



Temat 2 .

dr inż. Michał Malinowski

<https://www.drmalinowski.edu.pl>

Bezpieczeństwo narodowe
i przestrzeń
cyber/informacyjna

BEZPIECZEŃSTWO
INFORMACJI



- Bezpieczeństwo narodowe
- Bezpieczeństwo informacji
- Cyberbezpieczeństwo
- Usługa kluczowa
- Organizacja bezpieczeństwa informacji RP
- Incydenty bezpieczeństwa

Zadanie

Treść

Prezentacja zadania podczas zajęć.

Okolo 9 osób podczas zajęć

(0-2 pkt)



Bezpieczeństwo narodowe

Bezpieczeństwo narodowe

to stan, w którym państwo zapewnia ochronę swojej suwerenności, integralności terytorialnej oraz bezpieczeństwa obywateli przed zagrożeniami wewnętrznymi i zewnętrznymi.

Obejmuje ono działania mające na celu utrzymanie stabilności politycznej, gospodarczej i społecznej, a także ochronę przed różnorodnymi zagrożeniami, zarówno militarnymi, jak i niemilitarnymi.



Bezpieczeństwo narodowe

Kluczowe aspekty

Ochrona suwerenności państwa:

- Zapewnienie niezależności politycznej i decyzyjnej kraju

Integralność terytorialna:

- Utrzymanie nienaruszalności granic państwowych.

Bezpieczeństwo obywateli:

- Gwarantowanie życia, zdrowia i mienia mieszkańców kraju.

Stabilność wewnętrzna:

- Utrzymanie porządku publicznego oraz przeciwdziałanie zagrożeniom wewnętrznym, takim jak przestępczość czy terroryzm.

Obrona przed zagrożeniami zewnętrznymi:

- Przygotowanie i reagowanie na potencjalne agresje ze strony innych państw lub podmiotów.

Bezpieczeństwo narodowe

Elementy pojęcia bezpieczeństwa narodowego

Współcześnie bezpieczeństwo narodowe nie ogranicza się jedynie do aspektów militarnych.

Obejmuje również takie dziedziny jak:

Bezpieczeństwo ekonomiczne:

- Zapewnienie stabilności gospodarczej i ochrony interesów ekonomicznych kraju.

Bezpieczeństwo energetyczne:

- Gwarancja nieprzerwanych dostaw energii oraz dywersyfikacja źródeł energetycznych.

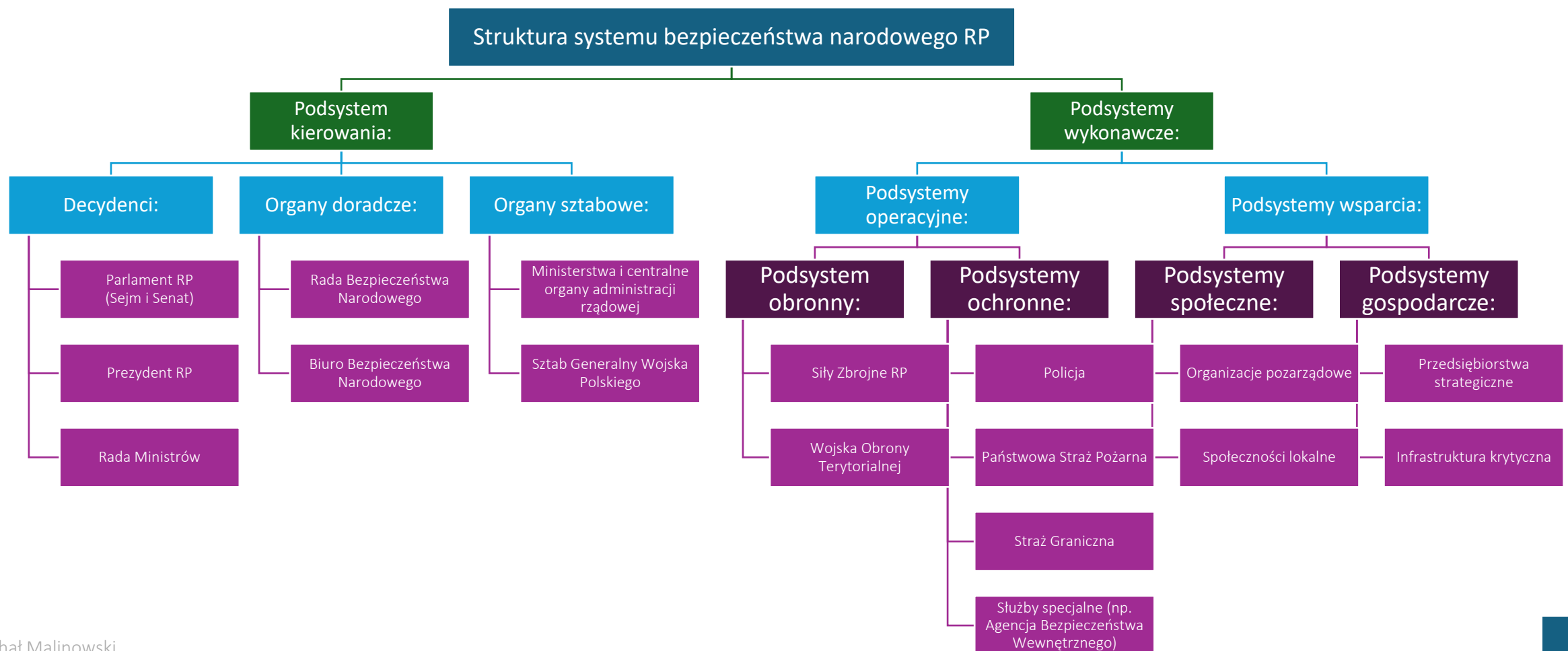
Bezpieczeństwo informacyjne:

- Ochrona przed zagrożeniami w cyberprzestrzeni oraz przeciwdziałanie dezinformacji.

Bezpieczeństwo ekologiczne:

- Dbłość o środowisko naturalne i przeciwdziałanie katastrofom ekologicznym.

