Krajowy System Cyberbezpieczeństwa a samorząd terytorialny - kompetencje samorządu związane z cyberbezpieczeństwem

Dr inż. Krzysztof Świtała
Wydział Prawa i Administracji
Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

Zakres szkolenia

- Geneza regulacji dotyczącej cyberbezpieczeństwa;
- Systematyka ustawy o Krajowym Systemie Cyberbezpieczeństwa (zakres przedmiotowy i podmiotowy);
- Cyberprzestrzeń i cyberbezpieczeństwo w kontekście zapewniania bezpieczeństwa informacyjnego;
- Jednostka samorządu terytorialnego jako podmiot publiczny zobowiązany do stosowania ustawy o Krajowym Systemie Cyberbezpieczeństwa;
- Obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;
- Obowiązki związane z zarządzaniem incydentem w podmiocie publicznym;
- Dodatkowe informacje przekazywane do CSIRT w związku ze zgłoszeniem incydentu w podmiocie publicznym;
- Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 a jednostki samorządu terytorialnego;
- Obowiązki jednostki samorządu terytorialnego w Krajowym Systemie Cyberbezpieczeństwa w relacji do innych pokrewnych regulacji związanych z zapewnianiem bezpieczeństwa informacyjnego i ochrony danych osobowych.

Cyberprzestrzeń

- Art. 2 ust. 1b ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej stanowi, że przez cyberprzestrzeń rozumie się **przestrzeń przetwarzania** i wymiany **informacji** tworzoną przez **systemy teleinformatyczne**, określone w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z **użytkownikami**.

Zgodnie z art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne system teleinformatyczny to zespół współpracujących ze sobą **urządzeń** informatycznych (ang. hardware) i **oprogramowania** (ang. software) zapewniający **przetwarzanie**, przechowywanie, a także wysyłanie i odbieranie **danych** (ang. content) przez **sieci telekomunikacyjne** za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy - Prawo telekomunikacyjne.

Regulacje prawne odnoszące się do problematyki cyberbezpieczeństwa

- **Cyberbezpieczeństwo** (art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa – UKSC) to odporność **systemów informacyjnych** na działania naruszające **poufność, integralność, dostępność** i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
  - Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa stanowi wdrożenie Dyrektywy 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 (NIS):
    - Podstawowym celem niniejszej dyrektywy jest osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego.
    - Wspomniany akt prawa UE nie odnosi się do obowiązków podmiotów publicznych - w tym jednostek samorządu terytorialnego.

Cyberbezpieczeństwo a bezpieczeństwo informacyjne

- **Cyberbezpieczeństwo** (art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa – UKSC) to odporność **systemów informacyjnych** na działania naruszające **poufność, integralność, dostępność** i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
- **Cyberbezpieczeństwo** oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami (art. 2 pkt 1 rozporządzenia UE z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie))
- **System informacyjny** (art. 2 pkt 14 UKSC) - system teleinformatyczny wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
- **Bezpieczeństwo sieci i systemów informatycznych** (art. 4 pkt 2 dyrektywy NIS) - oznacza odporność sieci i systemów informatycznych, przy danym poziomie **zaufania**, na wszelkie działania naruszające **dostępność,** autentyczność, **integralność lub poufność** przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne;
- **Bezpieczeństwo informacji** (ISO 27000 - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Przegląd i terminologia) – zachowanie **poufności, integralności i dostępności informacji**; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Atrybuty bezpieczeństwa informacji

- **Poufność** (ang. confidentiality) to właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
- **Integralność** (ang. integrity) to właściwość zapewnienia dokładności i kompletności aktywów (zasobów).
- **Dostępność** (ang. availiability) to właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.
- **Autentyczność** (ang. authenticity) to właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; dotyczy użytkowników, procesów, systemów lub nawet instytucji; autentyczność; związana jest z badaniem, czy ktoś lub coś jest tym/czym za kogo/co się podaje.

Europejska Agenda Cyfrowa (COM(2010) 245)

- Jest to inicjatywa przewodnia wyodrębniona w ramach strategii Europa 2020.
- Obszary działań agendy cyfrowej:
  - 2.1.3. Dynamiczny jednolity rynek cyfrowy - budowanie **zaufania** do środowiska cyfrowego;
  - 2.3. **Zaufanie i bezpieczeństwo**
    - Główne działanie 6: Przedstawienie w 2010 r. środków ukierunkowanych na prowadzenie na wysokim szczeblu udoskonalonej **polityki w zakresie bezpieczeństwa sieci i informacji, w tym inicjatyw ustawodawczych**, takich jak np. unowocześnienie Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), a także przedstawienie środków umożliwiających szybsze reagowanie na wypadek ataków cybernetycznych, w tym CERT dla instytucji UE;
    - Główne działanie 7: Przedstawienie do 2010 r. środków, w tym inicjatyw ustawodawczych, ukierunkowanych na zwalczanie ataków cybernetycznych na systemy informatyczne oraz powiązanych przepisów dotyczących jurysdykcji w cyberprzestrzeni na szczeblu europejskim i międzynarodowym (do 2013 r.).

Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń

- Komisja Europejska w dniu 7 lutego 2013 roku opublikowała „Wspólny komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – **Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń**" (JOIN/2013/01).
- Dokument ten jest pierwszym dokumentem strategicznym UE w zakresie cyberbezpieczeństwa.
- W omawianej strategii Komisja zwraca się do Parlamentu Europejskiego i Rady o szybkie przyjęcie wniosku dotyczącego **dyrektywy w sprawie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji** w całej Unii, który reguluje **kwestie krajowych zdolności i krajowej gotowości, współpracy na poziomie UE oraz stosowania praktyk w zakresie przeciwdziałania zagrożeniom i wymiany informacji dotyczących bezpieczeństwa sieci i informacji**.

Systematyka ustawy o Krajowym Systemie Cyberbezpieczeństwa

- Rozdział 1. Przepisy ogólne
- Rozdział 2. Identyfikacja i rejestracja operatorów usług kluczowych
- Rozdział 3. Obowiązki operatorów usług kluczowych
- Rozdział 4. Obowiązki dostawców usług cyfrowych
- **Rozdział 5. Obowiązki podmiotów publicznych**
- Rozdział 6. Zadania CSIRT MON, CSIRT NASK i CSIRT GOV (Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego)
- Rozdział 7. Zasady udostępniania informacji i przetwarzania danych osobowych
- Rozdział 8. Organy właściwe do spraw cyberbezpieczeństwa
- Rozdział 9. Zadania ministra właściwego do spraw informatyzacji
- Rozdział 10. Zadania Ministra Obrony Narodowej
- Rozdział 11. Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa
- Rozdział 12. Pełnomocnik i Kolegium
- Rozdział 13. Strategia
- Rozdział 14. Przepisy o karach pieniężnych
- Rozdział 15. Zmiany w przepisach, przepisy przejściowe, dostosowujące i końcowe
- ZAŁĄCZNIK Nr 1. Sektory i podsektory oraz rodzaje podmiotów
- ZAŁĄCZNIK Nr 1. Usługi cyfrowe
  - Internetowa platforma handlowa
  - Usługa przetwarzania w chmurze
  - Wyszukiwarka internetowa

Podmioty publiczne (jednostki samorządu terytorialnego) w Krajowym Systemie Cyberbezpieczeństwa

- Na podstawie art. 4 pkt 7 UKSC w związku z art. 9 pkt 2 ustawy o finansach publicznych do podmiotów objętych Krajowym Systemem Cyberbezpieczeństwa należą jednostki samorządu terytorialnego oraz ich związki.

Obowiązki podmiotów publicznych (jednostek samorządu terytorialnego) w Krajowym Systemie Cyberbezpieczeństwa

- wyznaczenie **osoby odpowiedzialnej za utrzymywanie kontaktów** z podmiotami **Krajowego Systemu Cyberbezpieczeństwa**;
- **zgłaszanie** i obsługa **incydentu** (zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo);
- **informowanie** właściwego **CSIRT** (Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego).

Incydent w podmiocie publicznym i jego obsługa

- **incydent w podmiocie publicznym -** incydent, który powoduje lub może spowodować **obniżenie jakości lub przerwanie realizacji zadania publicznego** realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7-15 (art. 2 pkt 9 UKSC);
- **obsługa incydentu -** czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu (art. 2 pkt 10 UKSC).
- **zarządzanie incydentem -** obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu (art. 2 pkt 18 UKSC);

Obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa

Art. 21 ust. 1 UKSC:

- 1. Podmiot publiczny, o którym mowa w art. 4 pkt 7-15, realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do **wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa**.
- 3. **Jednostka samorządu terytorialnego może wyznaczyć jedną osobę** odpowiedzialną za utrzymywanie **kontaktów** z podmiotami krajowego systemu cyberbezpieczeństwa **w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne**.
- Aktualnie informację o wyznaczeniu takiej osoby przekazujemy przez formularz https://incydent.cert.pl/osoba-kontaktowa, na adres emailowy ksc@cert.pl lub w formie tradycyjnego pisma.

W odniesieniu do jednostki samorządu terytorialnego na podstawie art. 22 ust. 1 pkt 5 UKSC dane tej osoby (imię i nazwisko, numer telefonu oraz adres poczty elektronicznej) przekazujemy w terminie **14 dni od dnia jej wyznaczenia CSIRT NASK**.

