PLAN DZIAŁANIA
KT182
ds. Ochrony Informacji w Systemach Teleinformatycznych

STRESZCZENIE

W obszarze działania KT znajdują się zagadnienia systemowe i strategiczne rozwoju zabezpieczeń systemów informatycznych, a w szczególności: architektura i zarządzanie zabezpieczeniem systemów, metodologia projektowania zabezpieczeń, wytyczne dla usług zabezpieczeń, obszary i elementy zastosowań zabezpieczeń; techniki i mechanizmy zabezpieczenia systemów, techniki kryptograficzne i niekryptograficzne, mechanizmy (uwierzytelniania, kontroli dostępu, poufności danych, integralności); kryteria oceny zabezpieczeń systemów, wytyczne rozwoju i certyfikacji zabezpieczeń systemów (w tym również dla systemów rozproszonych i sieci komputerowych), metodologia i procedury administracyjne zapewnienia funkcjonalności zabezpieczeń, współpraca w zakresie sterowania jakością i testowania, mechanizmy zarządzania tożsamością, zapewnienie prywatności oraz bezpieczeństwo i testowanie technik biometrycznych.

Zagadnienia związane z opisem i przetwarzaniem dokumentów elektronicznych, w tym architektura i formaty przetwarzania, formaty prezentacji, interfejsy aplikacyjne, architektura zawartości i notacje, mechanizmy podpisu cyfrowego i szyfrowania dokumentów elektronicznych.

Zagadnienia związane ze standaryzacją interoperacyjności rozpowszechnianych platform aplikacyjnych w dziedzinie usług sieciowych (ang. web.services), architektury opartej na usługach (ang.Service-Oriented Architecture, SOA) przetwarzania w chmurze (ang.Cloud computing).

1 ŚRODOWISKO BIZNESOWE KT

1.1 Opis środowiska biznesowego

Na działalność gospodarczą objętą zakresem KT znaczący wpływ mają następujące uwarunkowania polityczne, gospodarcze, techniczne, prawne, społeczne i/lub aspekty regionalne/międzynarodowe:

Uwarunkowania techniczne

KT 182 działa w trzech głównych obszarach normalizacji międzynarodowej, będą komitetem lustrzanym dla następujących komitetów ISO/IEC JTC1:

- SC27 „IT Security Techniques"
- SC34 Document Description and Processing Languages
- SC38 Distributed Application Platforms and Services (DAPS)
- CEN/CENELEC JTC 13 Cybersecurity and Data Protection

W we wszystkich powyższych komitetach Polska ma status członka czynnego „P".

W obszarze technik zabezpieczeń teleinformatycznych działania Komitetu koncentrują się na następujących zagadnieniach:

- systemy zarządzania bezpieczeństwem informacji – normy zawierające wymagania i wytyczne

- kryptograficzne i niekryptograficzne techniki i mechanizmy zapewniające poufność, uwierzytelnienie podmiotu, niezaprzeczalność, zarządzanie kluczami oraz integralność danych

- kryteria oceny bezpieczeństwa oraz metodyki testów bezpieczeństwa produktów, zarówno w odniesieniu do funkcji jak i poziomu wiarygodności oceny

- usługi i aplikacje wspierające wdrożenie celów stosowania zabezpieczeń i zabezpieczeń zgodnie z ISO/IEC 27001

- aspekty bezpieczeństwa w zarządzaniu tożsamością oraz ochronie danych osobowych

W obszarze opisu oraz języków przetwarzania dokumentów prace Komitetu obejmują następujące zagadnienia:

- języki znacznikowe (SGML), interfejsy użytkownika, testowanie i rejestrowanie

- techniki przetwarzania dokumentów

- architektury zarządzania oraz wymiany informacji

- formaty XML-owe plików dokumentów: Office Open XML oraz Open Document Format oraz interoperacyjność formatów

W obszarze nowoczesnych technik informatycznych działania Komitetu są na wczesnym etapie i obejmują udział w pracach nad projektami norm dot. zagadnień, takich jak:

- Web Services

- Service Oriented Architecture (SOA)

- Przetwarzanie w chmurze (Cloud computing)

W obszarze Cyberbezpieczeństwa I Ochrony Danych działania Komitetu odzwierciedlają wczesny etap pracy Komitetu JTC13 i obejmują udział w pracach nad projektami norm.

