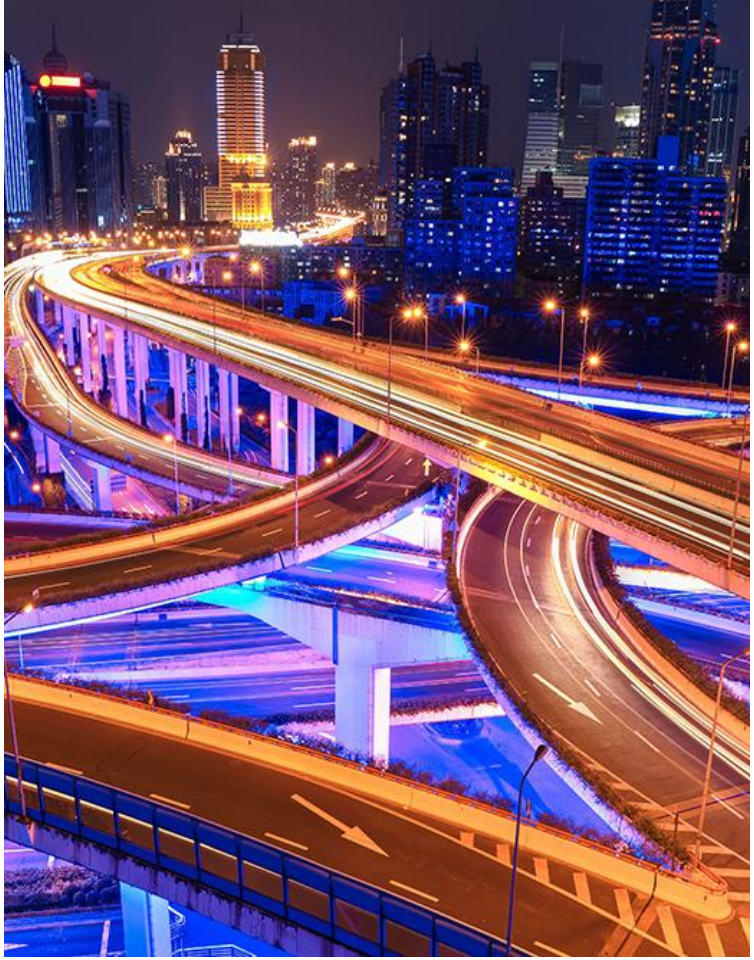


Ochrona IK i usługi kluczowej – teoretyczne i praktyczne aspekty budowy modelu zarządzania bezpieczeństwem na przykładzie TAURON Dystrybucja S.A.

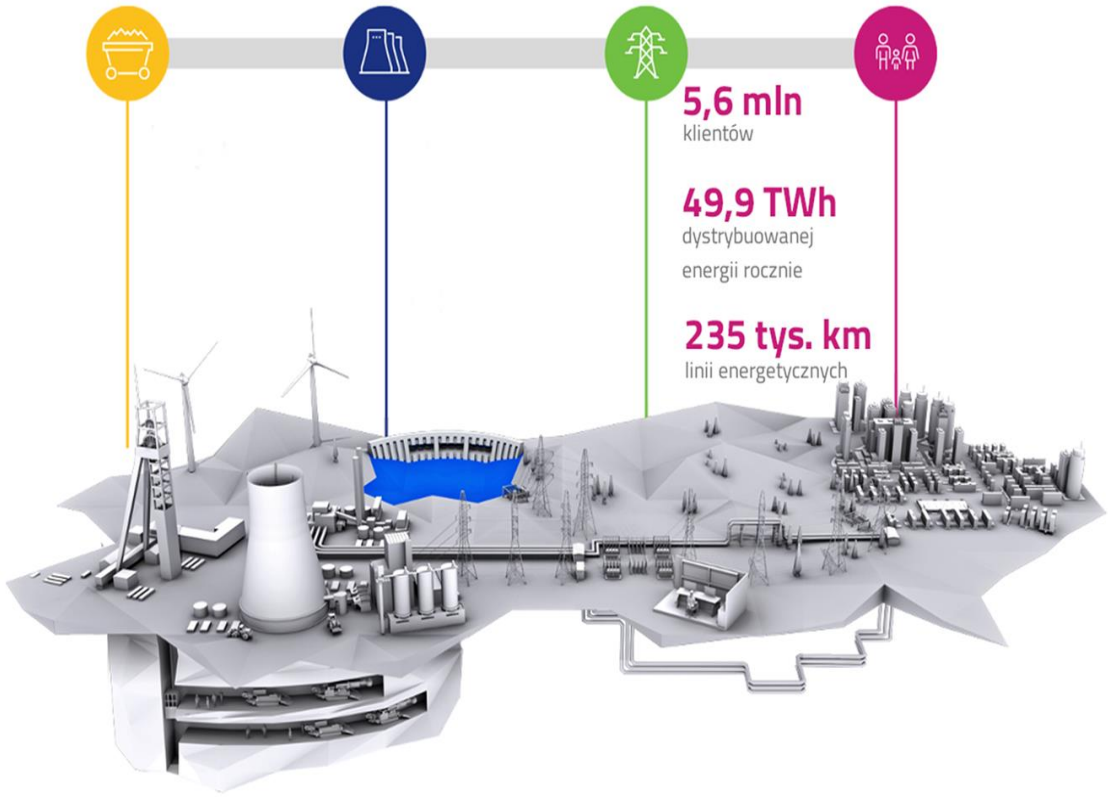
Warszawa, 5 czerwca 2019 r.

