

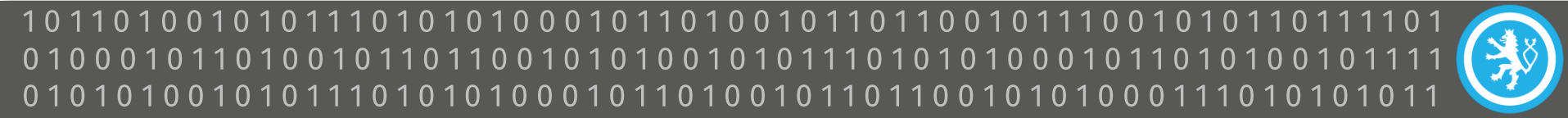
Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Dušan Navrátil

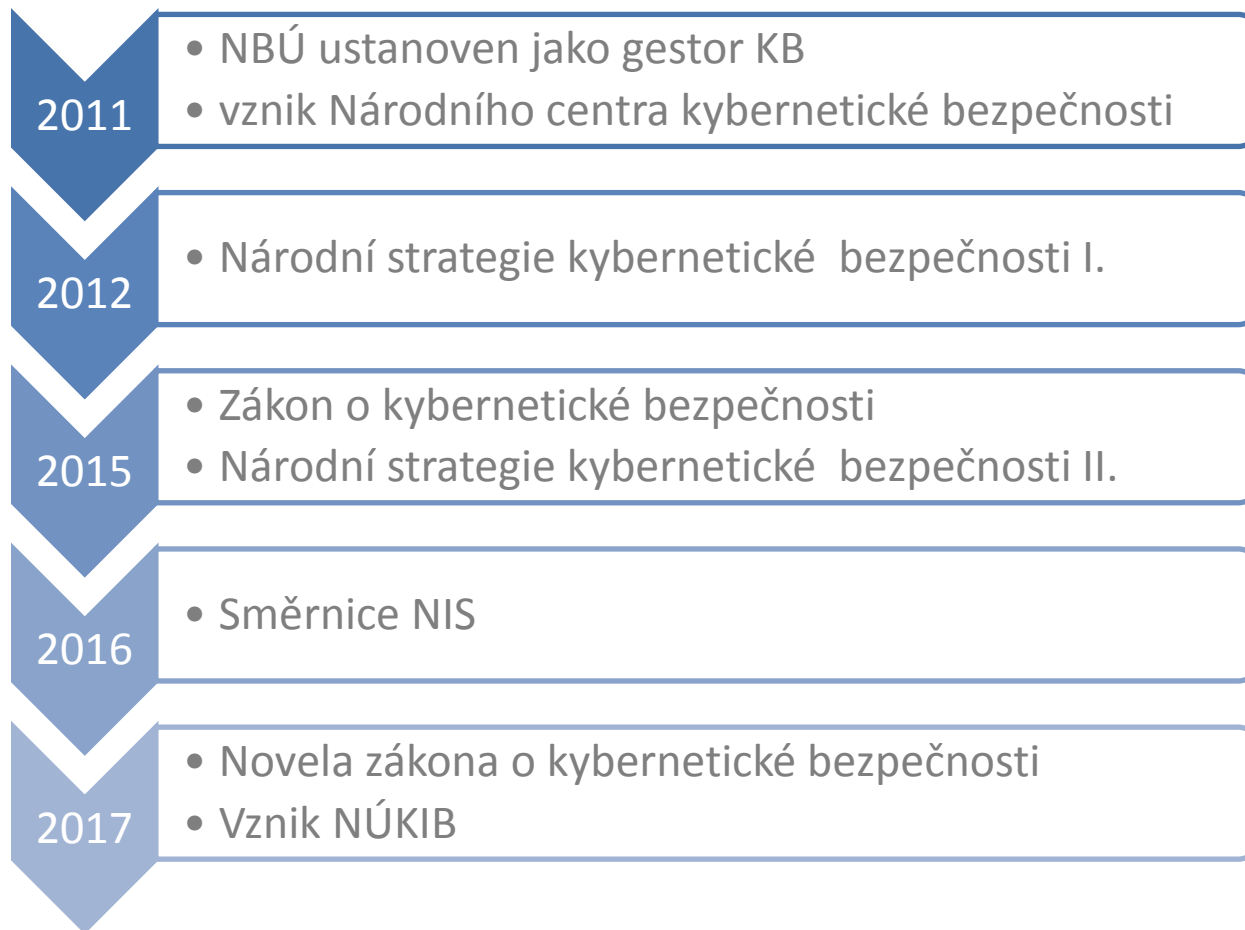
ředitel

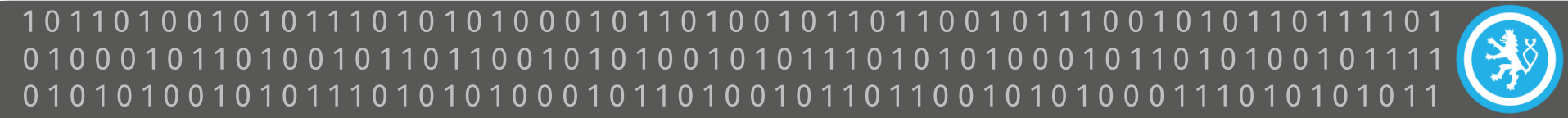
Národní úřad
pro kybernetickou
a informační bezpečnost