Uwarunkowania prawne i biznesowe

Normy opracowane w Komitecie lub znajdujące się w zakresie zainteresowania Komitetu na poziomie międzynarodowym (normy międzynarodowe nieprzeniesione do systemu Polskich Norm) są przywoływane w aktach prawnych. Wskazując normy jako najlepszą i najprostszą metodę spełnienia wymagań, Ustawodawca przyczynia

się do wzrostu zainteresowania daną normą i wpływa na rozszerzenie kręgu jej zastosowań.

W poniższej tabeli przedstawiono przywołania norm w aktach prawnych.

Obowiązujący akt prawny	Norma z zakresu prac Komitetu powołana w akcie prawnym
Polskie akty prawne	
ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych ZAŁĄCZNIK WYKAZ CERTYFIKATÓW UPRAWNIAJĄCYCH DO PRZEPROWADZANIA KONTROLI W ROZUMIENIU ART. 25 USTAWY Z DNIA 17 LUTEGO 2005 R. O INFORMATYZACJI DZIAŁALNOŚCI PODMIOTÓW REALIZUJĄCYCH ZADANIA PUBLICZNE	PN-ISO/IEC 27001
ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników	PN-ISO/IEC 27001
ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych	PN-ISO/IEC 27001
ROZPORZĄDZENIE 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	PN-ISO/IEC 27001 PN-ISO/IEC 17799 PN-ISO/IEC 27005 PN-ISO/IEC 24762 ISO/IEC 19757-2 ISO/IEC 29500 ISO/IEC 26300
ROZPORZĄDZENIE RADY MINISTRÓW z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.	PN-ISO/IEC 15408 ISO/IEC 15946-2
ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych	ISO/IEC 26300
Rozporządzenie Ministra Cyfryzacji z dn. 10 września 2018r ws. warunków organizacyjnych i technicznych dla podmiotów świadczących usługi w zakresie cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatora usług kluczowych	PN-EN ISO/IEC 27001
Akty prawne Unii Europejskiej	
ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) NR 1179/2011 z dnia 17 listopada 2011 r. ustanawiające specyfikacje techniczne w odniesieniu do systemów zbierania deklaracji on-line na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 211/2011 w sprawie inicjatywy obywatelskiej	ISO/IEC 27001 (PN-ISO/IEC 27001) ISO/IEC 27002 (PN-ISO/IEC 17799) ISO/IEC 27005 (PN-ISO/IEC 27005) ISO/IEC 27033
ROZPORZĄDZENIE KOMISJI (WE) NR 885/2006 z dnia 21 czerwca 2006 r. ustanawiające szczegółowe zasady stosowania rozporządzenia Rady (WE) nr 1290/2005 w zakresie akredytacji agencji płatniczych i innych jednostek, jak również rozliczenia rachunków EFGR i EFRROW	ISO/IEC 27002 (PN-ISO/IEC 17799)
ROZPORZĄDZENIE KOMISJI (UE) NR 73/2010 z dnia 26 stycznia 2010 r. ustanawiające wymagania dotyczące jakości danych i informacji lotniczych dla jednolitej europejskiej przestrzeni powietrznej	ISO/IEC 27002 (PN-ISO/IEC 17799)

Obowiązujący akt prawny	Norma z zakresu prac Komitetu powołana w akcie prawnym
DECYZJA WYKONAWCZA KOMISJI (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiająca normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym	ISO/IEC 15408 (PN-EN ISO/IEC 15408)

W ślad za wprowadzeniem norm do aktów prawnych pojawia się powszechnie, zarówno w postępowaniach o udzielenie zamówień publicznych, jak i postępowaniach prowadzonych na podstawie innych uregulowań niż ustawa Prawo Zamówień Publicznych, wymaganie znajomości norm lub wdrożenia u potencjalnego dostawcy systemu zarządzania bezpieczeństwem informacji, zgodnego z normą PN-ISO/IEC 27001 lub opracowania i wdrożenia takiego systemu w odniesieniu do przedmiotu zamówienia.