Jakub Czudiak / Przemysław Kwiecień

TAURON Dystrybucja – podstawowe informacje

TAURON Dystrybucja to kluczowa spółka z Grupy TAURON, która odpowiada za rozwój, eksploatację i utrzymanie sieci elektroenergetycznych na terenie południowej Polski.

Na mocy decyzji Prezesa Urzędu Regulacji Energetyki TAURON Dystrybucja pełni funkcję Operatora Systemu Dystrybucyjnego Elektroenergetycznego i posiada koncesję na przesyłanie i dystrybucję energii elektrycznej do dnia 31 grudnia 2025 r.



TAURON Dystrybucja – podstawowe informacje

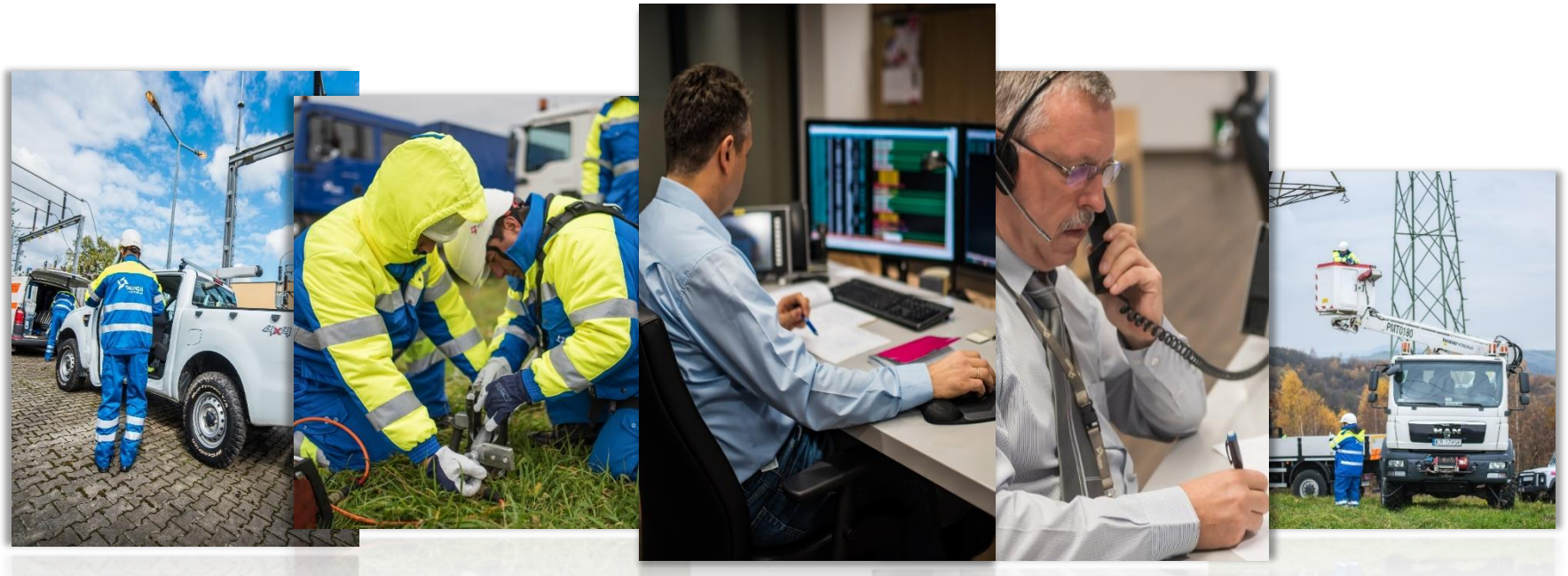
TAURON Dystrybucja jest największym dystrybutorem energii w Polsce i głównym dostawcą energii elektrycznej na terenie województw: małopolskiego, dolnośląskiego, opolskiego, śląskiego, częściowo: świętokrzyskiego, podkarpackiego, łódzkiego, wielkopolskiego oraz lubuskiego.