Kybernetická bezpečnost v ČR





Národní úřad pro kybernetickou a informační bezpečnost

- Vznik novelou zákona o kybernetické bezpečnosti od 1. 8. 2017
- Cca 40 odborných pracovníků
- Ústřední správní orgán pro:
 - kybernetickou bezpečnost
 - ochranu utajovaných informací v oblasti informačních a komunikačních systémů
 - kryptografickou ochranu
- Služby NÚKIB v oblasti kybernetické bezpečnosti:
 - provozovat Vládní CERT České republiky (GovCERT.CZ)
 - spolupráce s ostatními CERT A CSIRT
 - příprava bezpečnostních standardů
 - osvěta a podpora vzdělávání
 - výzkum a vývoj
 - ochrana utajovaných informací v oblasti IS/KS
 - kryptografická ochrana
 - Kontaktní místo GALILEO



1011010010101110101010001011010010110110010111001010110111101
0100010110100101101100101010010101110101010001011010100101111
0101010010101110101010001011010010110110010101000111010101011



**Kybernetická
obrana**



**Ochrana
kritické
informační
infrastruktury**

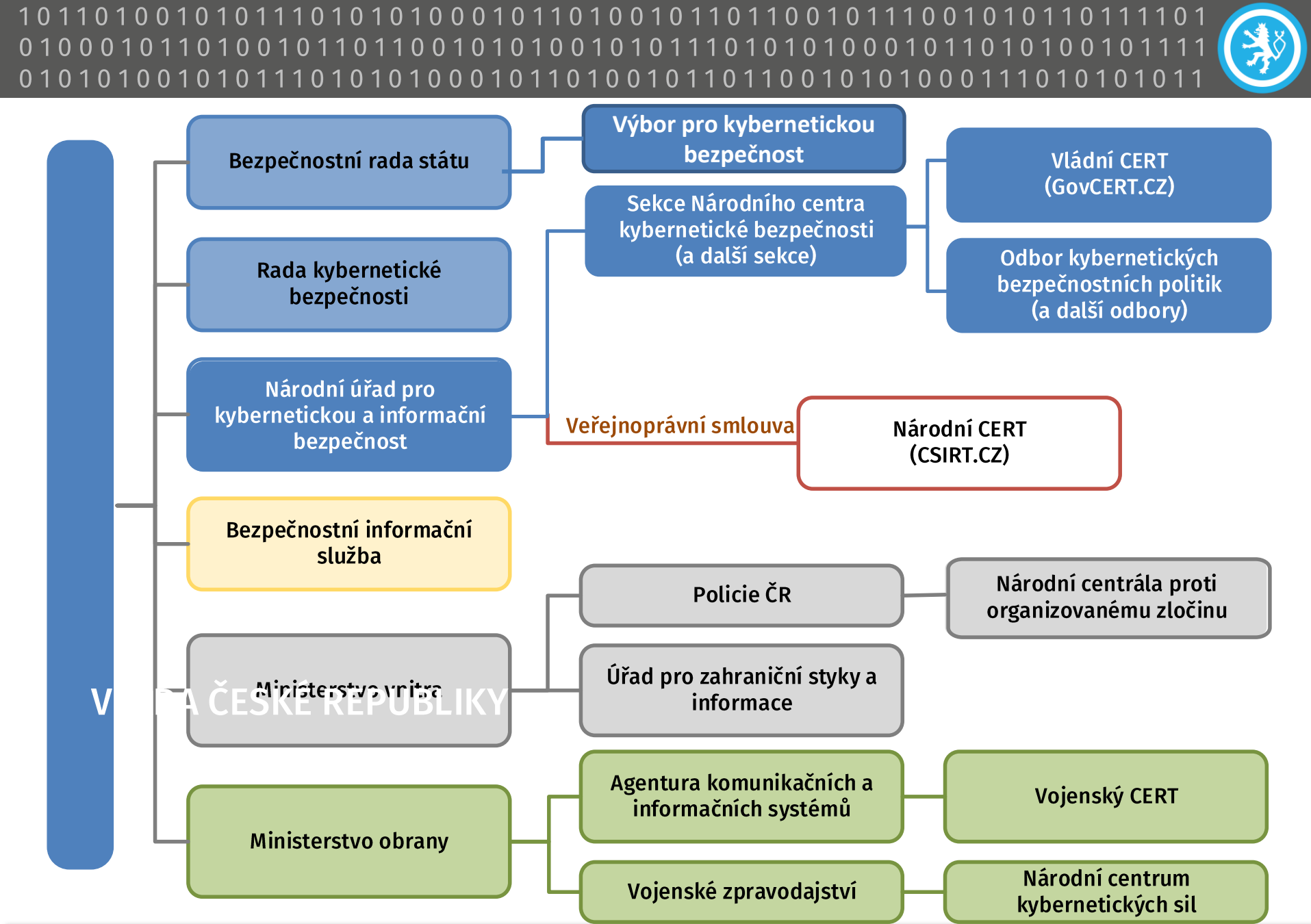


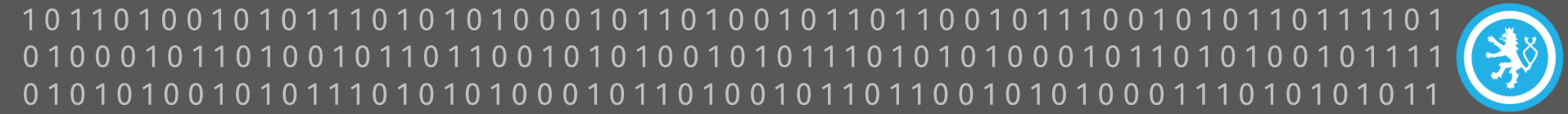
**Kybernetická
kriminalita**



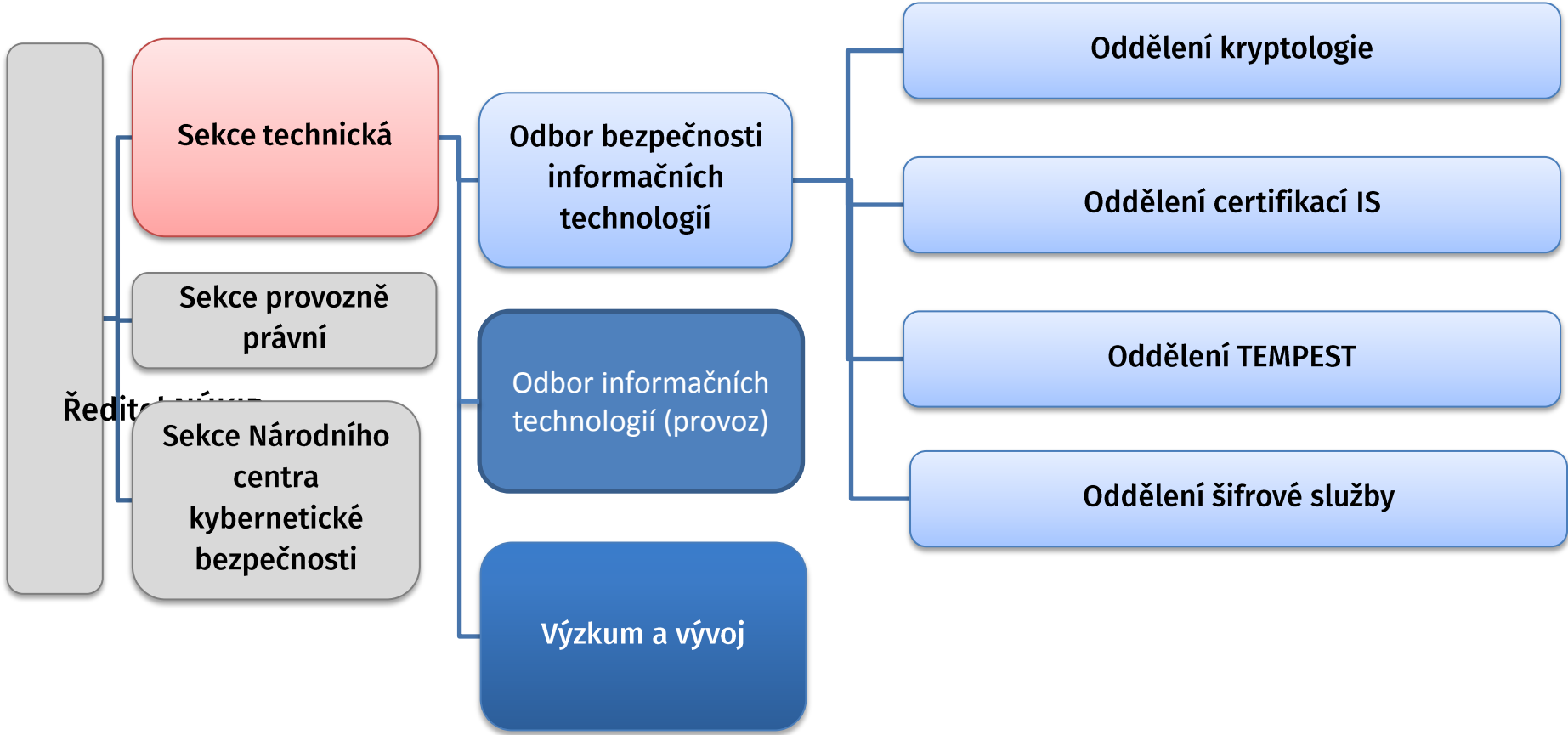
**Působení
zpravodajských
služeb**

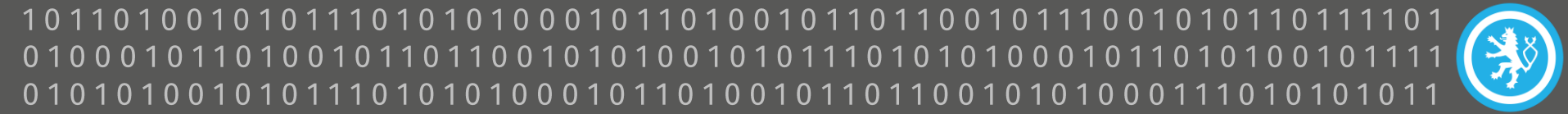
ROLE STÁTU PŘI ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI



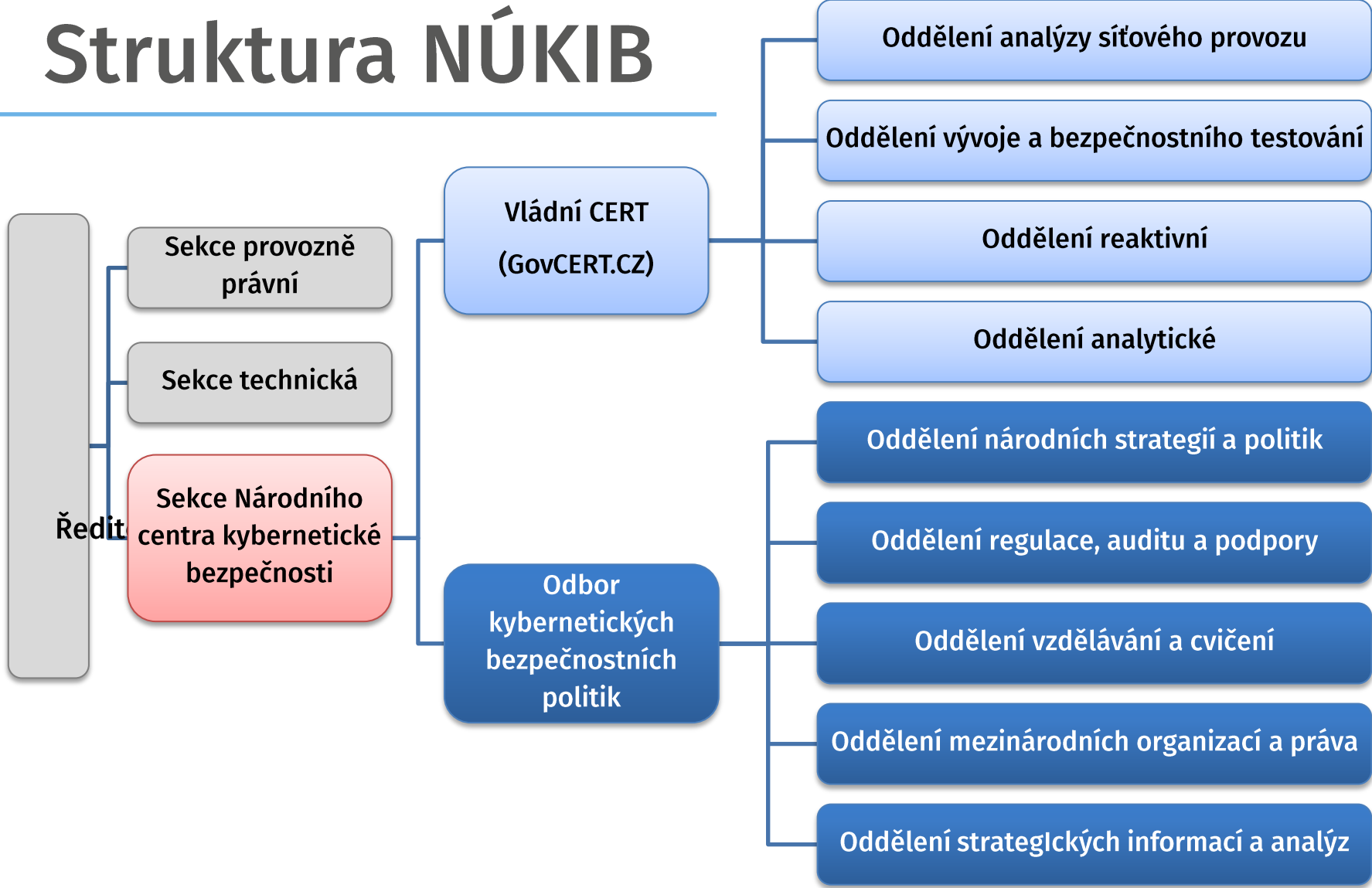


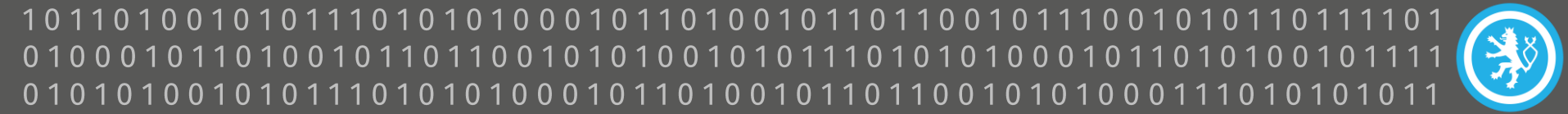
Struktura NÚKIB



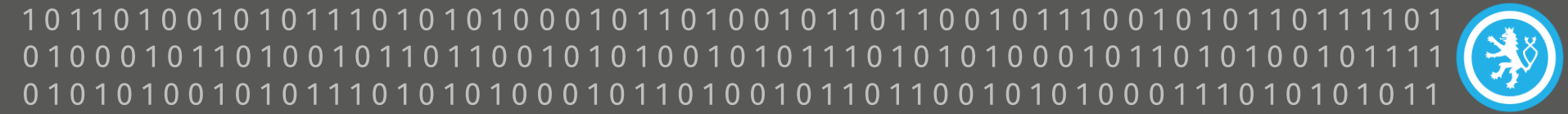


Struktura NÚKIB



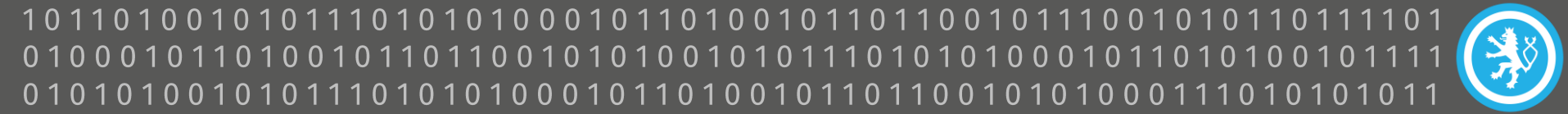


Odbor bezpečnosti informačních a komunikačních technologií



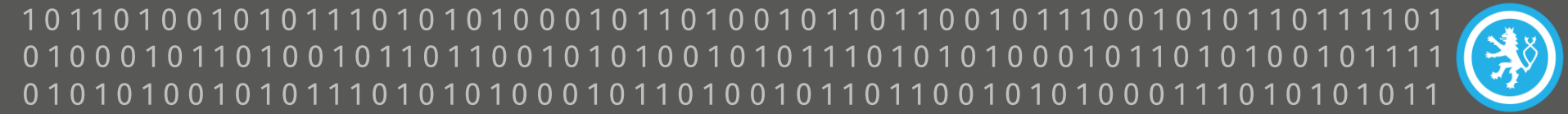
Odbor bezpečnosti informačních a komunikačních technologií

