PROTOKÓŁ nr 7 / 2022-26
z posiedzenia SITK RP Krajowej Sekcji Kolejowej z dnia 10.03.2026 r.

Posiedzenie Krajowej Sekcji Kolejowej SITK RP odbyło się w dniu 10 marca 2026 r. lokalizacyjnie na zaproszenie Kierownictwa Instytutu Kolejnictwa

LOKALIZACJA: Instytut Kolejnictwa ul. Chłopickiego 50, 04-275 Warszawa

Obecni wg listy obecności – 35 osób KSK z oraz osoby z IK.

PORZĄDEK OBRAD

posiedzenia Krajowej Sekcji Kolejowej SITK RP w dniu 10 marca 2026 r.

Lp.	Temat	Prowadzący	Uwagi
1.	Przywitanie uczestników oraz rozpoczęcie obrad.	J. Paś M. Kaczorek I. Jasiński	
2.	Przyjęcie porządku obrad.	I. Jasiński	
3.	Dyskusja i przyjęcie Protokołu z poprzedniego posiedzenia w dniu 11 grudnia 2025 r.	I. Jasiński	
4.	Budowanie kompetencji pracowników podmiotów kolejowych w zakresie cyberbezpieczeństwa.	M. Pawlik	Prezentacja tematu
5.	Wycieczka techniczna po Instytucie Kolejnictwa	M. Pawlik	
6.	Dyskusja, wolne wnioski, sugestie.	M. Kaczorek I. Jasiński	Uczestnicy
7.	Zakończenie posiedzenia	M. Kaczorek I. Jasiński	

Realizacja porządku obrad przedstawiała się następująco:

Ad. 1. i 2. Spotkanie otworzył i przywitał uczestników Kol. dr inż. Jacek Paś oraz Sekretarz SITK RP Krajowej Sekcji Kolejowe kol. Ireneusz Jasiński również w imieniu Przewodniczącego dr inż. Macieja Kaczorek (który z uwagi na zajęcia służbowe nie mógł uczestniczyć osobiście). Następnie Sekretarz przedstawił proponowany porządek obrad. Został on przyjęty przez aklamację.

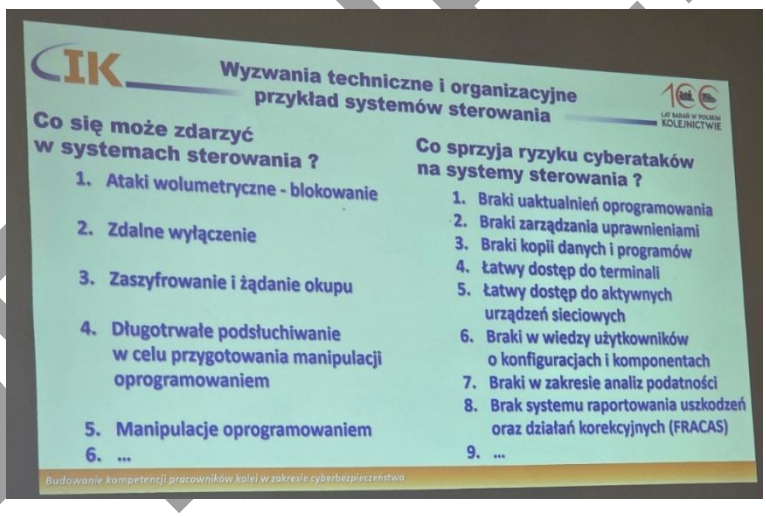
Ad. 3. Przez aklamację został przyjęty Protokołu z poprzedniego posiedzenia w dniu 11 grudnia 2025 r.

