Journal of KONBiN 2020
Volume 50, Issue 4
DOI 10.2478/jok-2020-0090

Sławomir DYGNATOWSKI[1], Włodzimierz DYGNATOWSKI
[1]*Military University of Aviation (Lotnicza Akademia Wojskowa)*

PRAWNE PODSTAWY CYBERBEZPIECZEŃSTWA NA TLE POLSKIEGO I EUROPEJSKIEGO USTAWODAWSTWA

Legal basis of cybersecurity on the background of polish and UE legislation

Streszczenie: *Ostatnie dekady przyniosły bardzo szybki rozwój technik informatycznych, co znalazło swoje odzwierciedlenie we wszystkich dziedzinach życia społecznego oraz gospodarczego. Niestety postępująca cyfryzacja i obecność w sieci osób indywidualnych, podmiotów prywatnych, jak również państw sprawia, że są oni wystawieni na nowe niespotykane do niedawna rodzaje zagrożeń. Sprawcą tych zagrożeń mogą być pojedyncze osoby, zorganizowane grupy przestępcze lub wywiady obcych państw. Zagrożenia i wektory ataków przyjmują różne postacie, a ich ewolucja trwa cały czas wraz z postępującym rozwojem szeroko rozumianej cyberprzestrzeni. Aby móc skutecznie walczyć z coraz liczniejszymi zagrożeniami w cyberprzestrzeni, potrzebne są nie tylko środki techniczne, organizacyjne, lecz również formalno-prawne ramy reagowania na cyberataki. W niniejszym artykule autorzy przedstawiają prawne porównanie podstaw cyberbezpieczeństwa na tle polskiego i europejskiego ustawodawstwa.*
Słowa kluczowe: cyberataki, cyberbezpieczeństwo, prawne podstawy reagowania na cyberataki

Summary: *The last decades have brought about the rapid development of information technology, which was reflected in all areas of social life and economic. Unfortunately, the ongoing digitization and the presence of individuals, private entities as well as countries in the network makes them exposed to new types of threats that have never been seen before. The perpetrators of these threats may be individuals, organized criminal groups or foreign country interviews. Threats and vectors of attacks has many forms, and their evolution continues all along with the progressive development of broadly understood cyberspace. In order to be able to effectively fight with the increasing threats in cyberspace, not only technical and organizational measures are needed, but also the formal and legal framework to combat cyber-attacks. In this article, the authors discuss the legal comparison of the basics of cyber security against the Polish background and EU legislation.*
Keywords: cyber-attacks, cyber-security, legal grounds for responding to cyber-attacks

1. Wstęp

Ostatnie dekady przyniosły bardzo szybki rozwój technik informatycznych, co znalazło swoje odzwierciedlenie we wszystkich dziedzinach życia społecznego oraz gospodarczego. Jest to związane nie tylko z rozwojem internetu oraz jego coraz większą dostępnością, lecz przede wszystkim z rozwojem chmur obliczeniowych, m.in. modeli usług typu SaaS oraz rozwiązań pozwalających na przechowywanie danych w chmurze. Internet jest bowiem platformą, na bazie której rozwijają się coraz to nowe usługi oparte na rozwiązaniach chmurowych.

Rozwój internetu przyczynił się do powstania społeczeństwa informacyjnego, które funkcjonuje w świecie realnym, lecz również spędza wiele czasu w cyberprzestrzeni. Towarzyszy temu zjawisko przenoszenia ze świata realnego usług, czynności i innych szeroko pojętych aktywności do cyberprzestrzeni [1].

Obecnie obserwuje się ewolucję internetu w tzw. internet rzeczy, czyli sieć połączonych ze sobą urządzeń typu smart wymieniających między sobą dane. Szybko rozwijają się również dziedziny związane z wykorzystaniem sztucznej inteligencji, uczeniem maszynowym czy rozszerzoną rzeczywistością.