- vývoj národních kryptografických algoritmů pro ochranu utajovaných informací
- vývoj národních kryptografických prostředků pro ochranu utajovaných informací
- certifikace kryptografických prostředků třetích stran
- certifikace informačních a komunikačních systémů nakládajících s národními utajovanými informacemi
- certifikace informačních a komunikačních systémů provozovaných na území ČR nakládajících s utajovanými informacemi NATO a EU



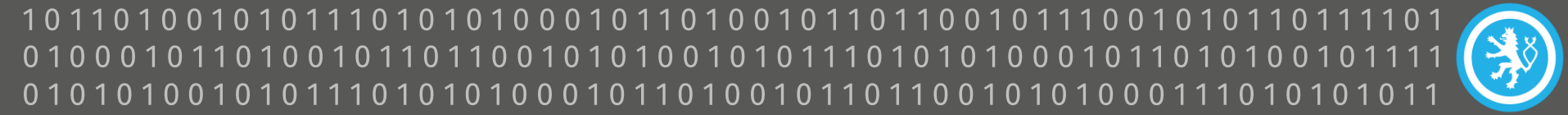
Odbor bezpečnosti informačních a komunikačních technologií

- měření možného úniku informací prostřednictvím parazitního elektromagnetického vyzařování (EMV):
 - z počítačů (včetně periferních zařízení)
 - ze stíněných komor
 - ze zabezpečených oblastí určených k nakládání s UI (zónová měření), ...
- vývoj zařízení k měření parazitního EMV



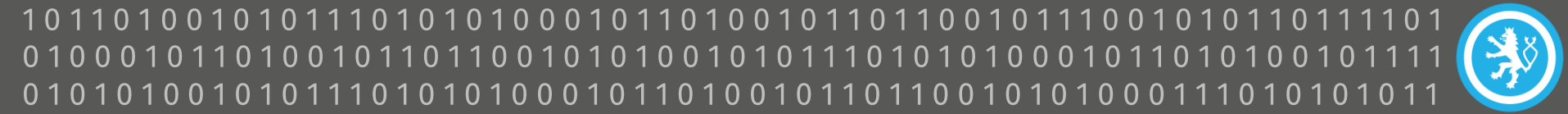
Odbor bezpečnosti informačních a komunikačních technologií

- plní roli národního distribučního pracoviště pro distribuci kryptografického materiálu (národního i cizího)
- vede národní krypto účet
- vyrábí národní kryptografický materiálu (klíče, dokumentace, ...)
- poskytuje prostředky mobilního šifrového spojení a spravuje jeho provoz



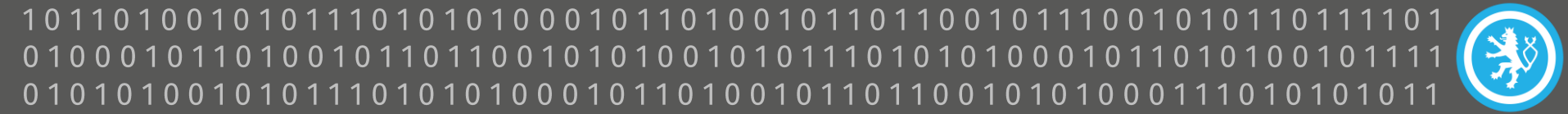
Vládní CERT

(Computer Emergency Response Team)



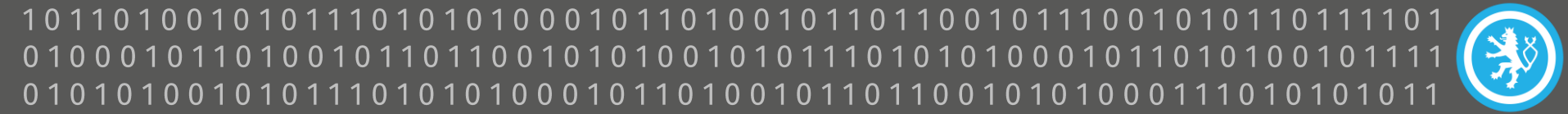
Zaměření vládního CERT

- Cílová skupina - veřejný sektor a kritická informační infrastruktura
- rozdělení týmu
 - zpracování incidentů
 - vývoj a bezpečnostní testování
 - síťová analýza
 - forenzní analýza



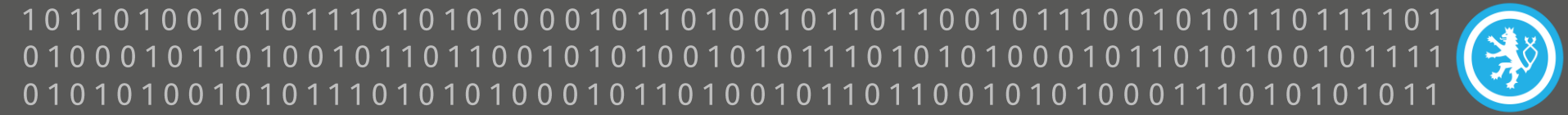
Zaměření vládního CERT

- **základní služby**
 - **proaktivní:** koordinace v rámci české bezpečnostní komunity a sdílení informací
 - **reaktivní:** zpracování a řešení incidentů, zpracování a analýza artefaktů
 - **detekce:** vyhledávání anomálií (např. systémové logy, veřejně dostupné informace - Botnet feeds, OSINT)



Zaměření vládního CERT

- analýza malware
- penetrační testování
- forenzní činnost
- řídicí a SCADA systémy
- síťová bezpečnost a analýza síťového provozu
- zranitelnosti virtualizovaných prostředí a cloudových řešení
- zranitelnosti IS s operačními systémy založenými na UNIX
- zranitelnosti IS s operačními systémy z rodiny Windows
- honeypoty