Dystrybuuje prawie 50 TWh energii elektrycznej rocznie na obszarze 57 940 km2, co stanowi 18,5% powierzchni Polski.

TAURON Dystrybucja – podstawowe informacje

Spółka wykorzystuje nowoczesne rozwiązania technologiczne i posiada potencjał gwarantujący klientom bezpieczeństwo zasilania i wysoki standard świadczonych usług. Dla zapewnienia realizacji celów strategicznych aktywnie poszukuje rozwiązań innowacyjnych.

Uczestniczy w pracach badawczo-rozwojowych oraz wdraża nowe technologie, ze szczególnym uwzględnieniem technologii smart grid.



TAURON Dystrybucja – operator IK oraz operator usługi kluczowej

Infrastruktura krytyczna (IK) to rzeczywiste i cybernetyczne systemy (obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa.

Zgodnie z zapisami ustawy o zarządzaniu kryzysowym IK to **systemy** oraz wchodzące w ich skład powiązane ze sobą **funkcjonalnie obiekty**, w tym obiekty budowlane, urządzenia, instalacje, **usługi kluczowe dla bezpieczeństwa państwa i jego obywateli** oraz służące zapewnieniu sprawnego funkcjonowania **administracji publicznej**, a także **instytucji i przedsiębiorców**.

TAURON Dystrybucja – operator IK oraz operator usługi kluczowej

W roku 2018 TAURON Dystrybucja została **uznana za operatora IK**, a wytypowane **obiekty zostały ujęte w** *Jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy* – dokumencie, w którym skatalogowane są obiekty i instalacje IK.

Decyzje o ujęciu danego obiektu w wykazie IK podejmuje się po przeprowadzeniu **analizy na podstawie szczegółowych kryteriów** zapisanych w niejawnym załączniku do Narodowego Programu Ochrony Infrastruktury Krytycznej.

Uznanie za operatora oraz ujęcie w wykazie nakłada na TD określone prawem obowiązki i skutkuje koniecznością podjęcia szeregu działań związanych z **zarządzaniem bezpieczeństwem**.

TAURON Dystrybucja – operator IK oraz operator usługi kluczowej

Ochrona infrastruktury krytycznej to wszelkie działania zmierzające do zapewnienia **funkcjonalności, ciągłości** działań i **integralności** infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz **ograniczenia i neutralizacji** ich skutków oraz **szybkiego odtworzenia** tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony, w szczególności przez **przygotowanie i wdrażanie**, stosownie do przewidywanych zagrożeń, **planów ochrony infrastruktury krytycznej** oraz **utrzymywanie własnych systemów rezerwowych** zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia.