Z uwagi na szeroki zakres zastosowania normy PN-ISO/IEC 27001, zainteresowane jej wdrożeniem są organizacje ze wszystkich sektorów, niezależnie od wielkości organizacji czy specyfiki działania.

1.2 Wskaźniki ilościowe dotyczące środowiska biznesowego

Poniższe wskaźniki ilościowe opisują środowisko biznesowe, w celu wsparcia działań KT poprzez zapewnienie niezbędnych danych:

Certyfikacja na zgodność z Polską Normą

Szczególnym zainteresowaniem rynku cieszą się normy zawierające wymagania z możliwością certyfikacji na zgodność. Z tego względu normy te funkcjonują nie tylko w sektorze administracji publicznej, ale także w sektorze przemysłu i usług.

Do tej grupy należą normy:

- PN-ISO/IEC 15408:2014 Kryteria oceny zabezpieczeń informatycznych (cz. 1, i 3) oraz PN-ISO/IEC 18045:2014 Metodyka oceny bezpieczeństwa
- PN ISO/IEC 27001:2007 Systemy zarządzania bezpieczeństwem informacji. Wymagania

Oficjalne statystyki ISO (zob. *http://www.iso.org/iso/iso-survey*) są prowadzone dla wszystkich certyfikatów systemów zarządzania wydawanych przez akredytowane jednostki certyfikujące. Zgodnie z danymi ISO, w 2017 roku było 705 polskich organizacji, które mają taki certyfikat, co lokuje nas na 12. miejscu na świecie.

Certyfikaty bezpieczeństwa dla produktów ewaluowanych zgodnie z normami ISO/IEC 15408 i 18045 są realizowane w innych krajach (zob. *https://commoncriteriaportal.org/products/* . europejskie programy oceny i

certyfikacji bezpieczeństwa zgromadzone w porozumieniu SOG-IS MRA (do tej organizacji należy też Polska) wydaje ok. 200 certyfikatów rocznie.

2 OCZEKIWANE KORZYŚCI Z REALIZACJI PRAC KT

- Wsparcie dla opracowywanych przepisów prawa oraz odniesień referencyjnych z uwagi na wskazanie JTC1/SC27, a co za tym idzie – KT 182 – jako pierwotnego źródła normalizacji działań w zakresie bezpieczeństwa informacji, cyberbezpieczeństwa oraz ochrony danych
- Opracowanie norm referencyjnych dla sektorowych norm z bezpieczeństwa informacji[a]
- Wzrost świadomości znaczenia ochrony informacji, zarówno w kontekście biznesowym, jak i bezpieczeństwa państwa, a także dla rozwoju społecznego (ochrona danych osobowych i prywatności, w szczególności przy użyciu środków komunikacji elektronicznej)
- Wypracowanie podstaw interoperacyjności dla zastosowań informatycznych (dokument elektroniczny, podpis elektroniczny, platformy usług informatycznych oraz przetwarzania w chmurze).

3 CZŁONKOSTWO W KT I STRUKTURA KT

Każdy podmiot krajowy zainteresowany daną tematyką ma prawo zgłosić chęć uczestnictwa w KT i po spełnieniu wymogów proceduralnych (procedura Z2-P3 w powiązaniu z Z2-P1) stać się członkiem KT. Każdy członek KT realizuje zadania KT poprzez swoich reprezentantów.
Aktualny skład KT jest podany na stronie www.pkn.pl, w *Wykazie OT*.

Komitet jest najliczniejszym z Komitetów Technicznych przy PKN, mając 37 członków.
Z uwagi na dużą liczebność Komitetu oraz rozległość obszarów normalizacyjnych, Komitet działa merytorycznie, wykorzystując Grupy Ekspertów, wypracowujących rekomendacje dla całego Komitetu.

4 CELE KT I STRATEGIA ICH REALIZACJI

4.1. Cele KT

Cele działalności Komitetu:

- Wspieranie bezpieczeństwa państwa oraz bezpieczeństwa gospodarczego przez propagowanie powszechnie stosowanych rozwiązań z zakresu bezpieczeństwa informacji
- Przeciwdziałanie wykluczeniu elektronicznemu przez wspieranie interoperacyjności w komunikacji elektronicznej

- Propagowanie rozwiązań nowoczesnych, sprawdzonych w praktyce
- Ułatwienie współpracy transgranicznej dla zwalczania cyber-przestępczości

Cele te Komitet zamierza osiągnąć w następujący sposób:

- Tłumaczenie norm ISO/IEC z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych
- Wprowadzanie norm międzynarodowych do systemu PN metodą uznania specyfikacji technicznych w szczególności dot. formatów dokumentów oraz algorytmów i technik kryptograficznych
- Organizowanie i uczestnictwo w konferencjach krajowych i międzynarodowych dotyczących normalizacji bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych

4.2. Strategia ustalona do osiągnięcia celów KT

Z uwagi na wolumen sprzedaży wyznaczający zainteresowanie rynku, przy ustalaniu Programu prac, Komitet za priorytet uznał tłumaczenie i wprowadzenie do systemu PN norm międzynarodowych z rodziny ISO/IEC 2700x.
Aby realizować cele swojej działalności Komitet aktywnie działa na w komitetach technicznych ISO przy opracowywaniu norm międzynarodowych, w szczególności w SC27 oraz SC38 oraz CEN/CENELEC JTC13.

4.3. Aspekty środowiskowe

[nie mają zastosowania]

5 CZYNNIKI WPŁYWAJĄCE NA REALIZACJĘ PROGRAMU PRAC KT I WPROWADZANIE NOWYCH TN DO PROGRAMU PRAC

Każdy zainteresowany ma możliwość zgłaszania tematów normalizacyjnych (TN) wypełniając Karty nowego tematu (KNT) lub Karty propozycji tematu normalizacyjnego (KPT).

Każdy zgłoszony TN jest wprowadzany do programu KT. KT decyduje o kontynuacji lub zaniechaniu tematu normalizacyjnego.

W programie prac prezentowane są wszystkie TN będące aktualnie w opracowaniu.

Program prac KT znajduje się na stronie www.pkn.pl , w Wykazie OT, po wybraniu numeru właściwego KT.

Drugi element numeru tematu normalizacyjnego wskazuje numer Podkomitetu Technicznego opracowującego temat, np. numer tematu normalizacyjnego XXX.1.XXXX oznacza wykonywanie w KT XXX PK 1 (Podkomitecie Technicznym nr 1 Komitetu Technicznego XXX). Jeżeli drugi element przyjmuje wartość zero oznacza to, ze TN jest opracowywany w KT.

Istotnym czynnikiem ograniczającym możliwości realizacji celów Komitetu jest problem braku finansowania wprowadzania norm ISO-wskich do systemu PN.
Brak jest na rynku podmiotów bezpośrednio zainteresowanych finansowaniem norm, a jednocześnie jest duże zainteresowanie ze strony różnych środowisk polskimi normami z zakresu bezpieczeństwa informacji, zwłaszcza normą ISO/IEC 27001 oraz normami wspierającymi jej wdrożenie (rodzina norm ISO/IEC 2700x). Ponadto, należy podkreślić, że korzystanie z tych norm jako podstaw dla wymagań wprowadzanych do aktów prawnych Rzeczypospolitej Polskiej powinno skutkować zapewnieniem finansowania wprowadzania tych norm do systemu PN.
Kolejnym czynnikiem powodującym opóźnienie prac jest zbyt późne wprowadzanie do Programu prac normalizacyjnych opublikowanych już norm międzynarodowych.
Z uwagi na charakter prac, do Programu powinny być wprowadzane projekty norm na etapie DIS lub FDIS.

6 WYKAZ PROPOZYCJI TEMATÓW NORMALIZACYJNYCH, DLA KTÓRYCH KT PRZEWIDUJE POZYSKANIE ZAMAWIAJĄCYCH W RAMACH PRAC NA ZAMÓWIENIE

Brak propozycji tematów w ramach prac na zamówienie