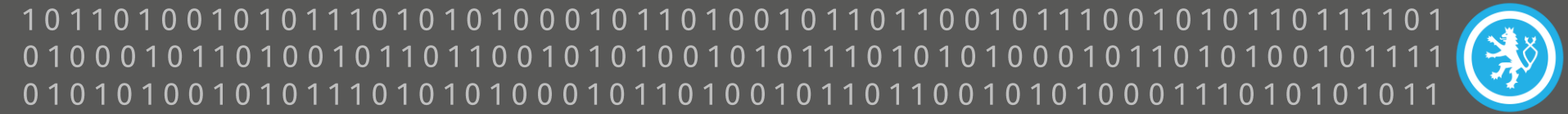


Odbor kybernetických bezpečnostních politik (OKBP)



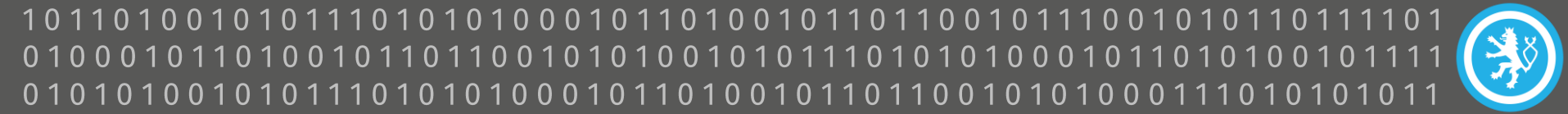
Odbor kybernetických bezpečnostních politik

- Rozdělení týmu na oddělení
 - oddělení národních strategií a politik
 - oddělení regulace, auditu a podpory
 - oddělení vzdělávání a cvičení
 - oddělení mezinárodních organizací a práva
 - oddělení strategických informací a analýz



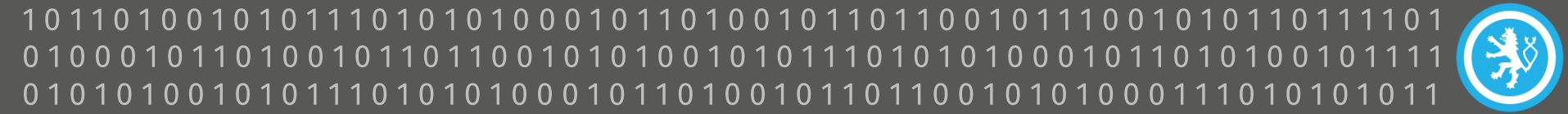
Zaměření OKBP - strategie

- implementace Národní strategie kybernetické bezpečnosti
- plnění, koordinace a kontrola Akčního plánu
- **příprava dlouhodobých plánů a projektů**
 - „Spolek přátel kybernetické bezpečnosti“ - Kyberliga
 - plánování rozvoje kapacit
 - spolupráce se soukromým sektorem
- **vyhodnocování nových hrozeb na strategické úrovni**
- koordinace činností souvisejících s plněním Národní strategie kybernetické bezpečnosti na národní úrovni



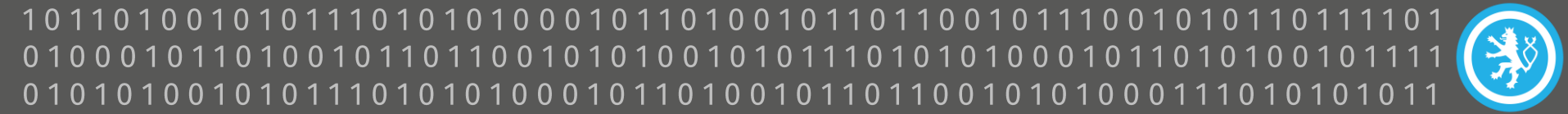
Zaměření OKBP - regulace

- **Regulace**
 - stanovení subjektů a systémů spadajících pod regulaci dle kritérií ZKB
 - příprava legislativy (vyhlášky k ZKB)
- **Audit** (kontrola ZKB)
 - kontrola dodržování ZKB podobně jako u auditu systému řízení bezpečnosti informací podle ISO 27 001
- **Podpora**
 - výklad ustanovení ZKB, výklad vyhlášek
 - metodická podpora při implementaci ZKB



Zaměření OKBP - regulace

- Aktuální stav určení kritické informační infrastruktury a významných informačních systémů
 - **Významné informační systémy (VIS)**
 - Značné množství subjektů prozatím neurčilo své VIS - spisové služby, úřední desky a ekonomické systémy. Zvažujeme, zda nevydat metodické doporučení aby tak učinili.
 - **Kritická informační infrastruktura (KII)**
 - Určování KII dosud neskončilo. Určování bylo vzhledem k jiným úkolům přerušeno a bude k němu opět přistoupeno. Aktuálně je možné říci, že je již určeno cca 60 % - 70 % **systémů splňující kritéria pro KII** – tj. možný nárůst KII očekáváme v řádu nižších desítek (odhadem cca 40 **systémů**).