Bezpieczeństwo narodowe



Podstawowe dokumenty

Nazwa dokumentu	Data publikacji	Opis	Link
Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.	2 kwietnia 1997 r.	Najwyższy akt prawny w Polsce, określający podstawy ustroju państwa, prawa i obowiązki obywateli oraz zasady funkcjonowania organów państwowych.	https://www.sejm.gov.pl/prawo/konst/polski/kon1.htm
Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2020 roku	12 maja 2020 r.	Dokument określający kompleksową wizję kształtowania bezpieczeństwa narodowego Polski we wszystkich jego wymiarach, uwzględniający zarówno aspekty wewnętrzne, jak i międzynarodowe.	https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf
Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej	21 listopada 1967 r.	Ustawa regulująca zasady obrony państwa, w tym obowiązki obywateli w zakresie obronności oraz organizację Sił Zbrojnych RP.	https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19670440220
Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym	26 kwietnia 2007 r.	Ustawa definiująca zasady organizacji i funkcjonowania systemu zarządzania kryzysowego w Polsce, mającego na celu zapobieganie sytuacjom kryzysowym oraz reagowanie na nie.	https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdU20070890590
Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych	5 sierpnia 2010 r.	Ustawa określająca zasady ochrony informacji niejawnych, w tym organizację i funkcjonowanie systemu ochrony takich informacji w Polsce.	https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101821228
Traktat Północnoatlantycki (NATO)	4 kwietnia 1949 r.	Międzynarodowy traktat ustanawiający Sojusz Północnoatlantycki, którego Polska jest członkiem od 1999 roku, stanowiący fundament zbiorowej obrony i współpracy w zakresie bezpieczeństwa.	https://www.nato.int/cps/en/natolive/official_texts_17120.htm
Protokół do Traktatu Północnoatlantyckiego o akcesji Rzeczypospolitej Polskiej	12 marca 1999 r.	Dokument formalizujący przystąpienie Polski do NATO, określający warunki członkostwa i zobowiązania wynikające z traktatu.	https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.bbn.gov.pl/download/1/15755/ProtokoldoTraktatu.pdf&ved=2ahUKEwjSwla13_qLAX8FBAIHU5KNagQFnoECBUQAQ&usg=AOvVaw3r9Hdfsx6GFvf3v8NRR73L
Koncepcja Strategiczna NATO z 2010 r.	19 listopada 2010 r.	Dokument określający cele i zadania NATO w zmieniającym się środowisku bezpieczeństwa, w tym strategię reagowania na współczesne zagrożenia.	https://www.nato.int/cps/en/natolive/official_texts_68580.htm
Raport o zagrożeniach bezpieczeństwa narodowego	2020 r.	Dokument wskazujący najważniejsze zagrożenia dla bezpieczeństwa narodowego oraz oceniający ryzyko ich wystąpienia, stanowiący podstawę do planowania działań zaradczych.	https://www.gov.pl/web/rcb/raport-o-zagrozeniach-bezpieczenstwa-narodowego
Rekomendacje do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2024 roku	4 lipca 2024 r.	Dokument zawierający rekomendacje dotyczące aktualizacji i dostosowania strategii bezpieczeństwa narodowego w odpowiedzi na zmieniające się uwarunkowania i pojawiające się nowe zagrożenia.	https://www.prezydent.pl/storage/file/core_files/2024/7/4/7fa9f08052b51758d6ed4e9a11a9d32d/REKOMENDACJE%20SBNRP%204%20lipca%202024.pdf

Bezpieczeństwo informacji

Bezpieczeństwo informacji

jest rozumiane jako ochrona informacji i systemów informacyjnych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem działania, modyfikacją lub zniszczeniem w celu zapewnienia poufności, integralności i dostępności.

W polskim porządku prawnym, kwestie związane z bezpieczeństwem informacji są regulowane przez szereg aktów prawnych, takich jak:

Nazwa dokumentu	Data publikacji	Link
Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych	5 sierpnia 2010 r.	https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101821228
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych	10 maja 2018 r.	https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	5 lipca 2018 r.	https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

Bezpieczeństwo informacji

Poufność

Właściwość informacji polegająca na tym, że dostęp do niej mają wyłącznie osoby, podmioty lub procesy uprawnione, a jest ona chroniona przed dostępem nieautoryzowanym lub nieuprawnionym ujawnieniem.

Kluczowe aspekty

Ochrona przed nieuprawnionym dostępem

- Zapobieganie włamaniom do systemów informatycznych.
- Kontrola dostępu do informacji (uprawnienia, uwierzytelnianie).

Ochrona przed nieautoryzowanym ujawnieniem

- Ograniczenie ryzyka wycieku informacji poufnych.
- Stosowanie szyfrowania danych podczas transmisji i przechowywania.

Klasyfikacja informacji

- Informacje jawne, poufne, tajne i ściśle tajne (zgodnie z Ustawą o ochronie informacji niejawnych).

Wycieki danych osobowych (np. numery PESEL, dane medyczne).

Przechwycenie korespondencji elektronicznej (np. e-maili służbowych)

Szpiegostwo przemysłowe.

Bezpieczeństwo informacji

Integralność

właściwość informacji polegająca na zachowaniu jej dokładności, kompletności oraz niezmienności. Integralność zapewnia ochronę przed nieautoryzowaną lub przypadkową modyfikacją, zniszczeniem albo utratą danych.

Kluczowe aspekty

Dokładność informacji

- Zapewnienie, że dane pozostają prawidłowe i wiarygodne.
- Zapobieganie błędom podczas transmisji, przetwarzania oraz przechowywania informacji.

Kompletność informacji

- Gwarancja, że wszystkie dane są dostępne w pełnym, niezmienionym kształcie.
- Ochrona przed przypadkowym lub zamierzonym usunięciem części informacji.

Niezmiennność informacji

- Zapewnienie, że informacje nie zostały nieuprawnienie zmienione.
- Stosowanie mechanizmów kontrolnych (np. sumy kontrolne, podpisy cyfrowe).

Nieuprawnione zmiany danych w systemie bankowym (np. zmiana salda konta).

Zainfekowanie baz danych przez złośliwe oprogramowanie (ransomware).

Błędy w aktualizacji oprogramowania powodujące utratę integralności kluczowych danych.

Bezpieczeństwo informacji

Dostępność

właściwość informacji oraz powiązanych z nią zasobów, zapewniająca, że uprawnione osoby, podmioty lub procesy mają możliwość uzyskania dostępu do informacji w wymaganym czasie i zakresie, bez zakłóceń.

Kluczowe aspekty

Dokładność informacji

- Zapewnienie, że dane pozostają prawidłowe i wiarygodne.
- Zapobieganie błędom podczas transmisji, przetwarzania oraz przechowywania informacji.

