścia systemowego, uwzględniającego zarówno infrastrukturę, jak i użytkowników oraz obowiązujące regulacje[12].

Cyberbezpieczeństwo stanowi zatem element szerszego systemu zarządzania bezpieczeństwem państwa, w którym istotne znaczenie ma identyfikacja zagrożeń, ocena ryzyka oraz wdrażanie adekwatnych środków ochrony. Takie ujęcie wskazuje, że zapewnienie bezpieczeństwa w cyberprzestrzeni nie ogranicza się wyłącznie do aspektów technologicznych, lecz obejmuje również kształtowanie odpowiednich postaw i świadomości wśród osób korzystających z systemów informatycznych[13].

Wraz ze wzrostem znaczenia cyberprzestrzeni zwiększa się także skala oraz złożoność zagrożeń, które oddziałują zarówno na infrastrukturę techniczną jak i na użytkowników systemów teleinformatycznych.

RODZAJE I CHARAKTERYSTYKA CYBERZAGROŻEŃ

Współczesne cyberzagrożenia charakteryzują się dużą dynamiką oraz rosnącym stopniem złożoności. Rozwój technologii cyfrowych, powszechność urządzeń mobilnych oraz integracja systemów teleinformatycznych z procesami zarządzania i dowodzenia powodują, że potencjalne wektory ataku ulegają stałemu rozszerzaniu[14]. W literaturze przedmiotu

[11] M. Marczyk, B. Terebiński, *System łączności brygady obrony terytorialnej (BOT) w wojskowym systemie telekomunikacyjnym. Ujęcie teoretyczne*, „Kwartalnik Bellona", Military Publishing Institute, Warszawa 2021.
[12] M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.
[13] Tamże.
[14] Tamże.

wskazuje się, że zagrożenia w cyberprzestrzeni mogą mieć charakter zarówno techniczny, jak i społeczny, a ich skuteczność często wynika z połączenia obu tych elementów.

Do podstawowych rodzajów cyberzagrożeń zalicza się m.in. złośliwe oprogramowanie (malware), ataki typu phishing, ransomware, ataki typu Distributed Denial of Service (DDoS) oraz działania z zakresu inżynierii społecznej[15]. W przypadku środowiska wojskowego szczególne znaczenie mają zagrożenia ukierunkowane na zakłócenie łączności, pozyskanie informacji o charakterze operacyjnym oraz destabilizację procesu dowodzenia[16]. Jak podkreśla się w opracowaniach dotyczących bezpieczeństwa informacji, skuteczność ataku bardzo często nie wynika wyłącznie z zaawansowania technologicznego, lecz z wykorzystania podatności organizacyjnych i błędów użytkowników.

Powyższe wnioski znajdują potwierdzenie w aktualnych raportach dotyczących cyberbezpieczeństwa, w których podkreśla się, że jednym z dominujących trendów jest wzrost liczby ataków wykorzystujących techniki socjotechniczne oraz złośliwe oprogramowanie, w szczególności ransomware. Zwraca się również uwagę na rosnącą skalę incydentów wymierzonych w infrastrukturę krytyczną oraz systemy administracji publicznej, a także na coraz większe znaczenie operacji informacyjnych prowadzonych z wykorzystaniem cyberprzestrzeni. Analizy wskazują, że skuteczność wielu ataków wynika nie tyle z zaawansowania technologicznego, ile z wykorzystania podatności organizacyjnych oraz błędów użytkowników, co czyni czynnik ludzki jednym z kluczowych elementów systemu bezpieczeństwa[17].

W ostatnich latach zauważalny jest wzrost zagrożeń związanych z wykorzystaniem mediów społecznościowych oraz analizą dużych zbiorów danych (big data)[18]. Synergia tych obszarów umożliwia prowadzenie działań dezinformacyjnych, profilowanie użytkowników oraz budowanie przekazów oddziałujących na określone grupy odbiorców. Zjawisko to stało się szczególnie widoczne w kontekście konfliktu zbrojnego na Ukrainie, gdzie działania informacyjne i cybernetyczne stanowiły istotny element szerszej strategii oddziaływania[19]. Oprócz klasycznych ataków na infrastrukturę teleinformatyczną obserwowano intensywne

---

[15] M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.
[16] B. Terebiński, *Teleinformatyka wojskowa,* Akademia Sztuki Wojennej, Warszawa 2021.
[17] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023.
NASK – Państwowy Instytut Badawczy, Raport z działalności CERT Polska 2023, Warszawa 2024.
[18] J. Waszewski, *„Nie ukryjesz się". Konsekwencje synergii big data, mediów społecznościowych i neuronauki*, Akademia Sztuki Wojennej, Warszawa 2021.
[19] *Disinformation in the Russian invasion of Ukraine*,
https://en.wikipedia.org/wiki/Disinformation_in_the_Russian_invasion_of_Ukraine.

kampanie dezinformacyjne, próby destabilizacji systemów komunikacyjnych oraz działania mające na celu wywołanie paniki wśród ludności cywilnej i żołnierzy.