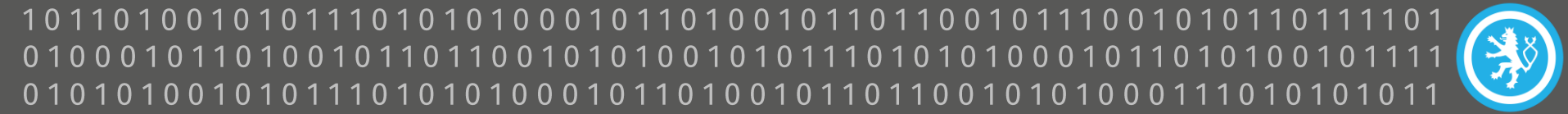


Zaměření OKBP - regulace

- Aktuální stav určení kritické informační infrastruktury a významných informačních systémů**

Počet správců kritické informační infrastruktury (KII) a významných informačních systémů (VIS) a informačních/komunikačních systémů KII/VIS (stav k 10. 8. 2017)

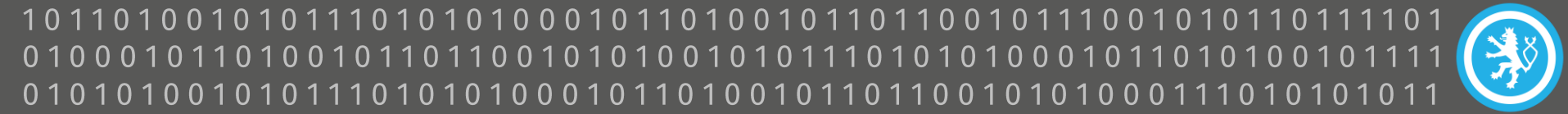
Typ systému	Počet systémů	Počet správců
KII	112	46
VIS	169	62
Celkem	281	108



Zaměření OKBP - regulace

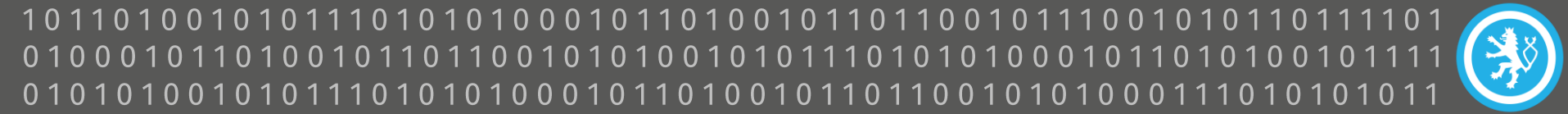
Hrubé odhady počtu provozovatelů základních služeb (PZS) a informačních systémů základních služeb (ISZS) v jednotlivých odvětvích a pododvětvích

Odvětví/pododvětví PZS	Je v odvětví určena KII? (počet správců/systémů)	Odhad počtu PZS (nad rámec KII)	Odhad počtu systémů – ISZS
1.1 energetika - elektřina	ANO (6/27)	3 (některé subjekty budou zařazeny do KII)	10
1.2 energetika - plyn	ANO (2/4)	4 - 6	6 - 10
1.3 energetika - ropa	ANO (2/5)	3	3 - 6
1.4 energetika - teplárenství	NE	20 – 30 (některé subjekty budou zařazeny do KII)	30 - 60
2.1 doprava - letecká	ANO (1/1)	2	4 - 6
2.2 doprava - silniční	NE	2	4
2.3 doprava - železniční	ANO (1/1)	4	4 - 8
3. Bankovníctví	ANO (3/6)	19	38
4. Infrastruktura finančních trhů	NE	3 - 4	4 - 8
5. zdravotnictví	NE	16	32 - 40
6. dodávky a rozvody pitné vody	ANO (1/1)	20 (některé subjekty budou zařazeny do KII)	20
7. digitální infrastruktura	NE	4 - 10	8 - 20
8. chemický průmysl	NE	5	10
CELKEM	-	105 – 121 PZS	173 - 260 ISZS



Zaměření OKBP - regulace

- Na základě usnesení vlády provádí metodickou podporu v oblasti kybernetické bezpečnosti na ministerstvech a dalších vybraných orgánech
- Zpracovává a jednou ročně vládě předkládá informaci o stavu kybernetické bezpečnosti



Zaměření OKBP - regulace

**Povinnými subjekty jsou především
správci a provozovatelé:**

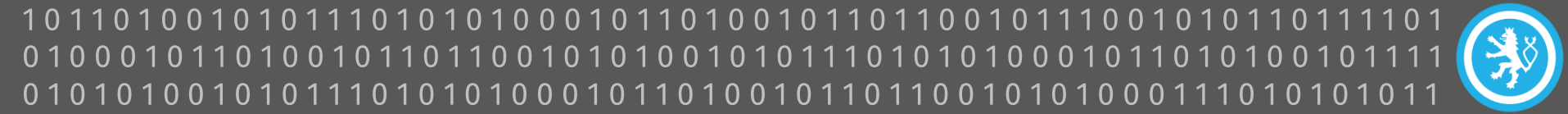
- prvků kritické informační infrastruktury
- významných informačních systémů
- informačních systémů základní služby
a poskytovatelé digitální služby

Veřejná správa

- ministerstva
- ústřední správní orgány
- kraje

Soukromý sektor

- energetické společnosti
- plynárenské společnosti
- telekomunikační operátoři
- bankovní instituce
a mnoho dalších



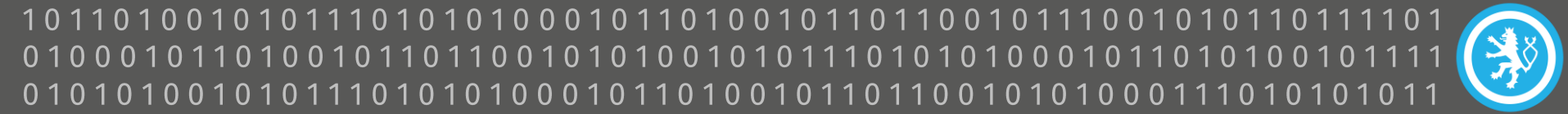
Zaměření OKBP - vzdělávání a cvičení

- komplexní příprava technických cvičení:
 - Cyber Coalition, Locked Shields, Cyber Europe
 - CyberCzech 2015, CyberCzech 2016, CECSP 2016
- komplexní příprava netechnických / table-top cvičení:
 - Locked Shields, Cybereurope, Crisis management exercise, Strategic TTX