Kompletność informacji

- Gwarancja, że wszystkie dane są dostępne w pełnym, niezmienionym kształcie.
- Ochrona przed przypadkowym lub zamierzonym usunięciem części informacji.

Niezmienność informacji

- Zapewnienie, że informacje nie zostały nieuprawnienie zmienione.
- Stosowanie mechanizmów kontrolnych (np. sumy kontrolne, podpisy cyfrowe).

Ataki typu DoS/DDoS – blokowanie dostępu do usług sieciowych.

Awaria systemów krytycznych – niedostępność usług bankowych, administracyjnych czy komunikacyjnych.

Uszkodzenie infrastruktury telekomunikacyjnej przez prace budowlane – np. koparka przecinająca światłowody

Cyberbezpieczeństwo

Cyberbezpieczeństwo

to szczególny obszar bezpieczeństwa informacji, koncentrujący się na ochronie informacji w środowisku cyfrowym przed cyberzagrożeniami, takimi jak ataki hakerskie, malware, phishing, czy ataki DDoS.

Cyberbezpieczeństwo

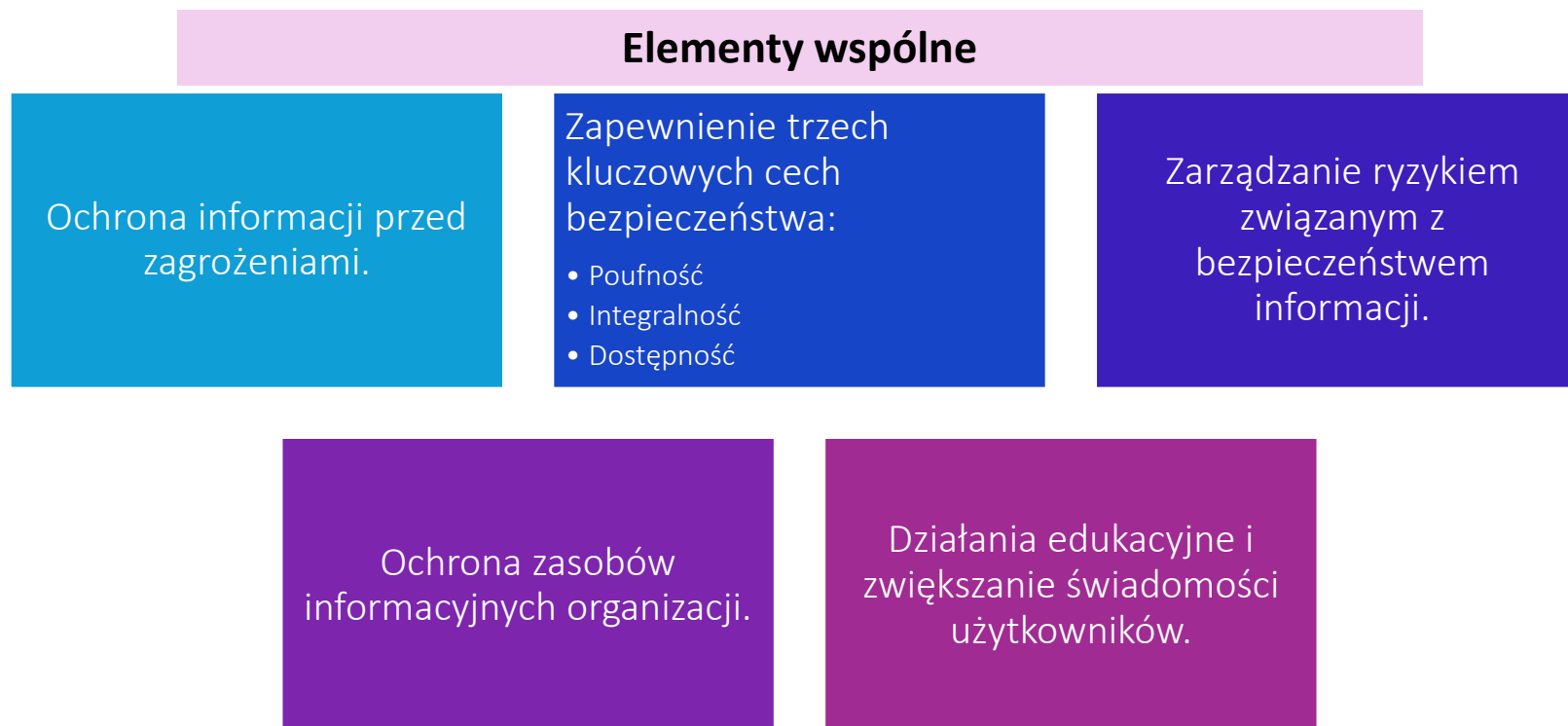
odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych oraz związanych z nimi usług oferowanych przez te systemy; obejmuje również umiejętność skutecznego przeciwdziałania incydom cyberbezpieczeństwa oraz minimalizowania skutków takich incydentów.

Źródło definicji:

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560)

Cyberbezpieczeństwo

Cyberbezpieczeństwo vs bezpieczeństwo informacji



Cyberbezpieczeństwo

Kluczowe różnice

Kryterium	Bezpieczeństwo informacji	Cyberbezpieczeństwo
Zakres ochrony	Informacje w każdej formie (papierowej, elektronicznej, ustnej).	Informacje i systemy w formie cyfrowej (elektronicznej).
Rodzaj zagrożeń	Wszystkie rodzaje zagrożeń dla informacji (fizyczne, techniczne, organizacyjne).	Zagrożenia związane z technologią cyfrową i internetem (cyberataki, malware).
Metody ochrony	Techniczne, fizyczne i organizacyjne.	Przede wszystkim techniczne i technologiczne.
Podstawy prawne	Szersze, obejmujące ustawy dotyczące danych osobowych, informacji niejawnych, zarządzania kryzysowego.	Specjalistyczne, np. Ustawa o krajowym systemie cyberbezpieczeństwa.
Cel działań	Ochrona całościowa zasobów informacyjnych.	Ochrona przed cyberzagrożeniami i incydentami w przestrzeni cyfrowej.

Cyberbezpieczeństwo

Autentyczność

właściwość informacji oraz systemów informacyjnych polegająca na możliwości jednoznacznego potwierdzenia tożsamości osób, podmiotów lub źródła pochodzenia informacji, zapewniająca, że informacja jest prawdziwa i pochodzi od deklarowanego nadawcy.