Niestety postępująca cyfryzacja i obecność osób indywidualnych, podmiotów prywatnych, jak również państw w cyberprzestrzeni sprawia, że są oni wystawieni na nowe, niespotykane do niedawna rodzaje zagrożeń. Sprawcą tych zagrożeń mogą być pojedyncze osoby, zorganizowane grupy przestępcze lub wywiady obcych państw. Zagrożenia i wektory ataków przyjmują różne postacie, a ich ewolucja trwa cały czas wraz z postępującym rozwojem szeroko rozumianej cyberprzestrzeni. Najpopularniejsze są ataki przy użyciu wirusów, malware czy ataki socjologiczne. Ich celem jest zazwyczaj chęć zysku, czego dobitnym dowodem są ataki z użyciem szkodliwego oprogramowania typu ransomware. Ataki są przeprowadzane również z czysto chuligańskich pobudek bez konkretnego celu.

Oprócz działań pojedynczych przestępców lub całych ich grup, niezwykle groźne są działania wywiadów obcych państw, które prowadzą w stosunku do siebie działania asymetryczne, tyle że nie w świecie rzeczywistym, a w cyberprzestrzeni. Dzięki odpowiedniej infrastrukturze, licznej kadrze doświadczonych informatyków, a także często nieograniczonym środkom są w stanie przeprowadzać skuteczne ataki na infrastrukturę obcych państw, np. energetykę, transport, media. Prowadzą również, a może przede wszystkim, liczne działania wywiadowcze.

Cyberprzestrzeń staje się również narzędziem do manipulacji całymi narodami. Dowodem na to są np. działania terrorystów islamskich czy Rosji, która jest oskarżana o wpływ na wyniki wyborów prezydenckich w USA lub na wyjście Wielkiej Brytanii z UE.

Niestety obecnie brak jest spójnych i jednolitych rozwiązań prawnych regulujących cyberataki o charakterze przestępczym, jak i te mające znamiona wojny cybernetycznej czy

informacyjnej. Dlatego aby móc skutecznie walczyć z coraz liczniejszymi zagrożeniami w cyberprzestrzeni potrzebne są nie tylko środki techniczne, organizacyjne, lecz również formalno-prawne ramy reagowania na cyberataki.

Przedmiotem niniejszego artykułu jest omówienie i porównanie prawnych podstaw cyberbezpieczeństwa na tle polskiego i europejskiego ustawodawstwa.

2. Historia i rozwój cyberataków

Rozwój zagrożeń pochodzących z cyberprzestrzeni postępował równolegle do rozwoju internetu oraz technik informatycznych. Nie tylko zagrożenia, lecz również cel i motywacje sprawców zmieniały się w czasie, wraz z postępującym rozwojem cyber-przestrzeni.

Początkowo ataki ograniczały się do użycia tzw. robaków (malware) oraz wirusów. Celem tych ataków były zazwyczaj podmioty prywatne, a z czasem również stacje prywatnych użytkowników. Motywacją sprawców ataku była z początku chęć wykazania się lub wykradzenia wrażliwych danych. Dopiero z czasem, w szczególności od końca ubiegłego wieku, główna motywacja ataków przyjęła charakter finansowy. Kolejnym motywem, którym kierują się przede wszystkim organizacje terrorystyczne i wywiady obcych państw jest wojna informacyjna, ataki na infrastrukturę innych państw, a także działania o charakterze szpiegowskim.

Poniżej zostały przedstawione przykładowe cyberataki, które miały miejsce na przestrzeni ostatnich kilkunastu lat:

1. **1998–2000 r. Moonlight Maze –** kampania ataków przeprowadzona przez grupę hakerów o nazwie Moonlight Maze. Ataki były wymierzone m.in. w Pentagon, NASA i inne organizacje rządowe. Był to jeden z pierwszych zaawansowanych cyberataków z wykorzystaniem trojana, skierowanych przeciwko systemom Solaris [2].
2. **2003 r. Titan Rain –** oznaczenie nadane przez rząd federalny USA po serii skoordynowanych ataków na amerykańskie systemy komputerowe. Sugeruje się, że za atakami stał chiński rząd, chociaż ich dokładny charakter i cel pozostaje nieznany. Hakerzy Titan Rain uzyskali dostęp do wielu sieci komputerowych firm o istotnym znaczeniu dla USA, a ich celem były poufne informacje znajdujące się na serwerach takich firma jak Lockheed Martin, Sandia National Laboratories, Redstone Arsenal i NASA [3].
3. **2007 r. Atak cybernetyczny na Estonię –** w maju 2007 r. systemy komputerowe organizacji rządowych oraz podmiotów prywatnych (m.in. sieci energetyczne, banki) stały się celem zorganizowanych ataków typu DoS. Władze tego kraju publicznie oskarżyły Rosję o inspirowanie tych działań.

4. **2007 r. Syria** – Izraelczycy wykorzystali wirusa komputerowego Suter, który pozwolił nie tylko na atak na sieci komputerowe i telekomunikacyjne syryjskiego systemu obrony przeciwlotniczej, ale jednocześnie na monitorowanie i przejęcie kontroli m.in. nad systemami radarowymi obrony powietrznej. Dzięki temu zbombardowano syryjski ośrodek wojskowy, w którym prowadzono prace nad bronią atomową, bez zaalarmowania syryjskiej obrony przeciwlotniczej. Jest to przykład użycia ataku cybernetycznego w celach militarnych.
5. **2008 r. Osetia** – atak cybernetyczny na gruzińskie media, agencje informacyjne, stronę internetową prezydenta Micheila Saakaszwiliego, rządu, ministra spraw zagranicznych oraz ministra obrony. Atak został przeprowadzony z wykorzystaniem botnetu. Sposób działania oraz ślady wskazują na rosyjskich hakerów [4].
6. **2009 r. Operacja Aurora** – cyberatak chińskich hakerów z wykorzystaniem podatności 0-day w programie Internet Explorer. Zaatakowane zostały amerykańskie firmy m.in.: Google, Adobe Systems, Northrop Grumman, Yahoo i Symantec. Celem ataku było uzyskanie nowoczesnych technologii oraz specjalistycznego oprogramowania używanego przez te firmy [5].
7. **2014 r. Atak na Sony Pictures –** 24 listopada 2014 r. grupa hakerów o nazwie Guardians of Peace z powodzeniem przeprowadziła cyberatak na Sony Pictures Entertainment, uzyskując dostęp do informacji 47 tys. obecnych i byłych pracowników Sony Pictures Entertainment oraz do poufnych wiadomości e-mail dotyczących aktorów, transakcji finansowych, wynagrodzeń kadry kierowniczej i pełnych kopii niewydanych filmów.
8. **2015 r. Wyciek danych z portalu Ashley Madison –** w lipcu 2015 r. portal randkowy Ashley Madison, wykorzystywany do zdrad małżeńskich, został zaatakowany przez hakerów z Impact Team. Wykradziono i ujawniono dane blisko 37 milionów użytkowników, łącznie ponad 300 GB danych, w tym m.in. prawdziwe nazwiska użytkowników, dane bankowe, transakcje kartą kredytową. Wyciek danych użytkowników na tak wielką skalę był rezultatem przede wszystkim słabych zabezpieczeń portalu, braku usuwania danych wrażliwych użytkowników [6].

3. Rodzaje cyberataków

Wśród cyberzagrożeń szczególnie istotne są te wymierzone przeciwko infrastrukturze krytycznej państwa, kontrolowanej za pomocą systemów informatycznych. Dlatego wyjątkowo niebezpieczne są ataki skierowane np. na systemy komunikacyjne, energetykę czy transport. W ujęciu militarnym można wyróżnić cztery podstawowe formy ataku informacyjnego:

- zrywanie procedur wymiany informacji,

- manipulowanie informacją (dezinformacja, zatajanie, przekształcanie informacji),
- nieautoryzowane korzystanie z zasobów informacyjnych (np. baz danych) oraz kopiowanie i niszczenie danych,
- masowe niszczenie oprogramowania systemowego.

Ataki tego typu mogą być prowadzone z wykorzystaniem następujących metod i narzędzi:

- wirusów komputerowych,
- bomb logicznych,
- blokowania wymiany informacji w systemach łączności,
- fałszowania informacji znajdujących się w bazach danych w systemach informatycznych przeciwnika,
- wprowadzania w obieg – z wykorzystaniem różnych technologii komunikowania – spreparowanych informacji [7].

Złośliwe oprogramowanie (malware)

Są to wszelkiego rodzaju aplikacje, skrypty i fragmenty kodu mające szkodliwy wpływ na systemy komputerowe. Przyjmują one różnorakie postacie np. wirusów, koni trojańskich, robaków oraz ransomware [8].

Phishing

Phishing to jedna z form oszustwa internetowego polegająca na podstępnym wyłudzeniu od użytkownika jego danych (np. haseł, numerów kart kredytowych, danych kont bankowych), poprzez podszycie się pod osobę lub instytucję.

Atak phishingowy oparty jest na socjotechnice i polega na przesyłaniu wiadomości podszywających się pod powiadomienia, wiadomości od kontrahentów, podmioty sektora finansowego, ubezpieczeniowego itp. Wiadomości te namawiają do podania danych przez użytkownika lub do zalogowania się w konkretnym systemie w celu zaktualizowania informacji, dzięki czemu dochodzi do przejęcia danych przez cyberprzestępców.

"Man in the middle" (MITM)

Atak typu "Man in the middle" (z ang. *człowiek w środku)* oznacza, że osoba atakująca system włącza się do komunikacji pomiędzy dwiema stronami i potajemnie zajmuje miejsce pomiędzy nimi. Dzięki temu pośredniczy w wymianie wszystkich wiadomości, podszywając się pod przeciwne strony (np. strona internetowa banku, poczta e-mail) [9]. Innymi słowy cała komunikacja pomiędzy stronami przechodzi przez atakującego, który może przechwytywać wrażliwe informacje, uzyskując informacje o sposobie działania danego systemu i podatnościach [9].

Aby zapobiec takim atakom, należy stosować mechanizmy uwierzytelniania lub używanie podczas komunikowania się znanych kluczy publicznych, dostępnych na

przykład w publicznej bazie danych, zamiast klucza otrzymanego od domniemanej drugiej strony (czyli w tym przypadku od podszywającego się napastnika) [9].

Atak DDoS (Distributed Denial of Service) – rozproszona odmowa usługi

Ataki DDoS to jeden z łatwiejszych ataków służących do wywołania paraliżu systemu lub infrastruktury sieciowej, aplikacyjnej. Celem tego ataku jest wywołanie niedostępności serwera, usługi lub infrastruktury. Atak może przyjąć różne postaci: wysycenie przepustowości serwera, co prowadzi do jego niedostępności, lub wykorzystanie zasobów systemu maszyny i zablokowanie odpowiedzi na poprawne zapytania. Innymi słowy polega na wysłaniu na serwer tak wielu informacji, że nie daje on rady z ich przetworzeniem i przerywa działanie [10].

SQL Injection

SQL Injection (SQLi) to metoda cyberataku polegająca na wstrzykiwaniu dodatkowych procedur do zapytania SQL, które wygenerowane przez aplikację jest przekazywane do bazy danych i tam wykonywane [11].

4. Prawne podstawy cyberbezpieczeństwa w Polsce i UE

W krajowym oraz unijnym porządku prawnym obszar cyberbezpieczeństwa został uregulowany odpowiednio ustawą o krajowym systemie cyberbezpieczeństwa [12] oraz dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywa 2016/1148), tzw. Dyrektywa NIS [13,17].

Przywołane powyżej regulacje są pewnym novum w unijnym oraz krajowym porządku prawnym. Są one odpowiedzią na zwiększającą się skalę i częstotliwość, a także wpływ cyberataków na prywatne oraz publiczne sieci i systemy informatyczne [13]. Ich celem jest stworzenie jednolitego i kompletnego systemu zarządzania ryzykiem cybernetycznym, w tym skutecznego i spójnego systemu reagowania na ataki oraz zagrożenia cybernetyczne. Ponadto mają one wpłynąć na poprawę wykrywania, zapobiegania i minimalizowania skutków ataków naruszających cyberbezpieczeństwo RP [13].

Zarówno ustawa, jak i rozporządzenie unijne wprowadzają jednolite definicje pojęć z obszaru cyberbezpieczeństwa oraz zasady postepowania, dzięki którym kraje UE będą mogły stworzyć ujednoliconą strategię lub przynajmniej zasady postępowania w zakresie utrzymania bezpieczeństwa cybernetycznego na obszarze Europejskiego Obszaru Gospodarczego. Ustawa wprowadza m.in. definicję legalną cyberbezpieczeństwa opisaną jako „odporność systemów informacyjnych na działania naruszające poufność,

integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".

Niestety prawodawca nie pokusił się o uregulowanie pojęcia „cyberprzestrzeni", które do tej pory nie doczekało się jednolitej definicji. Obecnie zarówno w Europie, jak i na świecie funkcjonuje wiele definicji „cyberprzestrzeni", co utrudnia utrzymanie bezpieczeństwa cyberprzestrzeni na globalnym poziomie. Proponuje się m.in., aby przyjąć, że cyberprzestrzeń to: zależny od czasu zbiór połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcję z tymi systemami" [14]. Istniejące bowiem definicje nie odnoszą się do całokształtu pojęcia cyberprzestrzeni, odwołując się do niektórych jej składników. Innymi słowy brak jest całościowej definicji tego pojęcia.

Reasumując, wydane regulacje zarówno krajowe, jak i unijne mają zdecydowanie pozytywny charakter. Stanowią one fundamenty do zbudowania jednolitego frontu przeciwko cyberprzestępcom oraz pozwolą skonsolidować rekcje krajów wchodzących w skład UE. Ujednolicenie przepisów powinno również pozytywnie wpłynąć na szybkość reakcji w przypadku ewentualnych cyberataków [15].

Oczywiście same regulacje prawne to dopiero pierwszy krok na drodze do stworzenia skutecznej strategii przeciwko cyberatakom. Kolejnym krokiem, może nawet znacznie trudniejszym, jest zbudowanie infrastruktury, która pozwoli wykorzystać w praktyce nowe regulacje. Obecnie za cyberbezpieczeństwo odpowiada MON (np. Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi oraz Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych), MSWiA, agencje typu ABW, SKW i SWW. Funkcjonuje również Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni, do którego zadań należy m.in. konsolidacja kompetencji i zasobów resortu obrony narodowej w obszarze kryptologii. Planowane jest również sformowanie wojsk obrony cyberprzestrzeni jednak ten komponent sił zbrojnych jest dopiero na etapie koncepcyjnym, planuje się że jego dowództwo zostanie powołane w 2022 r, zaś zdolność operacyjną osiągnie w 2024 r.

Niemniej, obecnie ich działania nie mają charakteru jednolitego, każda z tych instytucji działa samodzielnie. Również wydzielone siły i środki są dalece niewystarczające w stosunku do potrzeb i zagrożeń pochodzących z cyberprzestrzeni.

Na koniec warto zaznaczyć, iż w ocenie autorów omawiane regulacje dotyczą jedynie cyberataków o charakterze przestępczym, nie odnoszą się natomiast do ataków spełniających znamiona cyberwojny czy wojny informacyjnej. Dlatego postuluje się *de lege ferenda*, aby wprowadzić analogicznie jak w regulacjach USA przepisy dotyczące postępowania na wypadek wrogich aktów państw trzecich lub organizacji terrorystycznych przeprowadzanych w cyberprzestrzeni [16].

5. Podsumowanie

Rozwój cyberprzestrzeni i zagrożeń z nią związanych stanowi jedno z najważniejszych wyzwań, przed którymi stoi nie tylko Polska, lecz również inne kraje. Cyberprzestrzeń jest nowym polem walki, na którym dochodzi do ataków ze strony innych państw, grup terrorystycznych czy zorganizowanych grup przestępczych. Dlatego, zwłaszcza z punktu widzenia społeczeństwa informacyjnego, zapewnienie bezpieczeństwa sieci jest niezwykle ważne do stabilnego funkcjonowania i rozwoju gospodarki.