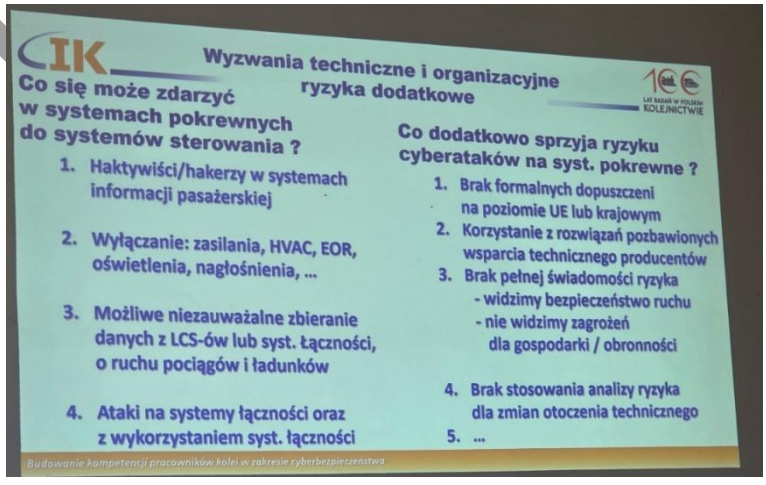
Ad. 4 i 6. Punkty te poprowadził, zgodnie z porządkiem obrad, Kolega dr hab. inż. Marek Pawlik, prof. IK, Z-ca Dyrektora ds. Interoperacyjności Kolei i jednocześnie członek Zarządu KSK.

Z prezentacji (w załączeniu) uczestnicy dowiedzieli się o cyberprzestrzeni, wktórej funkcjonują dwa rodzaje rozwiązań technicznych, tj.: systemy IT (informatyczne) oraz systemy OT (eksploatacyjne). Przedstawione zostały zasady tworzenia rozwiązań cyfrowych i wymiany danych w cyberprzestrzeni. Na tej bazie pokazane zostały cyfrowe zagrożenia i metody zapewnienia cyberbezpieczeństwa. Dotyczy to zarówno nas, osób fizycznych, jak i organizacji, firm.

Form, sposobów ataków jest, można by „powiedzieć – bez liku". Przykładowo są to ataki realizowane przez boty (złośliwe programy służące do realizacji fal ataków, których celem jest znalezienie słabego miejsca przez szybkie poszukiwanie na oślep), ransomware (szyfrowanie lub kradzież danych z żądanie okupu) czy phishig (przestępca podszywa się pod zaufaną osobę lub instytucję, aby wyłudzić poufne informacje lub nakłonić ofiarę do określonych działań) lub quishing (oszustwo z wykorzystaniem kodów QR) itd.

Ryzyka w cyberprzestrzeni kolejowej to jedne z bardziej niebezpiecznych z uwagi na charakter działalności, gdzie zdrowie i życie ludzi może być realnie zagrożone. W zapewnianiu cyberbezpieczeństwa szczególną rolę odgrywają odpowiednie służby, ale w zakresie transportu szynowego przepisy nakładają związane z tym obowiązki także na przewoźników kolejowych, zarządców infrastruktury i przemysł dostarczający cyfrowe rozwiązania techniczne transportu, aby wszystkie systemy i oprogramowanie były wolne od znanych podatności w momencie wprowadzania ich do eksploatacji oraz pozostawały zabezpieczone dzięki śledzeniu baz podatności i poprawkom bezpieczeństwa.
Jest to bardzo ważne m.in. w przypadku systemów sterowania ruchem (srk), ale nie tylko.





Ustawa o Krajowym Systemie Cyberbezpieczeństwa Dz. U. z 2026 r. poz. 20, zmieniona w roku bieżącym (Dz. U. z 2026 r. poz. 252), definiuje liczne obowiązki podmiotów kluczowych, a więc między innymi przewoźników i zarządców kolejowych.
Obowiązki te postrzegać należy w kontekście celu wprowadzenia krajowego systemu cyberbezpieczeństwa, który ustawowo zdefiniowany został następująco
„Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług przez podmioty kluczowe lub podmioty ważne*, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów."*

Instytut Kolejnictwa dla potrzeb wsparcia kolejowych podmiotów kluczowych w zakresie bezpieczeństwa cyfrowego od 2020 roku prowadzi Centrum Wymiany i Analizy Informacji podsektora transportu kolejowego „ISAC – Kolej", które przekazuje przewoźnikom i zarządcom kolejowym bieżące informacje o zagrożeniach z cyberprzestrzeni dla systemów IT i systemów OT wykorzystywanych przez podmioty kolejowe.
Prowadzi też działania w zakresie budowania kompetencji i wiedzy pracowników kolejowych między innymi w formule Cyfrowego Laboratorium Kolejowego CLK wykorzystującego:
- środowisko cyfrowe, w którym uczestnicy sami realizują zadania wcześniej omawiane przez prowadzących, oraz
- ekspertów własnych Instytutu Kolejnictwa i udostępnianych przez Centrum Technologii Bezpieczeństwa Akademii Górniczo-Hutniczej w Krakowie.