Kluczowe aspekty

Uwierzytelnianie tożsamości

- Potwierdzenie, że użytkownicy lub systemy są faktycznie tymi, za których się podają.
- Stosowanie metod takich jak hasła, uwierzytelnianie wieloskładnikowe (MFA) lub biometria.

Weryfikacja źródła informacji

- Możliwość potwierdzenia, że informacje nie zostały sfałszowane lub zmanipulowane.
- Używanie podpisów cyfrowych, certyfikatów elektronicznych i kryptografii asymetrycznej.

Zapewnienie wiarygodności informacji

- Zabezpieczanie przed podszywaniem się (spoofingiem).
- Ochrona przed manipulacją danych w trakcie transmisji.

Podszywanie się pod nadawcę e-maila (phishing).

Fałszowanie podpisów elektronicznych w dokumentach cyfrowych.

Nieautoryzowane użycie cudzych danych dostępowych do systemu.

Cyberbezpieczeństwo

Cyberprzestrzeń

przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, w tym sieci informatyczne wraz z ich powiązaniem i relacjami z użytkownikami

Źródło definicji:

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560)

Element cyberprzestrzeni	Opis elementu
Systemy teleinformatyczne	Urządzenia oraz oprogramowanie służące do gromadzenia, przetwarzania i przesyłania informacji (komputery, serwery, aplikacje).
Sieci informatyczne	Infrastruktura umożliwiająca transmisję danych między urządzeniami (np. LAN, WAN, Internet).
Dane	Informacje przechowywane, przetwarzane i wymieniane w postaci elektronicznej.
Użytkownicy	Osoby fizyczne, instytucje oraz organizacje wykorzystujące zasoby cyberprzestrzeni.
Powiązania i relacje	Zależności i interakcje pomiędzy użytkownikami, systemami teleinformatycznymi oraz sieciami, umożliwiające efektywną wymianę informacji.

Cyberbezpieczeństwo

Incydent cyberbezpieczeństwa

zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo, skutkując zagrożeniem poufności, integralności lub dostępności informacji.

Kluczowe aspekty

Realne lub potencjalne zagrożenie

- Może powodować szkody lub zakłócenia działania usług cyfrowych.
- Obejmuje zarówno celowe ataki, jak i przypadkowe zdarzenia.

Wpływ na bezpieczeństwo informacji

- Naruszenie poufności, integralności lub dostępności danych.
- Możliwość zakłócenia działania systemów krytycznych.

Obowiązki związane z incydem

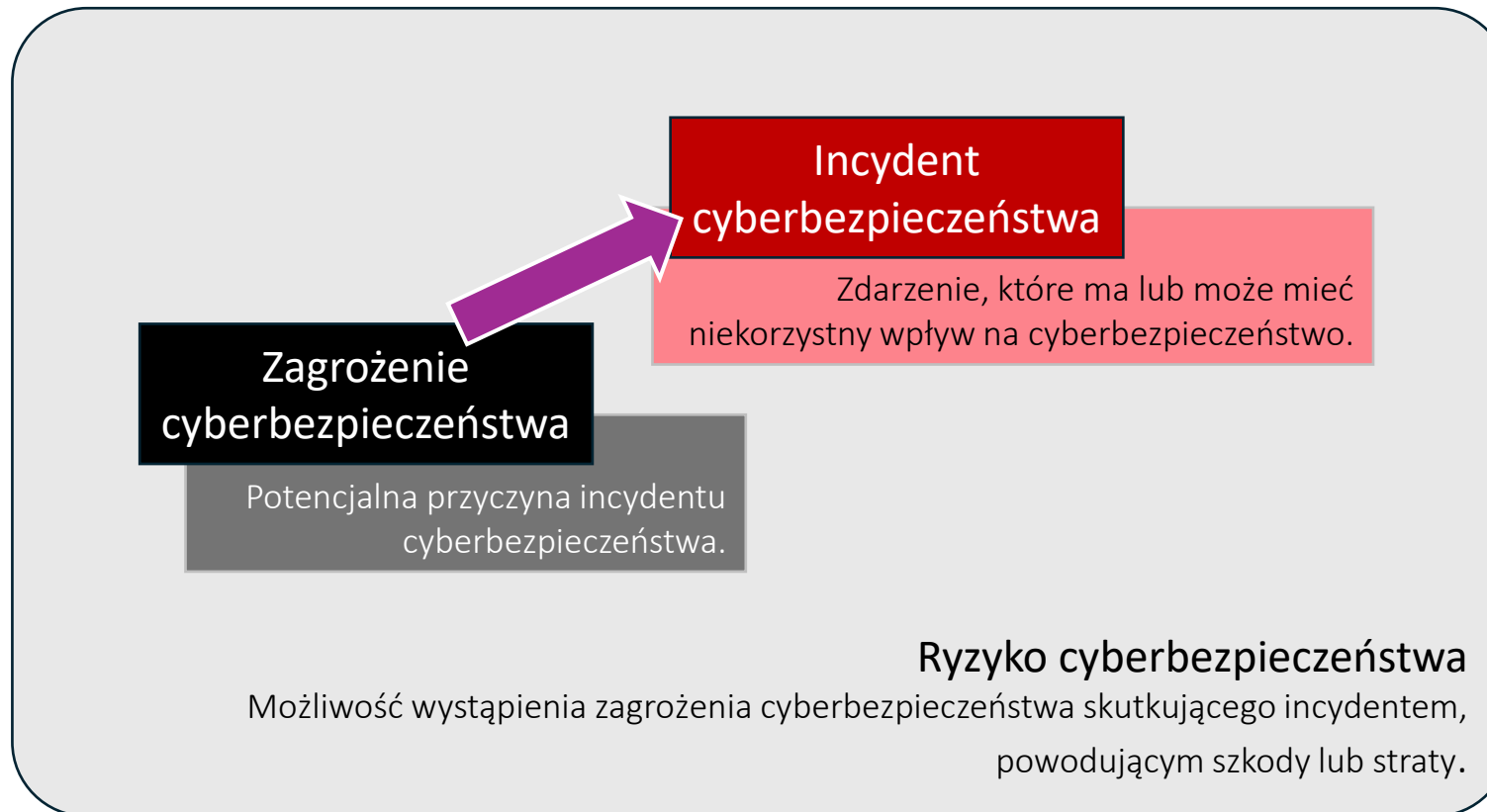
- Zgłoszenie incydentu do właściwego zespołu CSIRT.
- Analiza przyczyn i ograniczenie skutków incydentu.