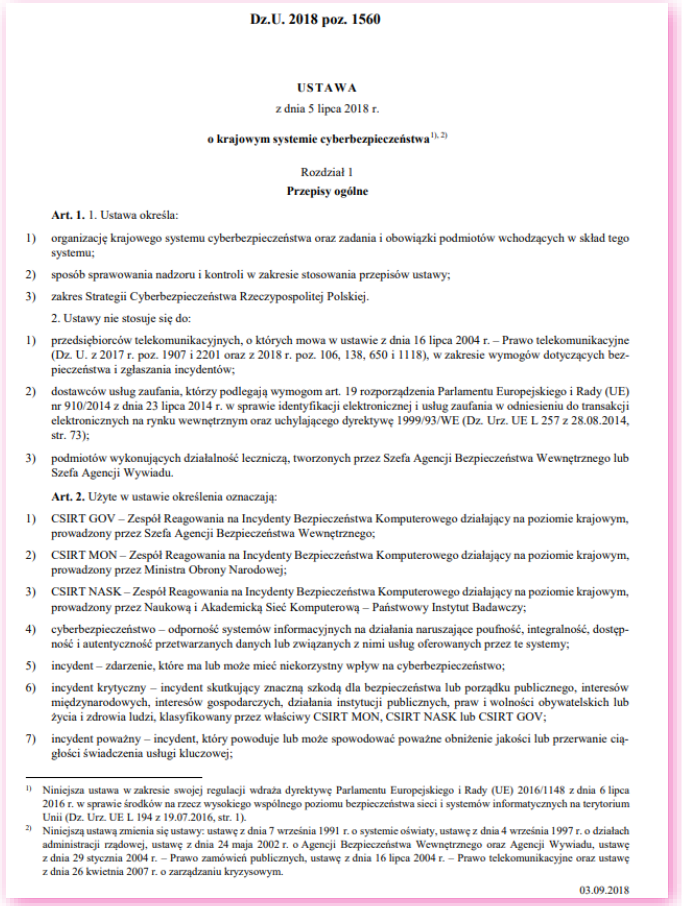
.

TAURON Dystrybucja – operator IK oraz operator usługi kluczowej

Na bazie unijnej regulacji - Dyrektywy NIS (Network and Information Systems Directive) powstaje w **Polsce krajowy system cyberbezpieczeństwa**,

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC) tworzy obszar regulacyjny. Podmiotami systemu są m.in. administracja rządowa i samorządowa, a także **operatorzy usług kluczowych** i cyfrowych.

Są to czyli najwięksi przedsiębiorcy z wybranych sektorów gospodarki, takich jak: **energetyka**, transport, sektor bankowy i finansowy, zdrowie, zaopatrzenie w wodę i infrastruktura cyfrowa. Ustawa zobowiązuje te podmioty do **zapewnienia odpowiedniego poziomu cyberbezpieczeństwa** oraz raportowania incydentów.



Dz.U. 2018 poz. 1560

USTAWA

z dnia 5 lipca 2018 r.

o krajowym systemie cyberbezpieczeństwa[1), 2)]

Rozdział 1

Przepisy ogólne

Art. 1. 1. Ustawa określa:

1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;

2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;

3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

2. Ustawy nie stosuje się do:

1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138, 650 i 1118), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;

2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73);

3) podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

Art. 2. Użyte w ustawie określenia oznaczają:

1) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;

2) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;

3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;

4) cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;

6) incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;

7) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;

[1)] Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę 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 (Dz. Urz. UE L 194 z 19.07.2016, str. 1).

[2)] Niniejszą ustawą zmienia się ustawy: ustawę z dnia 7 września 1991 r. o systemie oświaty, ustawę z dnia 4 września 1997 r. o działach administracji rządowej, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne oraz ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

03.09.2018

TAURON Dystrybucja – operator IK oraz operator usługi kluczowej

TAURON Dystrybucja jest przedsiębiorstwem energetycznym posiadającym koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji energii elektrycznej.

TAURON Dystrybucja **świadczy usługę kluczową** - dystrybucja energii elektrycznej oraz osiąga progi istotności skutku zakłócającego incydentu określone dla świadczenia usługi kluczowej.

Świadczenie usługi kluczowej *dystrybucja energii elektrycznej*, świadczonej przez TAURON Dystrybucja zależy od systemu informatycznego.