Obowiązki w zakresie zarządzania incydentem w podmiocie publicznym (art. 22 ust. 1 UKSC)

- zapewnia **zarządzanie incydentem** w podmiocie publicznym;
- **zgłasza incydent** w podmiocie publicznym niezwłocznie, **nie później niż w ciągu 24 godzin** od momentu **wykrycia**, do właściwego CSIRT MON, **CSIRT NASK** lub CSIRT GOV;
- **zapewnia obsługę incydentu** w podmiocie publicznym i incydentu krytycznego **we współpracy z właściwym CSIRT** (MON/**NASK**/GOV), przekazując niezbędne dane, w tym dane osobowe;
- zapewnia **osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy** pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;
- **przekazuje** do właściwego CSIRT (MON/**NASK**/GOV) dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, **w terminie 14 dni od dnia jej wyznaczenia**, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

Zgodnie z art. 26 ust. 6 pkt 1 lit. a UKSC do zadań CSIRT NASK należy koordynacja obsługi incydentów zgłaszanych przez jednostki samorządu terytorialnego

Treść zgłoszenia incydentu w podmiocie publicznym (art. 23 UKSC)

- **dane podmiotu zgłaszającego**, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres;
- imię i nazwisko, numer telefonu oraz adres poczty elektronicznej **osoby składającej zgłoszenie;**
- imię i nazwisko, numer telefonu oraz adres poczty elektronicznej **osoby uprawnionej do składania wyjaśnień** dotyczących zgłaszanych informacji;
- **opis wpływu incydentu** w podmiocie publicznym na realizowane zadanie publiczne (wskazanie tego zadania publicznego; liczby osób, na które incydent miał wpływ; momentu wystąpienia i wykrycia incydentu oraz czas jego trwania; zasięgu geograficznego obszaru, którego dotyczy incydent; przyczyny zaistnienia incydentu i sposobu jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego);
- informacje **o przyczynie i źródle incydentu;**
- informacje o **podjętych działaniach zapobiegawczych;**
- informacje o **podjętych działaniach naprawczych;**
- inne istotne informacje.

Zgłoszenie przekazywane jest w postaci elektronicznej, poprzez uzupełnienie formularza internetowego znajdującego się na stronie: https://**incydent.cert.pl** lub wysłanie wiadomości email na adres: cert@cert.pl.

Dodatkowe informacje przekazywane w związku ze zgłoszeniem incydentu w podmiocie publicznym (art. 23 ust. 2-5 UKSC)

- Podmiot publiczny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które **uzupełnia w trakcie obsługi incydentu** w podmiocie publicznym.
- Podmiot publiczny **przekazuje, w niezbędnym zakresie**, w zgłoszeniu, o którym mowa w art. 22 ust. 1 pkt 2, **informacje stanowiące tajemnice prawnie chronione**, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT (MON/NASK/GOV).
- Właściwy CSIRT (MON/NASK/GOV) **może zwrócić się do podmiotu publicznego o uzupełnienie zgłoszenia** o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.
- W zgłoszeniu podmiot publiczny **oznacza informacje stanowiące tajemnice prawnie chronione**, w tym stanowiące tajemnicę przedsiębiorstwa.

Fakultatywna możliwość przekazywania informacji do właściwego CSIRT (art. 24 UKSC)

- Podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego **może przekazywać** do właściwego CSIRT (MON/NASK/GOV) informacje, o których mowa w art. 13 ust. 1.
- Informacje te **przekazywane są w postaci elektronicznej**, a w przypadku braku możliwości przekazania ich w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

Zakres informacji przekazywanych fakultatywnie do właściwego CSIRT (art. 13 UKSC)

- Operator usługi kluczowej (przepis ten stosuje się odpowiednio do JST) może przekazywać do właściwego CSIRT (MON/NASK/GOV) informacje:
  - o innych **incydentach**;
  - o **zagrożeniach** cyberbezpieczeństwa;
  - dotyczące szacowania **ryzyka** (zgodnie z art. 2 pkt 13 UKSC jest to kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji);
  - o **podatnościach** (zgodnie z art. 2 pkt 13 UKSC to właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa);
  - o wykorzystywanych **technologiach**.

Obowiązek zapewnienia rozwoju lub utrzymania systemu teleinformatycznego wspierającego współpracę w ramach krajowego systemu cyberbezpieczeństwa (art. 46 ust. 1 UKSC)

- Minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:
  1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
  2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
  3) **zgłaszanie i obsługę incydentów**;
  4) szacowanie ryzyka na poziomie krajowym;
  5) ostrzeganie o zagrożeniach cyberbezpieczeństwa.