Atak ransomware blokujący dostęp do danych organizacji.

Wyciek danych osobowych klientów z serwera firmy.

Próba przejęcia kontroli nad systemem informatycznym instytucji publicznej.

Cyberbezpieczeństwo



Usługa kluczowa

Usługa cyfrowa

to usługa świadczona drogą elektroniczną, umożliwiającą przetwarzanie, przechowywanie, udostępnianie lub przesyłanie danych cyfrowych. Jest realizowana przez podmioty publiczne lub prywatne i stanowi kluczowy element funkcjonowania nowoczesnej gospodarki, administracji publicznej oraz społeczeństwa

(Przemysł 4.0 , 5.0).

Sektor	Przykłady usług cyfrowych
Administracja publiczna	ePUAP, CEIDG, e-ZUS, e-PIT, e-Dowód
Finanse i bankowość	Blik, bankowość internetowa (iPKO, mBank), PayU, Stripe, giełdy kryptowalut (Binance, Coinbase)
Handel elektroniczny	Allegro, Amazon, eBay, Shopify, systemy obsługi płatności (PayPal)
Telekomunikacja i media	Netflix, YouTube, Spotify, Zoom, Microsoft Teams, usługi VoIP
Chmura obliczeniowa	AWS, Google Cloud, Microsoft Azure, Dropbox, OneDrive
Zdrowie i medycyna	e-recepta, e-skierowanie, telemedycyna (ZnanyLekarz, Telmedicin), elektroniczna dokumentacja medyczna
Edukacja i szkolenia	Coursera, Udemy, Moodle, Google Classroom, Microsoft Teams for Education

Usługa kluczowa

Usługa kluczowa

usługa świadczona przez podmiot publiczny lub prywatny, niezbędna do utrzymania krytycznej działalności społecznej lub gospodarczej, której zakłócenie mogłoby istotnie wpłynąć na bezpieczeństwo publiczne, zdrowie obywateli lub gospodarkę.

Sektor	Przykłady usług kluczowych
Energetyczny	Dystrybucja energii elektrycznej Dostawa paliw płynnych Dostawy gazu ziemnego
Transportowy	Zarządzanie ruchem lotniczym (PAŻP) Usługi sterowania ruchem kolejowym (PKP PLK) Systemy zarządzania ruchem miejskim
Bankowy i infrastruktury rynków finansowych	Obsługa systemów płatniczych (np. Elixir, Blik) Usługi bankowości internetowej Obsługa transakcji giełdowych (GPW)
Ochrony zdrowia	Systemy e-recepty oraz e-skierowania Systemy telemedyczne (np. telekonsultacje medyczne) Elektroniczna dokumentacja medyczna
Zaopatrzenia w wodę pitną i jej dystrybucji	Dostarczanie wody pitnej Oczyszczanie i uzdatnianie wody Monitoring jakości wody
Infrastruktury cyfrowej	Usługi chmury obliczeniowej (np. GovCloud) Centra danych zapewniające ciągłość usług publicznych Utrzymanie sieci telekomunikacyjnych

Usługa kluczowa

Operator usługi kluczowej

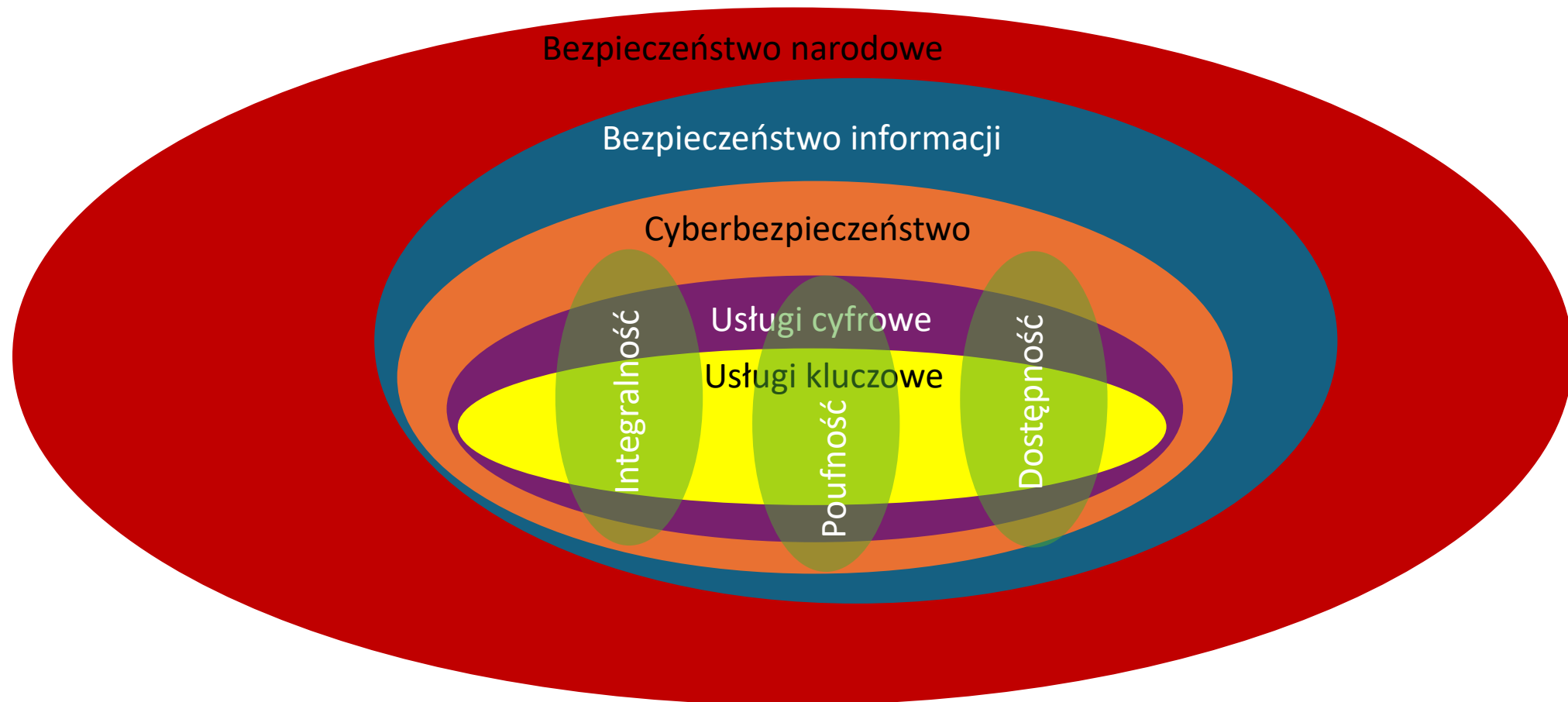
Podmiot świadczący usługi kluczowe dla utrzymania działalności społeczno-gospodarczej, podlegający szczególnym obowiązkom w zakresie cyberbezpieczeństwa.