W kwietniu 2019 r. decyzją Ministra Energii, TAURON Dystrybucja **uznany został za operatora usługi kluczowej.**

TAURON Dystrybucja – operator IK oraz operator usługi kluczowej

Ustawa o krajowym systemie cyberbezpieczeństwa nakłada na podmioty będące operatorami usług kluczowych **szereg obowiązków** i określa ścisłe terminy ich realizacji.

Podmiot którzy dotychczas realizował politykę cyberbezpieczeństwa według własnego uznania i własnej oceny ryzyka, będzie zobowiązany do stworzenia **struktury do zarządzania cyberbezpieczeństwem** oraz na podstawie procesu **szacowania ryzyka** będzie musiał wdrożyć lub **dostosować środki bezpieczeństwa** oraz udokumentować wszystkie prowadzone działania.

Właściwym podejściem jest **stworzenie całego systemu**, który zapewnia ciągłą identyfikację zagrożeń poprzez zapewnienie środków organizacyjnych i technicznych do wykrywania cyberataków na poziomie infrastruktury sieciowej oraz aplikacji będących elementami systemu informacyjnego służącego do świadczenia usługi kluczowej.

TAURON Dystrybucja – operator IK oraz operator usługi kluczowej – budowa modelu bezpieczeństwa

Utworzenie **Departamentu Bezpieczeństwa i Zgodności**, w ramach którego realizowane są dwa główne obszary zadaniowe:

Bezpieczeństwo **Informacji:**

- ✓ Ochrona Danych Osobowych (w zakresie zadań KODO)
- ✓ Ochrona Informacji Niejawnych
- ✓ Zarządzanie Bezpieczeństwem Informacji
- ✓ Zarządzanie Sprawami Obronnymi

Bezpieczeństwo **Systemów** IT/OT i **Infrastruktury** Obiektowej:

- ✓ Zarządzanie Bezpieczeństwem Systemów IT/OT
- ✓ Zarządzanie Bezpieczeństwem Infrastruktury Krytycznej
- ✓ Zarządzanie Zabezpieczeniami Technicznymi

TAURON Dystrybucja – operator IK oraz operator usługi kluczowej – budowa modelu bezpieczeństwa

Celem podejmowanych działań jest stworzenie **skutecznego, sprawnego** i **stabilnego** systemu zarządzania bezpieczeństwem.

Priorytety zadaniowe:

- Opracowanie i wdrożenie Planu Ochrony Infrastruktury Krytycznej.
- Zbudowanie i wdrożenie całościowej strategii bezpieczeństwa systemów technologicznych oraz wspierających systemów informatycznych, w tym wdrożenie wymagań wynikających z roli operatora usługi kluczowej w rozumieniu Ustawy o krajowym systemie cyberbezpieczeństwa.
- Wydanie i wdrożenie wytycznych w sprawie realizacji przedsięwzięć w ramach poszczególnych stopni alarmowych i stopni alarmowych CRP.
- Standaryzacja Systemów Ochrony Technicznej.

TAURON Dystrybucja – operator IK oraz operator usługi kluczowej – budowa modelu bezpieczeństwa

Realizowane działania:

- Inwentaryzowanie i kwalifikacja systemów technologicznych;
- Przegląd zinwentaryzowanych systemów informacyjnych i wykonanie analizy ryzyka;
- Wdrażanie narzędzi i zarządzanie incydentami bezpieczeństwa;
- Implementowanie zaleceń, wytycznych i dyspozycji przekazywanych przez właściwe organy i służby;
- Przygotowywanie i udział w warsztatach i szkoleniach; organizowanie, prowadzenie i udział w szkoleniach i warsztatach;
- Rozbudowywanie współpracy z administracją publiczną i instytucjami.

TAURON Dystrybucja – operator IK oraz operator usługi kluczowej – budowa modelu bezpieczeństwa

Skuteczna ochrona IK i usług kluczowych musi być oparta na **współpracy** oraz **budowaniu partnerstwa** pomiędzy operatorami, administracją publiczną i instytucjami naukowymi.

Proces **rozwoju** infrastruktury krytycznej jest ściśle powiązany z tworzeniem sprawnego mechanizmu systemu bezpieczeństwa - jest to **wyzwanie** i wspólny **obowiązek**.

Dziękuję za uwagę