Dyskusja ujawniła potrzebę szerokiego edukowania w obszarach cyberbepieczeństwa. Wśród powszechnie znanych, a właściwie nagłaśnianych medialnie zagrożeń, to jak przypomniał kol. Karol Trzoński – dane można stracić nawet podłączając telefon do ładowarki w środkach transportu publicznego. W dyskusji głos zabierali również kol. dr inż. Stanisław Zimnoch, kol. dr hab. inż. Andrzej Toruń prof. IK czy kol. Radosław Zawierucha.

Zgodnie z pkt. 5 po krótkim szkoleniu BHP i podziale na grupy uczestnicy udali się na wycieczkę techniczną po niektórych laboratoriach działających w ramach Instytutu Kolejnictwa.
W grupach uczestnicy zapoznali się z Laboratorium Badań Materiałów i Elementów Konstrukcji. Cykle badań wytrzymałościowych, metalograficznych czy ognioodporności oraz innych dają odpowiedź o możliwości stosowania lub nie danych materiałów, podzespołów czy zespołów w transporcie kolejowym.
Jedna grupa odwiedziła Laboratorium Automatyki i Telekomunikacji gdzie pokazane zostały między innymi komora klimatyczna, komora bezodbiciowa oraz wyposażenie pomiarowe do badań radiowych, elektrycznych czy badań z zakresu zakłóceń elektromagnetycznych.

Zakres działalności Instytutu Kolejnictwa w trzecim laboratorium przedstawiony został w postaci prelekcja prowadzonej przez Pana Andrzeja Zbiecia. Prezentacja ta dotyczyła prac prowadzonych prac w Laboratorium Badań Taboru. Chętnych kierujemy do https://www.youtube.com/watch?v=roNr2WE3n4g, gdzie można zapoznać się z filmem o działaniach IK.
Wysoki poziom profesjonalizmu i wiarygodności wyników zapewniane są dzięki akredytacji wielu procedur badawczych, co oznacza formalne uznanie, że laboratoria posiadają odpowiednie kompetencje techniczne i organizacyjne oraz stanowiska badawcze czy urządzenia pomiarowe do prowadzania wymaganych działań.
W uzupełnieniu badań Instytut Kolejnictwa prowadzi także weryfikacje procesów zarządzania jakością, procesy oceny zgodności, weryfikacji podsystemów, czy ocen bezpieczeństwa dla zmian technicznych i eksploatacyjnych.
Podczas wizyt technicznych w laboratoriach, z uwagi na potrzebę zachowania dyskrecji, niektóre stanowiska lub badane produkty były zasłonięte.

Zgodnie z pkt. 7, na zakończenie Krajowej Sekcji Kolejowej, Sekretarz – kol. Ireneusz Jasiński podziękował Gospodarzom za zaproszenie i przedstawiony program merytoryczny a członkom Sekcji za aktywność w tej kadencji, która dobiega końca. Podziękowania imienne złożył kol. Żanecie i Adamowi Bąkowskim za udostępniany Biuletyn ich autorstwa.
Przekazał otrzymana ustną informację o przyjęciu przez Zarząd Krajowy Medalu im. prof. dr inż. Antoniego Rosikoń.

Na tym zebranie zakończono.

Protokółował:
Sekretarz SITK RP KSK

Ireneusz JASIŃSKI

Przewodniczący SITK RP KSK

Maciej KACZOREK

Załączniki:
Biuletyn ŻiA.B,
Prezentacja dr hab. inż. Marek Pawlik, prof. IK