Dostawca usług cyfrowych

Podmiot świadczący usługi cyfrowe takie jak usługi przetwarzania w chmurze, wyszukiwarki internetowe oraz platformy handlu elektronicznego.

Kryterium	Operator usługi kluczowej	Dostawca usług cyfrowych
Zakres usług	Usługi niezbędne do funkcjonowania społeczeństwa i gospodarki (np. energetyka, zdrowie, transport)	Usługi cyfrowe: platformy handlu elektronicznego, usługi chmurowe, wyszukiwarki internetowe
Wpływ zakłóceń na społeczeństwo	Bezpośredni, istotny wpływ na bezpieczeństwo publiczne, zdrowie obywateli lub gospodarkę	Pośredni wpływ na działalność gospodarczą i społeczną (np. e-commerce)
Wymagania formalne i regulacje	Surowe wymagania regulacyjne, obowiązkowe zgłaszanie incydentów, obowiązek stosowania środków bezpieczeństwa	Łagodniejsze wymagania regulacyjne, obowiązkowe zgłaszanie tylko istotnych incydentów
Rodzaj podmiotów	Zazwyczaj infrastruktura krytyczna: szpitale, banki, operatorzy energetyczni, wodociągi	Firmy cyfrowe: dostawcy chmury (np. Amazon AWS, Google Cloud), wyszukiwarki (np. Google), platformy e-commerce
Nadzór organów państwowych	Ścisły nadzór organów państwowych (np. sektorowe CSIRT)	Mniejszy stopień kontroli, ogólnokrajowe CSIRT-y

Domeny bezpieczeństwa



Organizacja bezpieczeństwa informacji RP

Instytucje odpowiedzialne za bezpieczeństwo informacji w Polsce



NASK

RCB

CERT.PL
NASK



C: [SIRT/MON]

Organizacja bezpieczeństwa informacji RP

Instytucje odpowiedzialne za bezpieczeństwo informacji w Polsce

Instytucja	Zakres odpowiedzialności	Podstawa prawna
Agencja Bezpieczeństwa Wewnętrznego (ABW)	Ochrona informacji niejawnych, nadzór nad systemem ochrony informacji niejawnych	Ustawa o ochronie informacji niejawnych (2010)
Urząd Ochrony Danych Osobowych (UODO)	Nadzór nad ochroną danych osobowych, kontrola przestrzegania RODO	Ustawa o ochronie danych osobowych (2018) oraz RODO
Ministerstwo Cyfryzacji	Koordinacja krajowego systemu cyberbezpieczeństwa	Ustawa o krajowym systemie cyberbezpieczeństwa (2018)
Biuro Bezpieczeństwa Narodowego (BBN)	Opracowywanie strategii bezpieczeństwa narodowego, analiza zagrożeń strategicznych	Strategia Bezpieczeństwa Narodowego RP
Rządowe Centrum Bezpieczeństwa (RCB)	Zarządzanie kryzysowe, koordynacja reagowania na zagrożenia o charakterze narodowym	Ustawa o zarządzaniu kryzysowym (2007)
CSIRT NASK, CSIRT GOV, CSIRT MON	Reagowanie na incydenty cyberbezpieczeństwa oraz ich analiza	Ustawa o krajowym systemie cyberbezpieczeństwa (2018)
Ministerstwo Obrony Narodowej (MON)	Ochrona informacji niejawnych oraz cyberbezpieczeństwo sektora obronnego	Ustawa o ochronie informacji niejawnych (2010)
NASK Państwowy Instytut Badawczy	Realizacja zadań CSIRT na poziomie krajowym, reagowanie na incydenty cyberbezpieczeństwa	Ustawa o krajowym systemie cyberbezpieczeństwa (2018)

Organizacja bezpieczeństwa informacji RP

Ministerstwo Cyfryzacji

- Opracowywanie i koordynowanie polityki państwa w zakresie bezpieczeństwa informacji oraz cyberbezpieczeństwa.
- Przygotowanie projektów regulacji prawnych i nadzorowanie ich wdrażania.
- Koordynowanie krajowych działań związanych z cyberbezpieczeństwem.



Biuro Bezpieczeństwa Narodowego (BBN)

- Opracowywanie strategii oraz rekomendacji w obszarze bezpieczeństwa narodowego.
- Współpraca z innymi instytucjami w zakresie bezpieczeństwa informacyjnego i cyberbezpieczeństwa.



Organizacja bezpieczeństwa informacji RP

Agencja Bezpieczeństwa Wewnętrznego (ABW)

- Ochrona informacji niejawnych, zapobieganie szpiegostwu, cyberprzestępczości i terroryzmowi.
- Monitoring i przeciwdziałanie zagrożeniom związanym z bezpieczeństwem informacji.



Urząd Ochrony Danych Osobowych (UODO)

- Nadzór nad przestrzeganiem przepisów o ochronie danych osobowych (RODO).
- Wydawanie decyzji administracyjnych w przypadku naruszeń bezpieczeństwa danych osobowych.



Organizacja bezpieczeństwa informacji RP

Rządowe Centrum Bezpieczeństwa (RCB)

- Koordynacja działań zarządzania kryzysowego w sytuacjach zagrożeń bezpieczeństwa informacyjnego.
- Analiza zagrożeń dla bezpieczeństwa publicznego oraz informacyjnego kraju.



NASK Państwowy Instytut Badawczy

- Monitorowanie zagrożeń cybernetycznych oraz koordynacja działań reagowania na incydenty w cyberprzestrzeni.
- Prowadzenie badań naukowych oraz wdrażanie innowacyjnych technologii na rzecz zwiększenia bezpieczeństwa cyfrowego w Polsce.