Istotnym trendem jest również rosnąca liczba zagrożeń skierowanych przeciwko urządzeniom mobilnym[20]. Smartfony i tablety, wykorzystywane zarówno w życiu prywatnym, jak i służbowym, stanowią potencjalne źródło wycieku informacji. Aplikacje o niezweryfikowanym pochodzeniu, niezabezpieczone sieci Wi-Fi czy brak aktualizacji systemu operacyjnego zwiększają podatność użytkownika na ataki. W środowisku wojskowym problem ten nabiera szczególnego znaczenia, zwłaszcza w sytuacji korzystania z alternatywnych środków łączności poza infrastrukturą resortową.

Do nowszych form zagrożeń zalicza się również wykorzystanie sztucznej inteligencji do generowania treści dezinformacyjnych (deepfake), automatyzację ataków phishingowych oraz stosowanie narzędzi umożliwiających masowe skanowanie podatności systemów. Takie działania pozwalają na prowadzenie operacji o charakterze hybrydowym, łączących oddziaływanie informacyjne, psychologiczne i cybernetyczne.

Na gruncie krajowym podkreśla się konieczność stałego monitorowania zagrożeń oraz podnoszenia poziomu świadomości użytkowników systemów teleinformatycznych. Doświadczenia ostatnich lat wskazują, że zagrożenia cybernetyczne nie ograniczają się do infrastruktury krytycznej, lecz mogą dotyczyć również pojedynczych użytkowników, których zachowania w cyberprzestrzeni mają wpływ na bezpieczeństwo całej organizacji[21]. W świetle struktur wojskowych szczególne znaczenie ma zatem właściwe przygotowanie personelu do rozpoznawania zagrożeń oraz przestrzegania zasad bezpieczeństwa informacji.

W kontekście terytorialnej służby wojskowej (tsw) specyfika pełnionej służby powoduje, że zagadnienie cyberzagrożeń nabiera dodatkowego znaczenia. Żołnierze Obrony Terytorialnej (OT) funkcjonują na styku środowiska cywilnego i wojskowego, łącząc aktywność zawodową z obowiązkami służbowymi. Taki model pełnienia służby sprzyja częstemu korzystaniu z powszechnie dostępnych narzędzi komunikacyjnych oraz urządzeń mobilnych, co może zwiększać ekspozycję na zagrożenia w cyberprzestrzeni.

W warunkach rozproszonej struktury organizacyjnej oraz rotacyjnego charakteru szkoleń istotne znaczenie ma poziom indywidualnej świadomości zagrożeń. Nawet pojedyncze nieostrożne działanie użytkownika, takie jak otwarcie podejrzanej wiadomości czy udostępnienie informacji w mediach społecznościowych, może prowadzić do naruszenia zasad bezpieczeństwa informacji. W tym kontekście cyberzagrożenia nie dotyczą wyłącznie

[20] P. Verma, A. Dixit, *Bezpieczeństwo urządzeń mobilnych. Receptury,* Helion, Gliwice 2017.
[21] J. Andress, *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*, Helion, Gliwice 2022.

infrastruktury technicznej, lecz również zachowań i nawyków użytkowników systemów teleinformatycznych.

Doświadczenia związane z konfliktem na Ukrainie pokazują, że działania informacyjne oraz cybernetyczne mogą być ukierunkowane także na żołnierzy oraz ich otoczenie. Analiza treści publikowanych w przestrzeni internetowej, próby profilowania czy kampanie dezinformacyjne mogą stanowić element szerszych operacji oddziaływania. Z tego względu podnoszenie poziomu świadomości cyberzagrożeń wśród żołnierzy OT stanowi istotny element budowania odporności informacyjnej.

Przedstawione rodzaje cyberzagrożeń wskazują, że współczesne środowisko bezpieczeństwa charakteryzuje się wysokim poziomem niepewności oraz podatności na oddziaływanie zewnętrze. Skala i różnorodność zagrożeń powodują, że niezbędne staje się wdrażanie kompleksowych rozwiązań z zakresu cyberbezpieczeństwo, obejmujących zarówno środki techniczne, jak i działania organizacyjne oraz edukacyjne. Oznacza to konieczność przyjęcia systemowego podejścia do ochrony informacji, w którym istotną rolę odgrywa użytkownik.