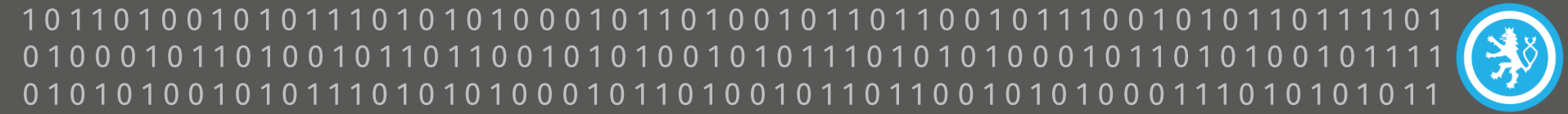
**LOCKED
SHIELDS**





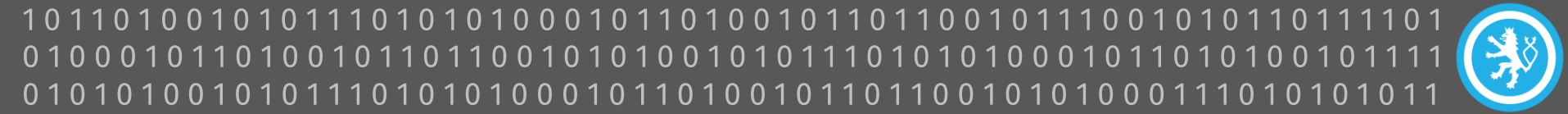
Zaměření OKBP - vzdělávání a cvičení

- osvěta, vzdělání a výzkum
 - akademická sféra:
 - Masarykova univerzita, Palackého univerzita, osvětová činnost
 - diplomové práce, výuka, stáže
 - e-learning - projekt „Digitální stopa“
 - vzdělávání zaměstnanců veřejné správy (spolupráce IVS)
- další rozvoj
 - „Koncepce vzdělávání v kyberprostoru“ s MŠMT a MPSV „uživatel především“
 - administrace výzkumu – vlastní
 - koordinace výzkumu mezi státem, akademickou a soukromou sférou



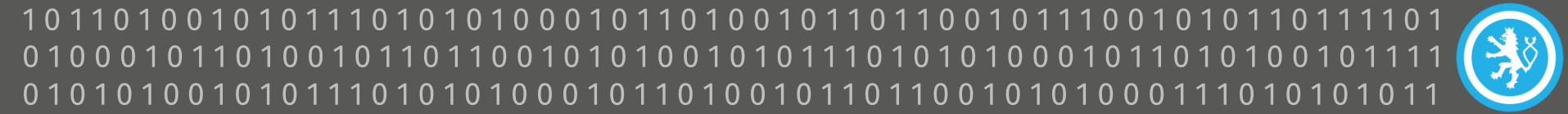
Zaměření OKBP – mezinárodní vztahy, právo

- reprezentace České republiky v rámci mezinárodních organizací
- mezinárodní spolupráce
 - EU – implementace směrnice NIS, Horizont 2020
 - NATO – Cyber Defence Committee
 - OBSE – CBMs, confidence building measures
- vnitrostátní spolupráce
 - Úřad vlády České republiky, Ministerstvo vnitra, Ministerstvo zahraničních věcí, Ministerstvo spravedlnosti, Ministerstvo obrany
- spolupráce a právní podpora v rámci NÚKIB



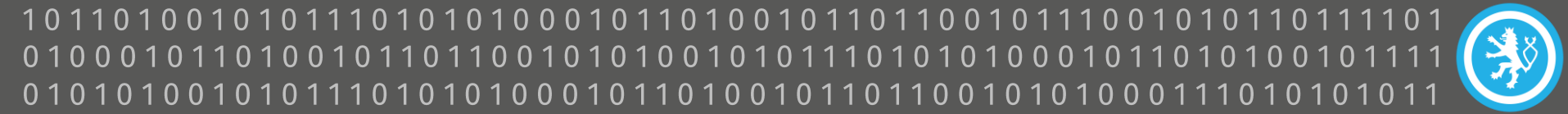
Zaměření OKBP – mezinárodní vztahy, právo

- **strategičtí partneři**
 - USA – FBI, DHS, Ministerstvo obrany, Microsoft, Cisco
 - Jižní Korea – zpravodajská komunita
 - Izrael – MalMab, National Cyber Bureau, CyberGym
- **cyber attaché – USA, Izrael, Brusel**
- **kapacity NÚKIB v oblasti kybernetické bezpečnosti nástrojem zahraniční politiky ČR**
- **rozvojová pomoc:**
 - TAIEX (Ukrajina, balkánské země, Kazachstán, ...)
 - technická školení pro partnery (středoevropská kyber platforma) a budování mezinárodních vazeb, ...



Zaměření OKBP - strategické informace, analýzy

- využití informací z otevřených zdrojů
- tvorba technického a metodologického rámce pro práci s informacemi
- systém včasného varování
- prevence rizik
 - analýza kybernetických hrozeb a útoků prostřednictvím kontextualizace
- regionální a strategický segment
- informační podpora v krizových situacích
 - výměna informací s národními a mezinárodními partnery
 - platforma pro informování vedoucích činitelů ve věci kybernetické bezpečnosti státu



Děkuji Vám za pozornost

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

www.nukib.cz