Organizacja bezpieczeństwa informacji RP

Zespoły reagowania na incydenty komputerowe (CSIRT)

- Obsługa zgłoszeń o incydentach cyberbezpieczeństwa.
- Koordynacja działań w odpowiedzi na incydenty.
- Monitorowanie zagrożeń w cyberprzestrzeni i ostrzeganie użytkowników.

CSIRT GOV (dawniej CERT.GOV.PL)

- Zlokalizowany w Agencji Bezpieczeństwa Wewnętrznego (ABW)
- Obsługuje sektor administracji rządowej.

CSIRT MON (CSIRT Ministerstwa Obrony Narodowej)

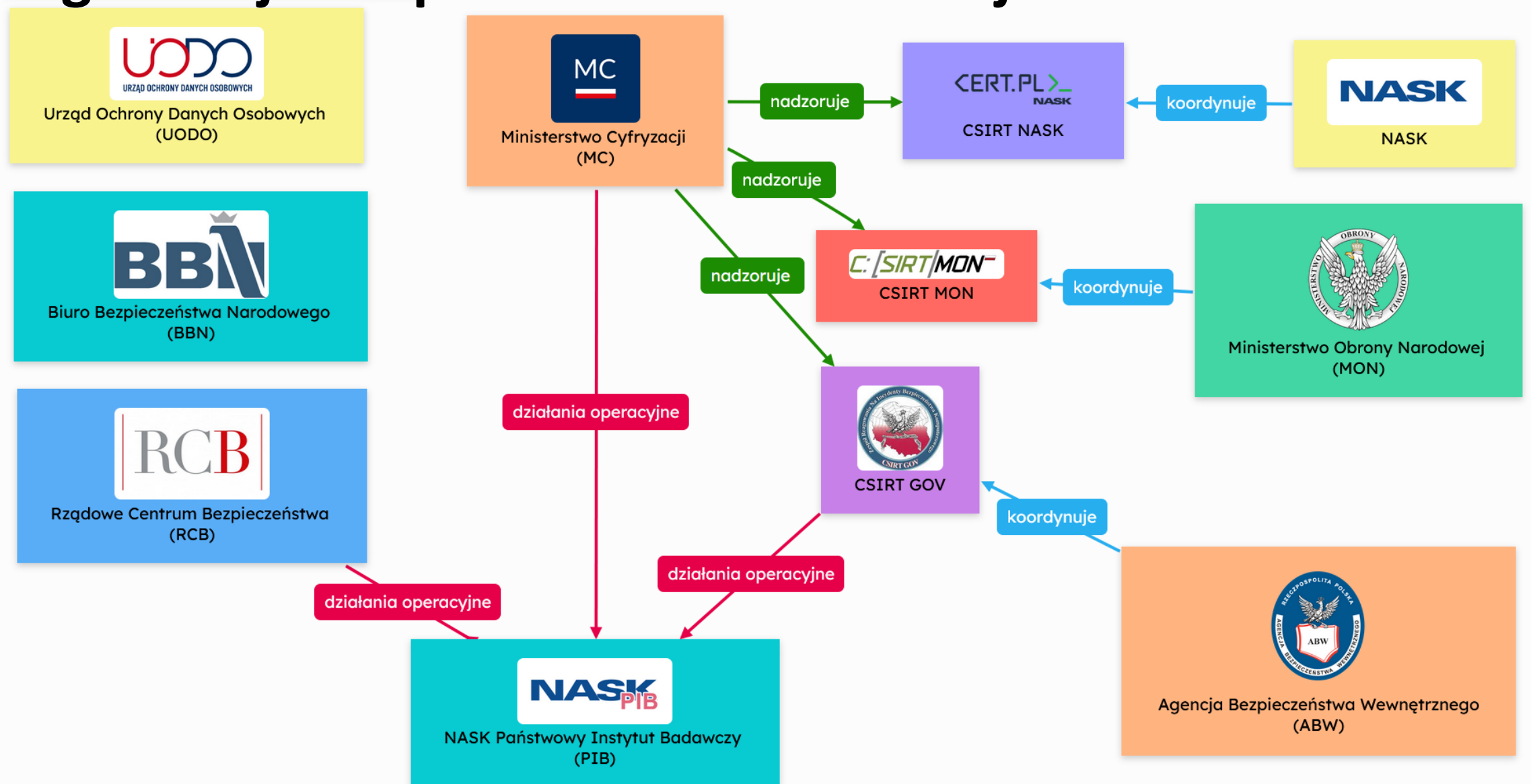
- Zlokalizowany w Dowództwie Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC)
- Obsługuje sektor obronności.

CSIRT NASK (CERT Polska)

- Zlokalizowany w NASK Państwowym Instytucie Badawczym
- Cywilny zespół reagowania na incydenty, obejmuje sektor prywatny oraz obywateli.