Pomimo wprowadzenia prawnych ram walki z cyberzagrożeniami w postaci ustawy o krajowym systemie cyberbezpieczeństwa oraz dyrektywy Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywa 2016/1148) konieczne jest jeszcze przełożenie tych przepisów na potrzebne środki techniczne i organizacyjne. Obecnie system obrony przed cyberzagrożeniami jest podzielony pomiędzy wiele państwowych instytucji, gdzie każda z nich ma swoje własne cele i zakres kompetencji. Potrzebne jest zbudowanie jednolitego systemu obrony i reagowania na zagrożenia pochodzące z cyberprzestrzeni, kontrolowanego przez jedną instytucję. Ponadto należy rozwijać możliwości prowadzenia operacji wyprzedzających, a nie tylko defensywnych.

6. Literatura

1. K. Liedel, M. Grzelak, Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, Bezpieczeństwo Narodowe nr 22, II – 212.
2. Cyberpaleontologia: 20-letni zaawansowany atak, który nadal jest istotny; https://www.kaspersky.pl/o-nas/informacje-prasowe/2767/cyberpaleontologia-20-letni-zaawansowany-atak-ktory-nadal-jest-istotny; [dostęp: 5 marca 2019 r.].
3. Titan Rain; https://tophackers.wordpress.com/8-titan-rain/; [dostęp: 5 marca 2019 r.].
4. Cyberatak na prezydenta Gruzji; https://www.computerworld.pl/news/Cyberatak-na-prezydenta-Gruzji,159559.html; [dostęp: 5 marca 2019 r.].
5. Cyberatak groźniejszy niż uderzenie atomowe; https://forsal.pl/artykuly/522363, cyberatak-grozniejszy-niz-uderzenie-atomowe.html; [dostęp: 2 maja 2019 r.].
6. A timeline of the Ashley Madison hack; https://digitalguardian.com/blog/timeline-ashley-madison-hack; [dostęp: 2 maja 2019 r.].
7. A. Urbanek, Cyberwojna – zagrożenie asymetryczne współczesnej przestrzeni bezpieczeństwa, Studia nad Bezpieczeństwem, Nr 1, ss. 5-32, Rok 2016.
8. Złośliwe oprogramowanie; https://pl.malwarebytes.com/malware/; [dostęp: 24 kwietnia 2019 r.].

9. Co to jest atak Man-in-the-Middle?; http://www.crypto-it.net/pl/ataki/man-in-the-middle.html, https://plblog.kaspersky.com/co-to-jest-atak-man-in-the-middle/186/; [dostęp: 24 kwietnia 2019 r.].
10. Czym jest atak DDoS (cz. 1) – podstawowe informacje; https://sekurak.pl/czym-jest-atak-ddos-cz-1-podstawowe-informacje/ [dostęp: 24 kwietnia 2019 r.]; Co to jest Anty-DDoS?; https://www.ovh.pl/anty-ddos/ochrona-przed-ddos.xml [dostęp: 6 grudnia 2018 r.].
11. 6 typów cyberataków, które zagrażają cyberbezpieczeństwu Twojej firmy; ttps://greywizard.com/pl/blog/article/67-6-typw-cyberatakw-ktre-zagraaj-cyberbezpieczestwu-twojej-firmy; [dostęp: 24 kwietnia 2019 r.].
12. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 poz. 1560).
13. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.
14. K. Liedel, M. Grzelak, Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, Bezpieczeństwo Narodowe nr 22, II – 212 za Cyberspace: Definition and Implications, Cooperative Cyber Defence Centre of Excellence, http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf.
15. Zieja M., Smoliński H., Gołda P.: Information systems as a tool for supporting the management of aircraft flight safety, Archives of Transport Volume 36, Issue 4, 2015, Pages 67-76.
16. Zieja M., Ważny M., Stępień S.: Outline of a method for estimating the durability of components or device assemb.lies while maintaining the required reliability level. Eksploatacja i Niezawodność – Maintenance and Reliability, Volume 20, Issue 2, 2018, Pages 260-266.
17. Zieja M., Woch M., Tomaszewska J.: Analysis of the time between failures of aircrafts, 2nd International Conference on System Reliability and Safety, ICSRS 2017, Volume 2018 - January, 29 January 2018, Pages 112-118.