CYBERBEZPIECZEŃSTWO JAKO ELEMENT ŚRODOWISKA BEZPIECZEŃSTWA – ROLA CZYNNIKA LUDZKIEGO

Skala i złożoność współczesnych cyberzagrożeń powodują, że cyberbezpieczeństwo należy postrzegać jako integralny element systemu bezpieczeństwa państwa. Nie ogranicza się ono wyłącznie do wdrażania rozwiązań technicznych, lecz obejmuje działania organizacyjne, prawne oraz edukacyjne, których celem jest minimalizowanie ryzyka naruszeń poufności, integralności i dostępności informacji[22]. Ochrona informacji wymaga zatem podejścia systemowego, uwzględniającego zarówno infrastrukturę techniczną, jak i użytkowników systemów teleinformatycznych.

W literaturze przedmiotu podkreśla się, że jednym z kluczowych czynników wpływających na poziom bezpieczeństwa jest człowiek[23]. Nawet najbardziej zaawansowane zabezpieczenia techniczne nie eliminują ryzyka wynikającego z błędów użytkownika, braku świadomości zagrożeń czy nieostrożnych zachowań w cyberprzestrzeni. W środowisku wojskowym, w którym obieg informacji stanowi podstawę systemu dowodzenia oraz realizacji zadań, znaczenie odpowiedzialnych postaw użytkowników nabiera szczególnego wymiaru[24].

---

[22] M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.
[23] Tamże.
[24] B. Terebiński, *Teleinformatyka wojskowa*, Akademia Sztuki Wojennej, Warszawa 2021.

Współcześnie komunikacja interpersonalna w znacznym stopniu przeniosła się do przestrzeni cyfrowej. Powszechność komunikatorów internetowych, mediów społecznościowych oraz aplikacji mobilnych powoduje, że użytkownicy tworzą grupy wymiany informacji. W warunkach wojskowych może to generować określone ryzyka, związane między innymi z nieświadomym udostępnieniem informacji niejawnych osobom nieuprawnionym, błędną identyfikacją odbiorcy czy niedostateczną weryfikacją źródła komunikatu.

Szczególnego znaczenia nabiera także proces dezinformacji. Przekazy o charakterze sensacyjnym, odwołujące się do emocji odbiorców, mogą być wykorzystywane do destabilizacji środowiska informacyjnego oraz podważania zaufania do instytucji publicznych. W ramach jednej z kampanii Zespołu Działań Cyberprzestrzennych (ZDC) WOT skierowanych do żołnierzy i społeczeństwa zwrócono uwagę, że: „fake news nie musi być wiarygodny. Wystarczy, że jest sensacyjny”[25]. Mechanizm ten opiera się na szybkim rozpowszechnianiu treści wywołujących silne reakcje emocjonalne, co utrudnia ich racjonalną ocenę oraz weryfikację źródła.

Specyfika tsw, polegająca na łączeniu cywilnej aktywności zawodowej i prywatnej ze służbą wojskową, sprawia, że żołnierze funkcjonują równocześnie w dwóch środowiskach informacyjnych – cywilnym i wojskowym. Różnorodność wieku, doświadczenia zawodowego, wykształcenia oraz poziomu kompetencji cyfrowych może wpływać na zróżnicowany poziom świadomości zagrożeń. Część użytkowników może wykazywać mniejszą czujność wobec prób socjotechnicznych, manipulacji informacyjnej czy nieautoryzowanego dostępu do grup komunikacyjnych.

W tym kontekście cyberbezpieczeństwo należy postrzegać nie tylko jako zbiór procedur i zabezpieczeń technicznych, lecz jako element kultury organizacyjnej. Budowanie odporności informacyjnej wymaga systematycznych szkoleń, kształtowania właściwych nawyków oraz promowania odpowiedzialnych postaw w zakresie korzystania narzędzi komunikacyjnych. Poziom podnoszenia kompetencji w zakresie cyberbezpieczeństwa staje się zatem jednym z podstawowych warunków skutecznej ochrony informacji w strukturach wojskowych.

W obliczu przedstawionych zagrożeń oraz znaczenia czynnika ludzkiego dla poziomu bezpieczeństwa informacji zasadne staje się odniesienie powyższych rozważań do konkretnego środowiska organizacyjnego. Warto uwypuklić, że analiza sposobów komunikacji oraz

[25] WOT, post opublikowany w serwisie Facebook dnia 19.02.2026 r. https://facebook.com/story.php?story_fbid=1240346458268522&id=100068795396576.

wykorzystywanych narzędzi w strukturach wojskowych nabiera kluczowego znaczenia, ponieważ obieg informacji stanowi podstawę realizacji zadań.

Współczesna służba wojskowa obejmuje nie tylko działania kinetyczne, lecz również odpowiedzialność za ochronę bezpieczeństwa informacji oraz właściwe funkcjonowanie w cyberprzestrzeni, dlatego szczególnego znaczenia nabiera budowanie świadomości użytkowników w tym zakresie.