Organizacja bezpieczeństwa informacji RP

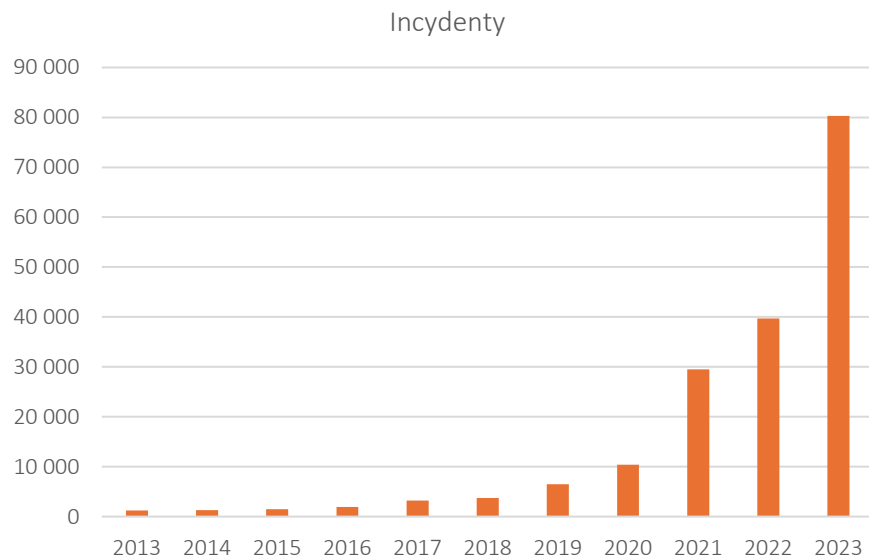


Organizacja bezpieczeństwa informacji RP

Relacje pomiędzy instytucjami	Opis współpracy i powiązań
Ministerstwo Cyfryzacji ↔ CSIRT NASK, CSIRT GOV, CSIRT MON	Ministerstwo Cyfryzacji nadzoruje działania zespołów CSIRT w ramach krajowego systemu cyberbezpieczeństwa. Odpowiada za politykę i strategię reagowania na incydenty.
Agencja Bezpieczeństwa Wewnętrznego ↔ CSIRT GOV	ABW koordynuje działania CSIRT GOV odpowiedzialnego za bezpieczeństwo sektora administracji publicznej oraz ochronę informacji niejawnych.
Ministerstwo Obrony Narodowej ↔ CSIRT MON	MON sprawuje nadzór nad działalnością CSIRT MON, który zabezpiecza sektor obronności oraz wojskowe systemy informacyjne.
NASK PIB ↔ Ministerstwo Cyfryzacji, CSIRT GOV, RCB	NASK PIB realizuje działania operacyjne w zakresie reagowania na incydenty cyberbezpieczeństwa, dostarcza raporty o zagrożeniach, współpracuje bezpośrednio z Ministerstwem Cyfryzacji oraz RCB w przypadku zarządzania kryzysowego.
Rządowe Centrum Bezpieczeństwa ↔ Wszystkie wymienione instytucje	RCB koordynuje zarządzanie kryzysowe na poziomie krajowym, współpracując ze wszystkimi wymienionymi instytucjami w sytuacjach poważnych zagrożeń informacyjnych lub cyberataków.
Urząd Ochrony Danych Osobowych ↔ Wszystkie instytucje	UODO monitoruje przestrzeganie przepisów dotyczących ochrony danych osobowych we wszystkich wymienionych instytucjach i interweniuje w przypadku ich naruszenia.
Biuro Bezpieczeństwa Narodowego ↔ Wszystkie instytucje	BBN przygotowuje ogólne strategie bezpieczeństwa narodowego, koordynując działania i konsultując z wymienionymi instytucjami w zakresie strategicznych zagrożeń cyberbezpieczeństwa.

Incydenty bezpieczeństwa

Liczba incydentów bezpieczeństwa

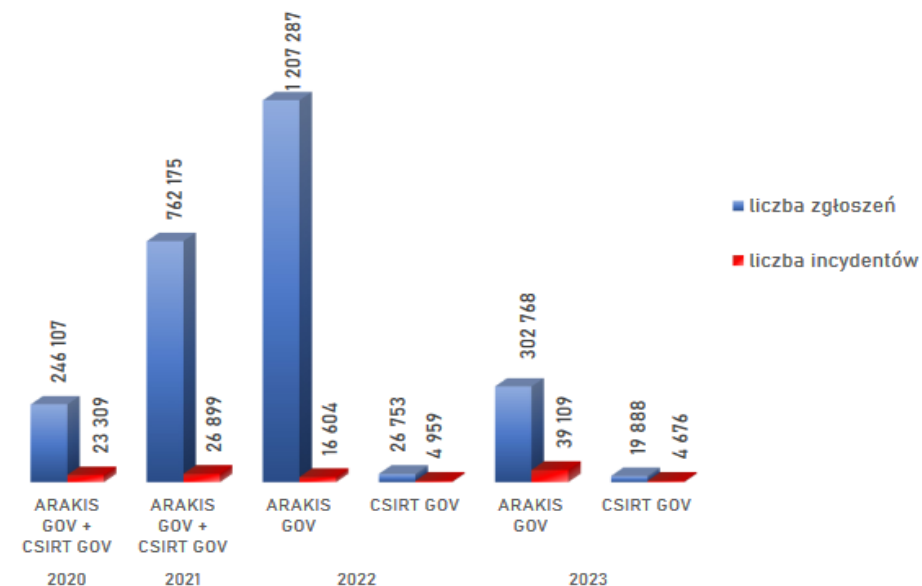


Raport roczny z działalności CERT POLSKA (CSIRT NASK)

https://cert.pl/uploads/docs/Raport_CP_2023.pdf

Liczba incydentów: **80 267** (2023)

~1 incydent na 282 użytkowników w roku



Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 (CSIRT GOV)

</download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf>

Liczba incydentów: **43 785** (2023)

Incydenty bezpieczeństwa

Typy incydentów obsługiwanych przez CERT Polska w 2023 r.

Typy incydentów	Liczba incydentów	Procent wszystkich
Oszustwa komputerowe	75 917	94,58%
Szkodliwe oprogramowanie	1 650	2,06%
Podatne usługi	964	1,20%
Obrażliwe i nielegalne treści	584	0,73%
Włamania	418	0,52%
Dostępność zasobów	385	0,48%
Próby włamań	205	0,26%
Atak na bezpieczeństwo informacji	59	0,07%
Inne	56	0,07%
Gromadzenie informacji	29	0,04%
Razem	80 267	100,00%

Incydenty obsługiwane przez CERT Polska w 2023 r.
w podziale na sektor gospodarki (>1%)

Sektor gospodarki	Liczba incydentów	Procent wszystkich
Handel hurtowy i detaliczny	19 253	23,99%
Infrastruktura rynków finansowych	18 943	23,61%
Media	10 191	12,70%
Energetyka	9 196	11,46%
Poczta i usługi kurierskie	5 319	6,63%
Infrastruktura cyfrowa	5 101	6,35%
Bankowość	2 481	3,09%
Produkcja	2 353	2,93%
Administracja publiczna	2 234	2,78%
Osoby fizyczne	2 105	2,62%
Usługi inne	902	1,12%
.....		
Razem	80 278	100,00%

Raport roczny z działalności CERT POLSKA (CSIRT NASK)

https://cert.pl/uploads/docs/Raport_CP_2023.pdf

Co zagraża informacji.....



Zadanie

Treść

(0-2 pkt)

Opisz cztery konkretne obszary regulowane przez *ustawę o krajowym systemie cyberbezpieczeństwa* i opisz ich wpływ na cyberbezpieczeństwo w Polsce.

Wielkość treści: ~ 1 strona A4

Termin przestania sprawozdania,
wskazany w zadaniu w Moodle.