Zgodnie z art. 89 UKSC minister właściwy do spraw informatyzacji był zobligowany do uruchomienia systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy, do **1 stycznia 2021 r.**

Przepisy stosowane do podmiotu publicznego uznanego za operatora usługi kluczowej

- **Art. 25 UKSC.** Do podmiotu publicznego, o którym mowa w art. 4 pkt 7-15, wobec którego wydana została decyzja o uznaniu za operatora usługi kluczowej, stosuje się przepisy rozdziału 3 w zakresie świadczenia usługi kluczowej, w związku z której świadczeniem został uznany za operatora usługi kluczowej.

Obowiązki operatora usługi kluczowej

- Obowiązek wdrożenia **systemu zarządzania bezpieczeństwem w systemie informacyjnym** wykorzystywanym do świadczenia usługi kluczowej (art. 8);
- Dodatkowe **obowiązki organizacyjne** operatora usługi kluczowej (art. 9 UKSC):
  - obowiązek wyznaczenia **osoby odpowiedzialnej za utrzymywanie kontaktów** z podmiotami krajowego systemu cyberbezpieczeństwa;
  - obowiązek zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy w zakresie zagrożeń cyberbezpieczeństwa;
- Obowiązek opracowania, wdrożenia i aktualizacji **dokumentacji cyberbezpieczeństwa** systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (art. 10 UKSC);
- Obowiązek **obsługi incydentów** przez operatora usługi kluczowej (art. 11 UKSC);
- Powołanie **wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo** (art. 14 UKSC);
- **Audyt bezpieczeństwa systemu informacyjnego** wykorzystywanego do świadczenia usługi kluczowej (art. 15 ust. 1 UKSC).

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024

- Załącznik do uchwały nr 125 Rady Ministrów z dnia 22 października 2019 r. wydanej na podstawie art. 68 UKSC.
- Strategia określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa (art. 69 ust. 1 UKSC).
- Obowiązek przyjęcia takiej krajowej strategii w zakresie cyberbezpieczeństwa wynika z art. 7 ust. 1 dyrektywy NIS.
- Cel szczegółowy 1 – rozwój krajowego systemu cyberbezpieczeństwa
  - Działanie 1.2. **Podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa** - rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz **jednostek samorządu terytorialnego** w zakresie **podnoszenia kompetencji** w projektowaniu procesów zwiększających cyberbezpieczeństwo, w szczególności: w doborze, wdrażaniu i utrzymaniu środków technicznych zwiększających cyberbezpieczeństwo, w tym korzystania z nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych, tworzenia bezpiecznych aplikacji oraz korzystania z bezpiecznych systemów mobilnych.
- Cel szczegółowy 4 – Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa
  - Działanie 4.1. **Zwiększanie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa Rzeczypospolitej Polskiej** - równocześnie rząd przygotuje i wdroży systemowe rozwiązanie w celu zapewnienia **merytorycznego wsparcia dla podniesienia kompetencji pracowników jednostek administracji samorządowej** w zakresie cyberbezpieczeństwa.

System Zarządzania Bezpieczeństwem Informacji w Krajowych Ramach Interoperacyjności

- **§ 20 ROZPORZĄDZENIA** RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie **Krajowych Ram Interoperacyjności**, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
- Podmiot realizujący zadania publiczne opracowuje i **ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji** zapewniający **poufność, dostępność i integralność** informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
- Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań wymienionych w ust. 2.
- Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych **analizą ryzyka** w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

Wspólne cechy rozwiązań prawnych chroniących Krajowy System Cyberbezpieczeństwa (UKSC) i czynności przetwarzania danych osobowych (RODO)

- Podejście oparte na **ryzyku**;
- Prowadzenie **dokumentacji** przetwarzania zasobów informacyjnych (w tym danych osobowych);
- Zgłaszanie i **zarządzanie incydentami**/naruszeniami;
- **Struktura organizacyjna** odpowiedzialna za zarządzanie bezpieczeństwem zasobów informacyjnych (w tym osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa/inspektora ochrony danych);
- Proaktywne podejście do zarządzania bezpieczeństwem zasobów informacyjnych (uwzględnianie **ochrony danych w fazie projektowania**, ciągłe doskonalenie).

Podsumowanie

- Problematyka zapewniania **cyberbezpieczeństwa stanowi istotny aspekt funkcjonowania podmiotów publicznych**, w tym jednostek samorządu terytorialnego.
- Cyberbezpieczeństwo **nie odnosi się tylko do zapewnienia poufności danych** przetwarzanych w systemach teleinformatycznych, ale zakres oddziaływania tej problematyki jest znacznie szerszy.
- **Zagrożenia** związane z cyberbezpieczeństwem mogą oddziaływać również na **osoby, które nie korzystają z systemów teleinformatycznych**.
- Aby zwiększyć skuteczność działań związanych z zapewnianiem cyberbezpieczeństwa warto stosować **normy techniczne** dotyczące bezpieczeństwa informacyjnego (przede wszystkim z rodziny standardów ISO 27000) i **wytyczne formułowane przez ENISA**
  (Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji).