NÚKIB

KONCEPCE ROZVOJE NÁRODNÍHO ÚŘADU PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

2020

Obsah

1 Úvodní slovo ředitele

Zajišťování kybernetické a informační bezpečnosti je neodmyslitelnou povinností moderního a sebevědomého státu. Ještě nedávno přitom byla kybernetická bezpečnost považována za disciplínu několika málo technických specialistů. Dnes po útocích na naše zdravotnická zařízení, po kybernetických incidentech, které ochromily fungování globálních firem, či po masivních vlnách podvodných a vyděračských e-mailů už nikdo nepochybuje, že jde o oblast, která se dotýká nás všech. Dotýká se bezpečnosti státu, jeho institucí, a zejména se dotýká bezpečnosti všech občanů.

Zároveň je kybernetická bezpečnost relativně nový obor. Proto všechny státy na světě stejně jako Česká republika stále hledají způsoby, jak se s výzvami, které kybernetická bezpečnost přináší, co nejlépe vypořádat. Česko je v tomto ohledu v mnoha věcech průkopníkem. Již v roce 2017 vznikl Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) jako samostatný úřad, který má tuto oblast v gesci. Ještě před tím vznikl zákon o kybernetické bezpečnosti, který představuje ucelený a světově oceňovaný právní rámec k zajišťování kybernetické bezpečnosti systémů, které jsou nezbytné pro chod státu a bezpečí jeho obyvatel.

Podstatně delší historii má v naší zemi zajišťování bezpečnosti utajovaných informací v informačních a komunikačních systémech. I v této oblasti jsme historicky dosáhli řady významných úspěchů a například v problematice TEMPEST patříme ke světové špičce.

Nic z toho ovšem neznamená, že máme hotovo. Ve skutečnosti jsme teprve na začátku. Kybernetické hrozby ze strany států, kyberteroristů, kyberkriminálních skupin a dalších aktérů budou téměř jistě sílit. Dále lze očekávat příchod zcela nových a přelomových technologií, jako je umělá inteligence nebo kvantové počítače, které zásadně ovlivní používanou kryptografii i další oblasti. NÚKIB má ve své gesci také veřejně regulovanou část systému Galileo, která na své plné praktické využití teprve čeká.

Aby Česká republika zajistila do budoucna bezpečí svých obyvatel i svých utajovaných informací a zajistila si suverenitu i v kyberprostoru, musí své kapacity v kybernetické a informační bezpečnosti průběžně posilovat a také vyhodnocovat, jestli je nastavený směr správný.

To je i důvod vzniku této koncepce. Předcházelo jí detailní mapování současných kapacit NÚKIB a analýza budoucích hrozeb, aby bylo možné zjistit, kde jsou slabá místa a jakým směrem je třeba Úřad dál rozvíjet. Výsledek naší práce 17. srpna 2020 schválila vláda v utajovaném režimu a dala tak jednoznačně najevo, že oblast naší činnosti považuje za důležitou a že počítá s investicemi, které jsou pro dobudování kapacit NÚKIB nezbytné.

Já i moji kolegové jsme přesvědčeni, že veřejnost má právo vědět, kam se hodlá NÚKIB v budoucnu ubírat a jaké výzvy před námi stojí. Proto nabízíme tuto verzi textu. Z původní, vládou schválené utajované koncepce jsme vyjmuli utajované skutečnosti, citlivé informace, jejichž zveřejnění by pro náš stát představovalo riziko (primárně se jedná o popis slabých míst, omezení a zranitelností), a maximum ostatního dáváme k dispozici. Zároveň jsme se snažili text formulovat tak, aby byl srozumitelný i pro širší veřejnost.

Na následujících stránkách se dočtete, jaké činnosti v současnosti NÚKIB dělá, i jakým hrozbám a trendům zřejmě budeme v budoucnu čelit. Koncepce obsahuje jak dlouhodobější vizi a směr rozvoje NÚKIB, tak sedmiletý plán rozvoje a navyšování kapacit, včetně předpokládaného zdrojového rámce.

Pevně doufám, že tato konce dále přispěje ke zvyšování povědomí o naší činnosti i o významu kybernetické a informační bezpečnosti mezi širokou i odbornou veřejností. Hrozby v oblastech, v nichž NÚKIB působí, se týkají nás všech. A proto věřím, že kvalitní komunikace a sdílení maximálního možného množství informací, jsou zcela nezbytné, pokud chceme těmto hrozbám účinně čelit.

Ing. Karel Řehka

2 ÚVOD

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) plní v současné době kompetence v několika oblastech podstatných pro zajišťování bezpečnosti České republiky (dále jen „ČR“). Jedná se zejména o:

(i) plnění role gestora a národní autority v oblasti kybernetické bezpečnosti a výkon státní správy v této oblasti včetně provozu technického dohledového pracoviště Vládní CERT[1],
(ii) plnění role gestora ochrany utajovaných informací ČR v informačních a komunikačních systémech a role garanta ochrany utajovaných informací v informačních a komunikačních systémech cizí moci včetně role národní autority ČR v oblasti kryptografické ochrany (dále jen „informační bezpečnost“) a
(iii) výkon státní správy v oblasti veřejně regulované služby evropského programu globálního navigačního družicového systému Galileo (dále jen „GNSS“).

NÚKIB vznikl k 1. srpnu 2017 vyčleněním uvedených činností ze struktury Národního bezpečnostního úřadu (NBÚ).[2] Důvodem jeho vzniku byla zvyšující se důležitost zabezpečování kyberprostoru pro fungování státu a celé společnosti a zároveň nutnost vybudování specializované instituce, která zastřeší výše uvedené oblasti a poskytne vhodné podmínky pro vykonávání nezbytných agend.

Samotná činnost NÚKIB vychází zejména z kompetencí daných zákonem č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB“), zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen „ZoUI“) a Rozhodnutím Evropského parlamentu a Rady č. 1104/20011/EU o podmínkách přístupu k veřejně regulované službě nabízené globálním družicovým navigačním systémem vytvořeným na základě programu Galileo (dále jen „Rozhodnutí PRS“). Tyto jsou dále rozvíjeny strategickými materiály, např. *Národní strategií kybernetické bezpečnosti České republiky na období let 2015 až 2020* společně s navazujícím Akčním plánem, které stanovují další úkoly NÚKIB v oblasti kybernetické bezpečnosti.[3]

I na základě těchto koncepčních dokumentů byl vládou ČR schválen materiál *Návrh rozvoje kapacit a schopností Národního centra kybernetické bezpečnosti Národního bezpečnostního úřadu do roku 2025*[4], který mimo jiné předpokládá výstavbu objektu Černá Pole a navýšení kapacit na 350 – 400 osob.

V návaznosti na tento dokument a s ohledem na změny, ke kterým došlo od jeho přijetí, včetně samotného vzniku NÚKIB, byl dále rozpracován dokument *Rozvoj Národního úřadu pro kybernetickou a informační bezpečnost*, který byl schválen vedením úřadu dne 1. srpna 2018. Tento materiál však nebyl projednán vládou ČR.

Od přijetí současných platných strategických dokumentů[5] schválených vládou došlo k některým zásadním změnám. Jedná se zejména o:

[1] Označení pro tzv. Computer Emergency Response Team.
[2] Na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.
[3] S ohledem na konec období zmíněných dokumentů dochází k přípravě jejich aktualizovaných podob na nadcházející pětileté období.
[4] Schváleno usnesením vlády ze dne 28. listopadu 2016 č. 1049.
[5] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020, Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 (SKB a AP), Návrh rozvoje kapacit a schopností Národního centra kybernetické bezpečnosti Národního bezpečnostního úřadu do roku 2025, Akční plán implementace PRS v ČR, aj.

- **kompetenční změny** – např. rozšíření okruhu povinných osob dle ZKB na základě přijetí směrnice EU o bezpečnosti sítí a informací (dále jen „NIS směrnice“)[6]; úkoly uložené vládou ČR provádět analýzy úrovně zajištění kybernetické bezpečnosti ve vybraných státních institucích; zvýšená aktivita mezinárodních organizací (EU, NATO) na poli kybernetické a informační bezpečnosti a v oblastech kosmického programu;
- **změny prostředí** – vývoj hrozeb a rizik v kyberprostoru a nárůst potřeby zajišťovat kybernetickou bezpečnost ze strany státu; vzrůstající množství kybernetických útoků na subjekty v ČR (např. sektor zdravotnictví); rostoucí počet subjektů vyžadujících asistenci ze strany NÚKIB; vzrůstající množství případů nežádoucích interferencí GNSS signálů;
- **technologické změny** – související rizika v oblastech, jako jsou například sítě 5G, využívání cloudových služeb, využívání online videokonferenčních služeb, rozvoj umělé inteligence a kvantových počítačů.

Cílem tohoto materiálu je reakce na uvedené změny a představení **koncepce rozvoje NÚKIB** včetně **potřebných kapacit a schopností v horizontu 7 let a vize rozvoje na další roky**. Koncepce reflektuje potřeby státu v oblasti působnosti úřadu a umožňuje efektivně plánovat personální a finanční zdroje potřebné pro jeho činnost.

2.1 Potřeba rozvoje a cíle koncepce

Primárním důvodem rozvoje kapacit a schopností NÚKIB je nezbytnost **naplňování daných kompetencí a úkolů**. Cílem je pak disponovat **schopností reagovat na zvyšující se počet a závažnost hrozeb** ovlivňujících bezpečnost informačních a komunikačních technologií v ČR ve spojení se zhoršujícím se bezpečnostním prostředím jak v kyberprostoru, tak i mimo něj.

Celkovým cílem rozvoje kapacit státu v oblasti kybernetické a informační bezpečnosti je **zajistit co nejvyšší míru bezpečnosti státu a jeho občanů**, stejně jako zajistit hladké fungování informačních a komunikačních technologií státních institucí a povinných subjektů významných pro chod státu, což ve svém důsledku umožní rozvoj konkurenceschopnosti České republiky a udržení kvality života občanů.

Další z klíčových činností NÚKIB je **garance plnění** úkolů v oblasti utajovaných informací vůči zahraničním partnerům, především EU a NATO, zejména IAA (Information Assurance Authority), TA (TEMPEST Authority), CAA (Crypto Approval Authority), CDA (Crypto Distribution Authority), SAA (Security Accreditation Authority), resp. NCSA (National CIS Security Authority) a Competent PRS Authority (CPA).

[6] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Proč je kybernetická a informační bezpečnost důležitá?

Informační a komunikační systémy a globální navigační družicové systémy jsou dnes využívány napříč celou společností. Jejich důležitost stoupá, jejich bezpečné využívání je základem pro fungování veřejných institucí a strategicky významných podniků a zároveň:

- zvyšují efektivitu a produktivitu různých odvětví lidské činnosti;
- stimulují ekonomiku, zvyšují konkurenceschopnost;
- zvyšují kvalitu života občanů.

Závislost společnosti na informačních a komunikačních technologiích a službách poskytovaných GNSS silně narůstá. Spolu s tím však sílí i hrozby spojené s jejich nefunkčností. Narušení jejich fungování může způsobit závažné následky. Může dojít k:

- závažným materiálním škodám;
- újmám na zdraví či životech obyvatelstva;
- reputačním škodám.

Dále jejich narušení může mít destabilizační efekt pro:

- ekonomickou prosperitu státu;
- národní bezpečnost.

V krajních případech může mít i vliv na svrchovanost státu.

Dosavadní útoky na instituce v ČR ukázaly, jakým problémem může být nedostatečné zajištění kybernetické a informační bezpečnosti. V důsledku těchto útoků došlo k významným reputačním i ekonomickým škodám a v případě útoků na zdravotnická zařízení k omezení poskytování zdravotní péče.

Těmto negativním aspektům se stát musí snažit zabránit, k čemuž potřebuje dostatečné kapacity. Je přirozené, že primární rozvoj kapacit státu v oblasti kybernetické a informační bezpečnosti musí začít u NÚKIB jakožto ústředního orgánu státní správy s působností v této oblasti.[7]

[7] Český systém zajišťování kybernetické bezpečnosti, jež nepojímá kybernetickou a informační bezpečnost jako izolované bezpečnostní odvětví, předpokládá nutnou aktivitu dalších státních i nestátních institucí a subjektů.

Vynaložené náklady na kybernetickou a informační bezpečnost však budou mít i tyto navázané pozitivní efekty:

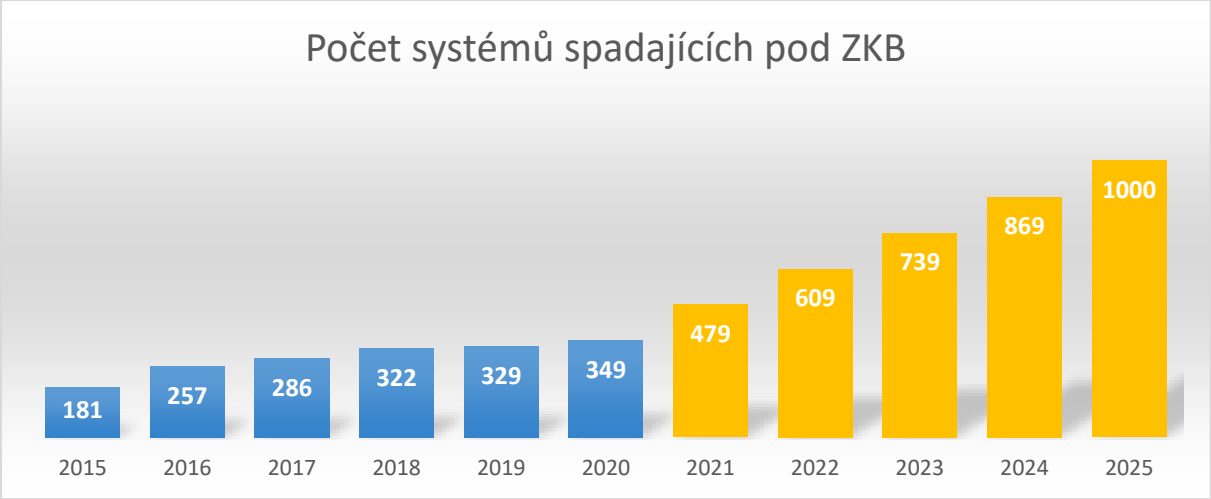
- **ekonomický růst**;
- **fungující informační společnost**;
- **zvýšení kvality života**;
- **posílení vlivu na mezinárodní úrovni s cílem prosazovat zájmy a pozice ČR**;
- **prohloubení důvěry občanů ve stát (a vládu ČR) a jeho bezpečnostní systém**.

Představovanou koncepci rozvoje je nutné interpretovat s ohledem na neustále se vyvíjející výzvy a hrozby v oblasti kybernetické a informační bezpečnosti a rostoucí počet závažných kybernetických útoků. Zejména v uplynulé době lze pozorovat značnou dynamiku vývoje potřeb státu v oblasti kybernetické i informační bezpečnosti. Proto je i tato koncepce pojímána rámcově s tím, že k jejím úpravám může v následujících letech dále docházet dle aktuálních a vyvíjejících se potřeb státu v této oblasti.

3 SOUČASNOST

3.1 Bezpečnostní prostředí

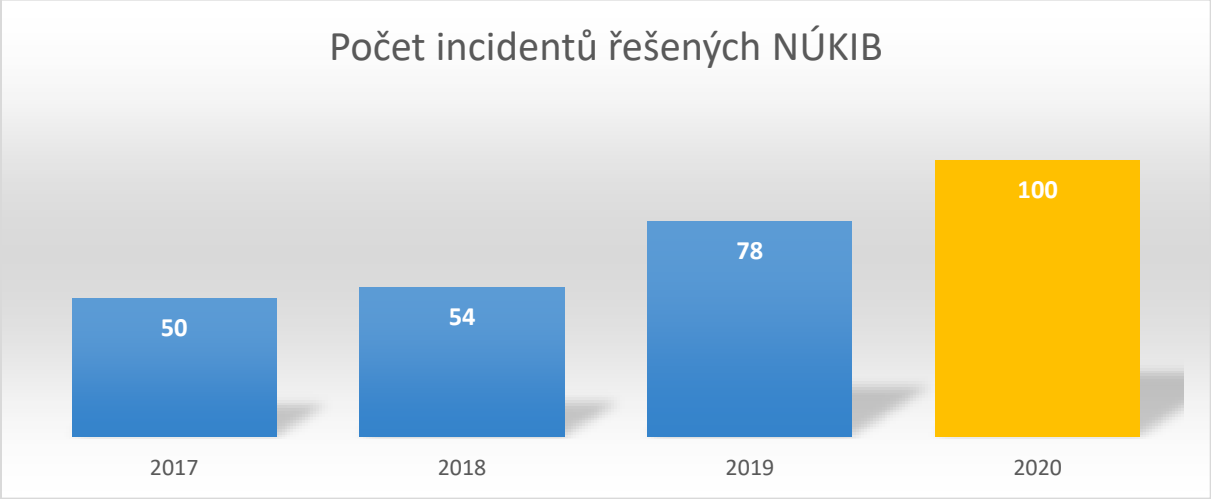
Česká republika se nachází ve stále složitějším bezpečnostním prostředí, které již několik let prochází zásadní proměnou. Velkou roli hraje kritická závislost státu a celé společnosti na moderních technologiích a kyberprostoru jako takovém. Tento trend potvrzuje kontinuální nárůst počtu systémů spadajících pod ZKB, tj. systémů, jejichž výpadek by ohrozil fungování státu a zdraví či život jeho obyvatel. Počet těchto systémů by se navíc měl zvyšovat i v následujících letech.



Obdobný trend lze sledovat i u informačních systémů certifikovaných pro nakládání s utajovanými informacemi. Jejich celkový počet je nyní 364. Z toho je 212 informačních systémů u provozovatelů z komerční sféry a 152 informačních systémů ve státní správě. Každoročně přichází cca 170 - 180 žádostí o certifikaci. Z toho je 30 - 40 nových informačních systémů, v ostatních případech se jedná o opakované certifikace. Dále z nich asi 10 - 15 každoročně zanikne (není požádáno o opakovanou certifikaci), roční nárůst je tedy o max. 15 - 20 informačních systémů.

Kromě růstu počtu systémů nezbytných pro chod státu spolu s rozmachem digitalizace společnosti rostou i kybernetické hrozby. Dochází k silnějšímu prolínání hrozeb, což umocňuje právě kyberprostor a moderní technologie. Tyto hrozby mohou narušit důvěru veřejnosti ve stát a jeho instituce a v krajních případech i stabilitu země, společnosti a demokratické uspořádání státu.

Zvýšená úroveň kybernetických hrozeb se projevuje i v podobě kontinuálního nárůstu počtu incidentů v systémech důležitých pro chod ČR.



Incidenty, které v současnosti postihují systémy důležité pro chod ČR, mohou mít značné ekonomické dopady. V případě středně velkých organizací se škody mohou pohybovat v řádu desítek miliónů korun, u velkých potom mohou dosáhnout dokonce stovek miliónů až miliard korun. Mimo ekonomických je nutné zohlednit i dopady bezpečnostní, reputační, společenské či další, ačkoli jejich vyčíslení nebo jiná kvantifikace jsou obtížnější. **Česká republika by měla být schopna takovýmto incidentům ideálně předcházet, minimálně jim však efektivně čelit a zmírňovat jejich dopady.**

Zajišťování kybernetické a informační bezpečnosti dnes výrazně přesahuje technologickou rovinu a vyžaduje ucelený přístup s důrazem na spolupráci a koordinaci zúčastněných aktérů. Diplomatická, právní, vzdělávací a další netechnická opatření jsou nezbytnými nástroji pro boj s kybernetickými hrozbami a pro budování odolné informační společnosti.

ČR se musí soustředit na aktuální problémy kybernetické a informační bezpečnosti a zároveň se musí být schopna adaptovat na nové, neustále se měnící bezpečnostní prostředí. **Lze očekávat, že význam kybernetické a informační bezpečnosti bude nadále narůstat.**

Tuto skutečnost reflektují i kroky mezinárodních organizací, zejména NATO a Evropské unie. Severoatlantická aliance na summitu ve Varšavě deklarovala kyberprostor jako další operační doménu. Evropská unie potom přijala například směrnici NIS, „kybernetický balíček“[8] nebo také Doporučení komise k bezpečnosti 5G sítí. **Z těchto aktivit na mezinárodním poli pro ČR vyplývají další povinnosti a závazky.**

Evropské státy rovněž usilují o nezávislost v oblasti družicové navigace. Konkrétním výsledkem těchto snah je služba Galileo, kterou Česká republika musí jednak administrovat pro plnění svých závazků, ale zejména by měla zajistit její plné využití (nejen) bezpečnostními složkami.

Zásadním tématem ovlivňujícím informační bezpečnost v budoucnosti, a to nejen v oblasti utajovaných informací, je oblast postkvantové kryptografie, která ovlivní kryptografii jako celek. Již v dnešní době je proto nutné se zabývat vývojem prostředků využívajících kvantově odolné algoritmy pro ochranu informací.

[8] Soubor koncepčních dokumentů a legislativních návrhů EU v oblasti kybernetické bezpečnosti.

3.2 NÚKIB a jeho role

Kybernetická bezpečnost je multioborovým fenoménem[9], **stát však musí mít instituci, která je určena pro celkovou koordinaci kybernetické a informační bezpečnosti. Tato instituce musí zabezpečit** identifikaci nejdůležitějších systémů pro stát, stanovení základních bezpečnostních opatření a procesů, návrhy na úpravu politik, regulaci, kontrolu i technickou pomoc a koordinaci při řešení kybernetických útoků na důležité systémy státu.

Stát musí mít také kapacity pro **zajištění ochrany utajovaných informací v informačních a komunikačních systémech** organizací, které nakládají s utajovanými informacemi. Zde je nutné se kromě certifikace a akreditace informačních systémů zabývat také oblastí kompromitujícího vyzařování a kryptografické ochrany. NÚKIB zde ze zákona plní roli gestora a národní autority.

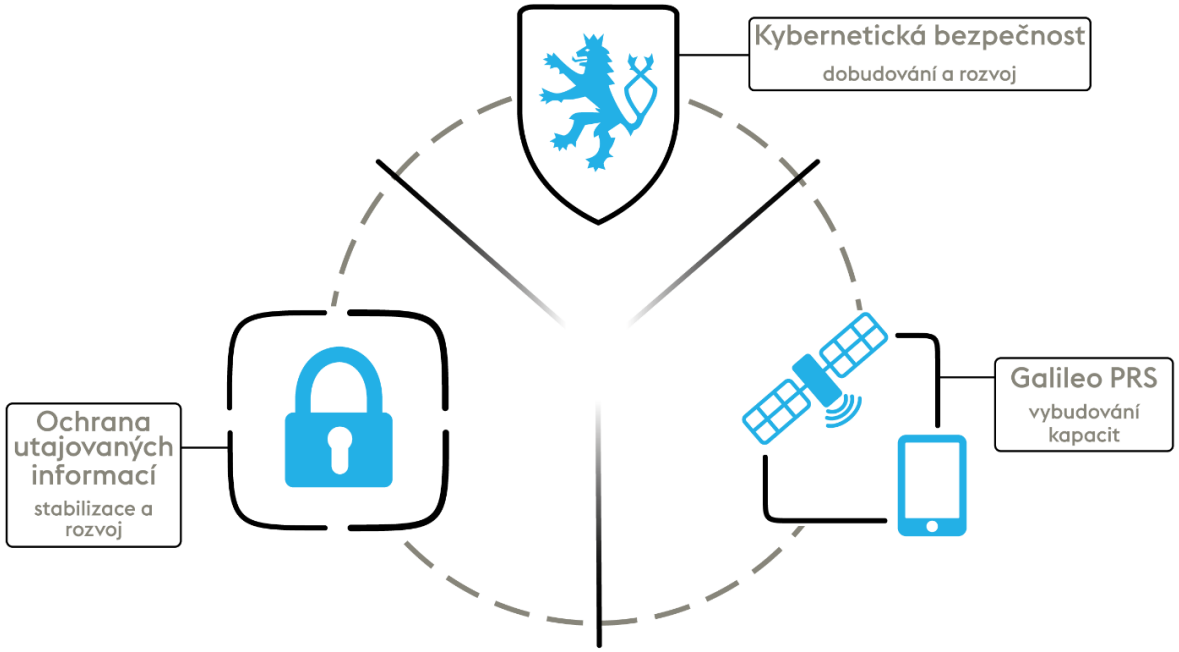
V souladu s ustanovením Rozhodnutí PRS[10] musí každý členský stát EU využívající **veřejně regulovanou službu poskytovanou systémem Galileo** (dále jen **„PRS“**)[11] ustanovit tzv. Příslušný orgán PRS odpovídající za bezpečnost PRS a řízení přístupu k této službě. V ČR tuto roli plní NÚKIB. Program Galileo má strategický význam pro nezávislost EU v oblasti družicové navigace a zejména pak PRS, která garantuje členským státům právo na neomezený a nepřetržitý přístup k této službě po celém světě. Jejím cílem je zajistit svým odběratelům dostupnost služby i v nejvážnějších krizových situacích.

NÚKIB je centrální institucí, která sdružuje výše uvedené kapacity pro oblast kybernetické a informační bezpečnosti v neutajovaných i utajovaných systémech a služby Galileo PRS.

[9] MPO – digitální ekonomika, ČTÚ – telekomunikace, MV – vnitřní bezpečnost, PČR, MZV – mezinárodní bezpečnost, diplomacie, MO – obrana státu atd.
[10] Rozhodnutí Komise v přenesené pravomoci ze dne 15. 09. 2015, kterým se doplňuje rozhodnutí Evropského parlamentu a Rady č. 1104/2011/EU, pokud jde o společné minimální standardy, které musí splňovat příslušné orgány PRS.
[11] Veřejně regulovaná služba je určena pouze státem určeným uživatelům pro kritické aplikace vyžadující nepřetržitost služby a kontrolu přístupu.

Nosné agendy NÚKIB

**Schéma znázorňující 3 pilíře činností NÚKIB.
Agendy jsou samostatné, navzájem jsou však propojené.**



Základní úkoly a role NÚKIB jsou definovány příslušnými zákony a usneseními vlády. V rámci jejich vykonávání pak NÚKIB provádí celou řadu specifických činností (plný výčet vykonávaných agend je uveden v příloze č. 1).

Poslání NÚKIB lze rámcově popsat v následujících kategoriích:

- **Expertní kapacita státu**

  NÚKIB slouží jako expertní kapacita státu pro oblast kybernetické a informační bezpečnosti.[12] Obdobně jako v jiných odvětvích bezpečnosti i v kybernetické a informační bezpečnosti potřebuje stát vlastní expertízu k zajištění nutné míry nezávislosti na třetích stranách.

- **Technická kapacita řešení a analýzy incidentů**

  NÚKIB v současné době hodnotí úroveň bezpečnosti systémů nakládajících s utajovanými informacemi a řeší případné bezpečnostní incidenty i kompromitace kryptografického materiálu.

  V souvislosti s výkonem funkce CPA[13] odpovídá NÚKIB za technické řešení implementace přístupu k PRS informacím pro definované uživatelské komunity a řeší případné bezpečnostní incidenty související s přístupem k této službě.

  Obdobně NÚKIB státu poskytuje významnou kapacitu pro řešení závažných kybernetických bezpečnostních incidentů: koordinuje výměnu informací, získává informace od partnerů, analyzuje data a doporučuje správcům opatření pro řešení problému. V případě zásadních dopadů subjektům pomáhá na místě.

[12] Pro účely tohoto textu zahrnuje pojem „kybernetická a informační bezpečnost“ všechny tři větve zaměření NÚKIB, tzn. bezpečnost utajovaných i neutajovaných systémů a PRS.
[13] **„Competent PRS Authority“** je příslušným orgánem PRS, který odpovídá za bezpečnost PRS a řízení přístupu k této službě.

- **Poskytování služeb**

  Úkolem NÚKIB je taktéž poskytovat služby, u kterých je z hlediska bezpečnosti, efektivity či specializace vhodné, aby je poskytoval sám stát. Jedná se o služby spojené s auditem plnění bezpečnostních standardů dle platných norem, penetračním testováním a hledáním zranitelností, analýzou síťového provozu a detekcí závadných komunikací, tréninkem a cvičením bezpečnostních a manažerských týmů nebo vzděláváním či metodickou pomocí a podporou.

  V případě PRS je NÚKIB ústředním orgánem státu zodpovědným za řízení a organizaci přístupu k PRS a zajišťuje nepřetržitý provoz dohledového centra PRS a utajeného spojení s bezpečnostním a monitorovacím střediskem systému Galileo.

- **Monitoring a analýza trendů**

  NÚKIB skrze monitoring a analýzu trendů v oblasti kybernetické bezpečnosti udržuje svou odbornost a zajišťuje informovanost regulovaných subjektů a dalších partnerů úřadu. Touto činností také napomáhá definovat oblasti, které vyžadují nové politiky a regulaci.

- **Tvorba strategií a politik**

  NÚKIB zpracovává návrhy k bezpečnostním strategiím či změnám politik v oblasti bezpečnosti. Tato činnost vyžaduje expertní znalost netechnických aspektů kybernetické bezpečnosti. Důležitá je také návaznost národních předpisů na předpisy a bezpečnostní standardy EU a NATO, které je nutné v národní legislativě vždy zohledňovat.

- **Regulace a podpora**

  NÚKIB provádí regulaci zejména tím, že identifikuje, případně certifikuje důležité informační a komunikační systémy, stanovuje zákonné požadavky pro zákonem definované subjekty a s těmito subjekty dále komunikuje, metodicky je podporuje a poskytuje asistenci.

- **Kontrola**

  Důležitou součástí funkčního systému zajišťování kybernetické a informační bezpečnosti je kontrola dodržování zákonných norem a bezpečnostních standardů u určených subjektů.

- **Koordinační role**

  Kybernetická a informační bezpečnost je vrstvou prolínající se ostatními sektory. Jako taková musí být koordinována napříč státními institucemi a nestátními partnery. Tuto koordinační roli v případech rozsáhlých kybernetických útoků nebo v případě tvorby nových politik kybernetické a informační bezpečnosti vykonává NÚKIB.

- **Vzdělávání a osvěta**

  Povědomí o kybernetické a informační bezpečnosti ještě stále není rozšířené jako běžná součást osobní bezpečnosti. Dále není dostatečně rozvinut systém školení a tréninků odborných pracovníků v této oblasti. Úkolem NÚKIB je proto vhodnými způsoby navyšovat povědomí o této problematice, a to jak u uživatelů či přímo pracovníků odpovídajících za bezpečnost důležitých systémů, tak u žáků a studentů i širší veřejnosti.

- **Mezinárodní spolupráce**

  Kybernetická a informační bezpečnost státu je zásadním způsobem provázána s kybernetickou a informační bezpečností mezinárodních partnerů. NÚKIB prosazuje mezinárodní spolupráci v této oblasti tak, aby co nejefektivněji přispíval k zajištění bezpečnosti ČR. Je naprosto zásadní, aby byla ČR na mezinárodním poli aktivní a mohla ovlivňovat tvorbu mezinárodních standardů a politik v rámci EU, NATO či OSN s cílem co nejlépe prosazovat své zájmy.

3.3 Současné kapacity

3.3.1 Personální kapacity

Výše uvedené agendy a činnosti uvedené v příloze č. 1 v současné době zabezpečuje 147 pracovníků, kteří jsou podporovaní dalšími 74 pracovníky zajišťujícími provozní a servisní činnosti.

S ohledem na činnosti, které NÚKIB musí zajišťovat v souladu se ZKB, ZoUI a usneseními vlády, **je současné personální zajištění nutno posílit**. Na NÚKIB se stále více obrací veřejný a soukromý sektor s **podněty a žádostmi o konzultace** v oblasti technické i netechnické expertízy kybernetické a informační bezpečnosti, mj. v analýze rizik, přípravě nové architektury sítí, bezpečnosti aplikací, zadávání zakázek v oblasti ICT, vzdělávání, specializaci na kybernetické hrozby atd. Pro uspokojení této poptávky je navýšení kapacit nezbytné.

3.3.2 Prostorové kapacity

V současné době je dislokace pracovišť NÚKIB jedním z nejpalčivějších problémů s ohledem na provoz, bezpečnost, náklady, logistiku a komunikaci mezi jednotlivými útvary. Nyní je NÚKIB umístěn v 5 lokalitách.

Současný roztříštěný stav má dopady na činnost NÚKIB v několika ohledech:

a) vysoké náklady na provoz;
b) snížená bezpečnost;
c) nedobudovaná informační a komunikační infrastruktura.

Bez ohledu na velikost potřebných prostor, která bude definována dále stanovenými směry rozvoje kapacit, je nutné zajistit vybudování jednoho pracoviště v Brně a jednoho v Praze.

3.4 Shrnutí současného stavu

S ohledem na výzvy, kterým ČR na poli kybernetické a informační bezpečnosti čelí, je **nutné kapacity pro boj se současnými i budoucími hrozbami rozvíjet** tak, aby stát dostál povinnosti zajistit občanům bezpečné prostředí.

V kontextu současné personální situace však **existuje značné riziko ztráty cenných schopností a expertízy** v případě odchodu klíčových pracovníků.

Vzhledem k výše uvedenému **je nutné zachovat koncepci a filozofii, na základě které byl NÚKIB a celý systém zajišťování kybernetické a informační bezpečnosti v ČR vybudován, a dále je rozvíjet nastoleným směrem**.

4 VÝZVY

Pro stanovení směru rozvoje NÚKIB a jeho kapacit je vedle vymezení současného stavu také potřeba identifikovat aktuální a očekávané výzvy. V tomto ohledu je zásadní otázka, jakým výzvám bude NÚKIB v následujících letech čelit.

4.1 Externí hrozby a nutnost požadované reakce

- **Růst počtu a sofistikovanosti kybernetických útoků**

  Vzhledem **k rostoucímu počtu možných cílů** a s tím souvisejících nových možností pro aktéry kybernetických hrozeb (tzv. attack surface) **lze očekávat růst počtu kybernetických útoků**. Zároveň roste **jejich sofistikovanost,** neboť státní i nestátní aktéři si čím dál více osvojují ofenzivní schopnosti v kyberprostoru. Zároveň je zde stále **nedostatečný tlak na adekvátní zabezpečení ICT služeb a produktů a** stejně tak **nedostatečná snaha mnoha správců informačních a komunikačních systémů o jejich zabezpečení.**

- **Prohlubování rozdílů v přístupu ke kybernetické a informační bezpečnosti u demokratických států a nedemokratických režimů**

  Se zaváděním nových technologií lze zejména v poslední době vidět praktické dopady **rozdílného nazírání na globální správu kybernetické bezpečnosti**, včetně (i) otázek globálních standardů pro používání nových technologií (např. 5G, IoT aj.) či (ii) reformy současně používaných standardů (např. základní protokoly, na kterých nyní běží celosvětová síť Internet). Skrze tyto diskuze jednotliví aktéři prosazují své zájmy, které mají přímý vliv na bezpečnost kyberprostoru.

  Vliv lze vidět (iii) v oblasti, jako je **normotvorba mezinárodního práva veřejného**, která vytváří rámec pro chování (zejména) států v kyberprostoru. Tato normotvorba může mít dopad na tak zásadní věci, jako je benevolentnější, či naopak restriktivnější přístup k ofenzivním činnostem v kyberprostoru, nebo naopak otázky základních lidských práv, jako je zavádění cenzury a monitorování chování jedinců v kyberprostoru.

  V neposlední řadě se jedná o (iv) arénu, kde demokratické a nedemokratické režimy **soupeří o technologickou převahu.**

  NÚKIB s ohledem na zákonné kompetence bude muset tyto změny reflektovat a ve spolupráci s MZV ČR zvýšit svou aktivitu na mezinárodním poli tak, aby byl schopen prosazovat zájmy a pozice ČR. S ohledem na respekt a prestiž, které Česká republika v oblasti kybernetické bezpečnosti doposud získala, je ovlivnění mezinárodních procesů v oblasti kybernetické a informační bezpečnosti ze strany ČR reálné.

- **Ohrožení důvěrnosti utajovaných systémů**

  Pro informační systémy určené pro nakládání s utajovanými informacemi je naprosto zásadním faktorem ochrana důvěrnosti informací. Vývoj kvantových počítačů povede k oslabení účinnosti soudobých kryptografických metod. Z toho důvodu je nutné se v oblasti výzkumu a vývoje zaměřit na vývoj prostředků používajících kvantově odolné algoritmy.

- **Výskyt nových hrozeb a fenoménů**

  V neposlední řadě lze velmi pravděpodobně očekávat dopad na celkovou úroveň kybernetické a informační bezpečnosti v důsledku **rozvoje nových technologií, ať už evolučních, nebo i přelomových (tzv. disruptivních)**. Jedná se zejména o kvantové výpočetní technologie, umělou inteligenci a její využití, bio-technologie, technologie podvrhnutí GNSS signálů, ale i takové, které v dnešní době ještě nelze předvídat.

  Tyto technologie mohou a budou hrát v budoucnosti významnou roli. Některé z nich lze již nyní identifikovat a připravovat se na ně. Příkladem může být výzkum v oblasti prostředků používajících kvantově odolné algoritmy. Je povinností státu tyto fenomény nepodcenit, aby ani v budoucnu nedošlo k ohrožení bezpečnosti obyvatel. NÚKIB bude zajišťovat jejich monitorování a předkládat návrhy řešení.

4.2 Výzvy vyplývající z digitalizace společnosti

- **Vytváření nových informačních systémů eGovernmentu a systémů státní správy**

  S ohledem na dosavadní vývoj lze předpokládat, že budou vznikat nové informační systémy eGovernmentu, ať již prostřednictvím vystavění nových služeb, nebo agregací existujících systémů či registrů. Bezpečnost bude zásadním předpokladem jejich budování. Lze proto očekávat vyšší nároky na činnosti a služby ze strany NÚKIB.

- **Porozumění problematice státních informačních a komunikačních systémů ze strany relevantních aktérů**

  S růstem důležitosti ICT a vytvářením komplexních digitálních služeb souvisí i otázka porozumění této problematice těmi, kteří při vytváření právních předpisů či politik mohou přímo ovlivnit jejich podobu a bezpečnost. Nejedná se pouze o záležitosti konceptů a architektury jednotlivých systémů, ale také o problémy spojené s hospodařením, veřejnými zakázkami, personálním zajištěním a procedurálně-právním nastavením jejich využívání.

  Na NÚKIB budou kladeny požadavky k podpoře relevantních aktérů nejen co do technických kapacit, ale také k poskytování pomoci v souvisejících oblastech a zajištění srozumitelnosti této problematiky.

- **Vývoj na poli informačních a komunikačních systémů v oblasti utajovaných informací**

  Jako výzvu lze také očekávat vývoj v oblasti informačních a komunikačních technologií nakládajících s utajovanými informacemi. Aktuálně využívané systémy vyžadují jistou míru konsolidace a zejména evoluce tak, aby vyhovovaly potřebám použitelnosti a bezpečnosti pro budoucí období. V oblasti ochrany utajovaných informací je navíc patrný trend u dodavatelů programových prostředků, kdy některé produkty přestávají být provozuschopné v off-line informačních systémech, a může tak dojít k přehodnocení současných přístupů k problematice.

5 VIZE NÚKIB

NÚKIB bude respektovaným, moderním a samostatným úřadem, jehož flexibilní a efektivní chod mu umožní plnit požadavky, jež na něj budou kladeny. Zejména bude schopen se aktivně podílet na zajištění kybernetické a informační bezpečnosti, souvisejících agend a procesů u institucí nezbytných pro chod ČR.

Jako národní autorita v daných oblastech se bude nadále zasazovat o funkční ekosystém, jehož součástí jsou zejména v oblasti kybernetické bezpečnosti aktéři privátního, akademického i veřejného sektoru. Pouze koordinováním tohoto celonárodního přístupu zapojujícího rozličné organizace lze dosáhnout funkčního systému zajišťování kybernetické a informační bezpečnosti.

Díky svým schopnostem NÚKIB zajistí včasné poskytování podpory v případě kybernetických útoků či incidentů definovaným povinným subjektům a případně dalším organizacím. Nebude působit pouze reaktivně, naopak dokáže proaktivně a kontinuálně poskytovat služby a podporu, jež povedou k navyšování odolnosti ČR v oblasti kybernetické bezpečnosti. Bude tak schopen činit prostřednictvím široké palety služeb: například konzultací, metodické podpory, penetračních testů, analytické podpory nebo cvičení.

Díky spolupráci jednotlivých celků bude NÚKIB efektivně plnit roli autority v oblasti ochrany utajovaných informací v informačních a komunikačních systémech včetně oblasti kryptografické ochrany a ochrany před únikem informací prostřednictvím kompromitujícího vyzařování na národní i mezinárodní úrovni.

NÚKIB se bude účinně podílet na vzdělávání obyvatel ČR. Bude tak schopen činit jak nepřímo (například podílením se na vzdělávacích osnovách či koncepcích), tak také přímo vzděláváním specialistů v oblastech působnosti NÚKIB, a to jak technického, tak netechnického zaměření.

Na mezinárodním poli NÚKIB dokáže proaktivně hájit a prosazovat zájmy České republiky a zvyšovat její reputaci. Bude tak činit aktivní účastí na zasedáních mezinárodních organizací či při bilaterálních jednáních stejně jako s pomocí vlastních aktivit. U klíčových partnerů a organizací tak bude činit osvědčeným způsobem – dislokací tzv. kybernetických přidělenců. Svojí činností bude nejen zvyšovat prestiž a přispívat k navýšení vlivu ČR, ale i přispívat ke stabilnímu a bezpečnému kyberprostoru.

V neposlední řadě bude NÚKIB aktivně čelit nastupujícím výzvám a trendům.

6 ROZVOJ KAPACIT DO ROKU 2027

Uplynulé období se pro NÚKIB neslo zejména v duchu pokračování nastavování systému zajišťování kybernetické bezpečnosti v ČR a vzniku a budování NÚKIB jako instituce samotné.

Kybernetická bezpečnost je na úrovni státu oproti jiným bezpečnostním oblastem, jako je obrana státu, fungování policejních složek, jaderná bezpečnost, bezpečnost letecké dopravy atd., stále ve fázi budování a vývoje. NÚKIB sice má základní pilíře činnosti nastavené, avšak značná část vyžaduje dobudování.

Zatímco v případě ochrany utajovaných informací v informačních a komunikačních systémech lze hovořit o stabilizaci a postupné evoluci činností, agendu kybernetické bezpečnosti je nutné teprve dobudovat a dále rozvíjet. Agenda Galileo PRS je před fází budování plných operačních kapacit.

Nezbytným předpokladem rozvoje NÚKIB je dostatečné **posílení současných kapacit.**

V první fázi rozvoje schopností úřadu je proto nutné jednotlivá pracoviště posílit tak, aby:

1. byla zajištěna zastupitelnost pracovníků pro vykonávání klíčových činností,[14]
2. byla zajištěna dostatečná kapacita pracovníků s cílem udržet institucionální paměť,
3. byla zajištěna minimální úroveň služeb a jejich standardů ze strany NÚKIB.

Posílení schopností je vhodné provést i s ohledem na aktuální požadavky na NÚKIB v rámci institucí státní správy. V současné době úřad často poskytuje podporu nad rámec aktuálních zákonných povinností (např. konzultace a poradenství institucím státní správy a samosprávy, nemocnicím, školám apod.). **NÚKIB se tak stává odborným pracovištěm přesahujícím původně určený záměr.** Vzhledem k vývoji hrozeb je však důležité, aby byl NÚKIB schopen i nadále podobnou podporu poskytovat.

6.1.1 Ochrana utajovaných informací

Ochrana utajovaných informací v informačních a komunikačních systémech je velmi významným pilířem národní, evropské a mezinárodní bezpečnosti. Její kvalita podstatně ovlivňuje skutečnost, zda budeme nadále úspěšní v boji proti současným vnějším a vnitřním bezpečnostním hrozbám souvisejícím s rostoucím extremismem, hrozbou teroristických útoků (včetně kyberterorismu) a s činností některých zahraničních zpravodajských služeb proti zájmům ČR, EU a NATO.

Dlouhodobou strategií ochrany utajovaných informací v ČR je systematické zavádění procesů řízení informační bezpečnosti vycházejících z mezinárodně uznávaných standardů a nejlepších praktik pro řízení bezpečnosti informací.

V současné situaci je nutno minimálně udržet schopnosti, které NÚKIB má a ve kterých je unikátní. Jedná se zejména o (i) zkušenosti v oblasti TEMPEST a (ii) kryptologie, které jsou navíc oceňované i u spojenců v NATO.

Tyto oblasti jsou vzájemně provázány a zastřešuje je problematika certifikací, resp. akreditací informačních systémů. NÚKIB tyto činnosti vykonává v kontextu členství v mezinárodních organizacích v rámci plnění rolí IAA (Information Assurance Authority), TA (TEMPEST Authority), CAA (Crypto Approval Authority), CDA (Crypto Distribution Authority) a SAA (Security Accreditation Authority), resp.

[14] Klíčovými činnostmi se rozumí činnosti, které (i) jsou specificky vyžadované k plnění zákona, nebo (ii) jsou zásadní pro zajištění základních funkcí NÚKIB.

NCSA (National CIS Security Authority), a také v rámci bilaterální spolupráce s jednotlivými národními partnery.

V oblasti kryptografické ochrany čeká NÚKIB řada výzev. Mezi ty významné bude patřit: analýza uživatelských potřeb; zajištění kryptografické ochrany novými generacemi prostředků a plán jejich obměny; koncepce zabezpečení skrze národní prostředky; vytvoření národního certifikačního schématu kryptografických prostředků aj. Neméně podstatná je také spolupráce se zpravodajskými službami a rezorty Ministerstva vnitra, Ministerstva obrany, Ministerstva zahraničních věcí a NBÚ, která je nutná pro definici uživatelských požadavků a nalezení shody na potřebných změnách.

6.1.2 Galileo PRS

Program Galileo je jedním komponentem evropského kosmického programu, jehož cílem je vybudování autonomního globálního navigačního družicového systému zejména pro potřeby občanů EU a jednotlivých členských států. Kromě otevřené služby, která je dostupná široké veřejnosti počítá program Galileo i se službou PRS, která je určená autorizovaným uživatelům, zejména bezpečnostním složkám, integrovanému záchrannému systému a dalším stanoveným subjektům. Tato služba garantuje mimo jiné nepřetržitý provoz, zvýšenou odolnost proti rušení signálu a vysokou přesnost.

Program Galileo se v současnosti nachází ve fázi zprovozňování služeb (tzv. Initial Services), které zahrnují pouze otevřenou službu, PRS a Search and Rescue službu v omezeném provozu. Nepřetržité celosvětové pokrytí v této fázi program Galileo negarantuje. NÚKIB plní funkci příslušného orgánu PRS (Competent PRS Authority, CPA) a hlavním cílem rozvoje kapacit NÚKIB je dosažení jeho plných operačních schopností.

Dosažení počátečních operačních schopností (IOC – Initial Operational Capabilities) a následně i plných operačních schopností (FOC – Full Operational Capabilities) bude v souladu s upřesněnými požadavky na fungování CPA vyžadovat navýšení počtu pracovníků a vybudování potřebné infrastruktury. To mimo jiné obnáší zřízení a provoz dohledového centra PRS, které bude v nepřetržitém (24/7) spojení s bezpečnostním a monitorovacím centrem programu Galileo.

6.1.3 Regulace dle ZKB

Pro plnění hlavního účelu NÚKIB je jedna z klíčových agend regulace dle ZKB. V rámci této agendy dochází zejména k (i) určování KII a PZS, (ii) koordinaci identifikace VIS, (iii) stanovování bezpečnostních opatření pro regulované subjekty, (iv) vydávání opatření dle ZKB (varování, reaktivní opatření, ochranná opatření), (v) nastavování regulatorního rámce a koordinace s ostatními regulátory, (vi) metodické pomoci atd.

Vzhledem ke skutečnosti, že se systém kybernetické bezpečnosti v ČR stále vyvíjí, dochází k vývoji počtu regulovaných subjektů, ať už změnou politiky státu nebo prostřednictvím implementace evropské legislativy. Předpokládáme, že v následujících letech by mělo přibýt dalších 300 regulovaných subjektů, přičemž počet určených systémů se může pohybovat mezi 700 až 1000 v závislosti na stanovených kritériích.

Je nutné posílit agendu regulace alespoň tak, aby plnila základní povinnosti ze zákona a aby byl NÚKIB nadále schopen zajistit alespoň minimální standard služeb poskytovaný regulovaným subjektům. To obnáší (i) schopnost komunikovat a konzultovat problémy spojené s nastavováním správy kybernetické bezpečnosti, (ii) poskytovat metodickou pomoc a podporu, (iii) vytvářet podpůrné materiály, které jednotlivým institucím pomohou při zajišťování kybernetické bezpečnosti, (iv)

spolupracovat a koordinovat svou činnost s dalšími regulátory na národní i evropské úrovni a (v) sledovat vývoj stavu využití a zabezpečení důležitých informačních a komunikačních systémů v ČR. Podstatná je také účast na jednání sektorových skupin a platforem, aby nebyl regulátor izolován od problémů správců v jednotlivých sektorech.

6.1.4 Kontrola a audit dle ZKB

Na kontrolu dle ZKB je nutné pohlížet nejen jako na represivní činnost, ale naopak zejména jako na preventivní pomoc povinným osobám s cílem předejít kybernetickým bezpečnostním incidentům. V rámci kontroly totiž dojde k popsání současného stavu systémů a odhalení nedostatků v jejich zabezpečení. Identifikované nedostatky pak povinná osoba odstraní, a tím dojde k posílení kybernetické bezpečnosti u kontrolovaných systémů a zvýšení kybernetické bezpečnosti České republiky jako takové.

V rámci kontroly by mělo docházet k rozšířené metodické pomoci subjektům a ke konzultacím, jak dále naplňovat požadavky ZKB s ohledem na co největší efektivitu. Množství kontrol, metodické pomoci a konzultací je vzhledem k narůstajícímu počtu regulovaných subjektů nedostatečné. Je proto nutné posílit lidské zdroje směrem k těmto službám.

6.1.5 Provoz Vládního CERT

Vládní CERT je specializovanou součástí NÚKIB určenou pro technickou stránku problematiky kybernetické bezpečnosti. Jeho činnost se vyznačuje vysokou různorodostí a množstvím poskytovaných služeb. Vládní CERT je specifický značnou provázaností jednotlivých odborných činností.

V rámci posílení současných kapacit k plnění aktuálních kompetencí a úkolů jsou identifikovány čtyři níže uvedené oblasti.

6.1.5.1 Zvládání incidentů

Zvládání incidentů je klíčovou službou NÚKIB v oblasti kybernetické bezpečnosti. Pracovníci podporující tuto činnost jako první přijímají hlášení o vzniku incidentu, zpracovávají ho a poskytují okamžitou pomoc napadeným subjektům. Dále zodpovídají za mezinárodní komunikaci zejména se svými protějšky, která je vzhledem k přeshraničnímu přesahu problematiky kybernetické bezpečnosti velmi intenzivní. Ač pro to nejsou určeny zvláštní prostředky, mohou být v případě závažných kybernetických incidentů tito pracovníci spolu s pracovníky souvisejících agend fyzicky vysláni k napadenému subjektu.

V rámci agendy zvládání incidentů by se z důvodu potřeby komplexní informovanosti o incidentech a jejich dopadech měla vytvořit pokročilá analytická kapacita pro vyhledávání hrozeb (tzv. Cyber Threat Intelligence). Tato operační vrstva by měla propojovat již existující technické a strategické analytické kapacity úřadu.

6.1.5.2 Forenzní analýza a analýza škodlivého kódu

Analytici Vládního CERT pomáhají zejména s řešením kybernetických incidentů, kdy vyvstává potřeba forenzní analýzy zjištěného kybernetického bezpečnostního incidentu a následné analýzy identifikovaného škodlivého kódu. Vyžaduje-li to situace, pomáhají zasažené instituci se zajištěním potřebných dat pro analýzu přímo v místě vzniku incidentu. V souvislosti s incidenty dále poskytují součinnost a spolupráci partnerům, a to zejména Policii ČR a zpravodajským službám.

Vzhledem k předpokladu, že se budou počty incidentů do budoucna zvyšovat, je potřeba i personálně rozšířit počet těchto pracovníků. Personální posílení povede ke zvládání většího počtu analýz nahlášených bezpečnostních incidentů a podpoře dalších projektů.

6.1.5.3 Penetrační testování

Penetrační testování patří mezi základní služby, jež NÚKIB nabízí povinným subjektům. Od skenu zranitelností se odlišuje tím, že se snaží aktivně prolomit zabezpečení testovaných systémů. Cílem této aktivity je odhalit možné zranitelnosti a slabá místa v infrastruktuře testovaných subjektů dříve, než budou odhalena a zneužita útočníky. NÚKIB ve výsledné zprávě doporučuje kroky k nápravě nedostatečného zabezpečení. Na základě dohody s testovaným subjektem se může jednat o externí či interní penetrační testování nebo o testy specifické, které mohou zahrnovat testy na míru, např. testy mobilních aplikací nebo specifických zařízení.

Vzhledem ke klíčovému významu této agendy je nutné zajistit růst počtu pracovníků zodpovědných za její plnění v následujících letech.

6.1.5.4 Analýza síťového provozu

Mezi základní služby v rámci síťové analýzy patří detekce škodlivých aktivit v síťovém provozu. K tomuto účelu využívají pracovníci zajišťující analýzu síťového provozu vlastní centrální analytický software, který byl vybudován v rámci projektu systému detekce, a také výstupy z projektu Honeypot. Oba tyto projekty jsou aktuálně ve fázi rozvoje a dalšího rozšiřování. Další velmi důležitou agendou je síťová forenzní analýza v rámci řešených kybernetických incidentů, s čímž souvisí i nutnost přípravy mobilních síťových sond využitelných při výjezdu k incidentům. Pro zajištění dostatečných znalostí a zkušeností pracovníků je vhodné, aby na denní bázi pracovali v dané oblasti. Přestože se jedná o velmi důležitou činnost, současné kapacity ji umožňují řešit pouze okrajově.

V případě projektu systému detekce je nutné personální posílení, aby mohlo být zajištěno plynulejší a efektivnější zapojování nových partnerů a byla s nimi zajištěna užší spolupráce při analýze dat. Také je nutné posílit kapacity k zajištění hlubších analýz prováděných nad detekovanými daty.

6.1.5.5 Další expertíza a vývoj nástrojů

Vládní CERT vykonává celou řadu povinností a služeb pro regulované i neregulované subjekty (např. nemocnice, mobilní operátory, banky atd.). Vyjma výše uvedených služeb se jedná o nabídku aktuálně připravovaných projektů (např. projekt neveřejného kanálu pro sdílení informací napříč povinnými subjekty apod.) nebo služby a expertízy v dalších oblastech kybernetické bezpečnosti (sledování a analýza informací o kybernetických hrozbách a zranitelnostech, vývoj vlastních nástrojů, expertíza na různé operační systémy a v neposlední řadě vývoj vlastního prostředí pro technické cvičení CyberCzech atd.). Pracovníci Vládního CERT dále podporují kontrolní činnost či aktivity v oblasti tvorby politik.

Vzhledem k významu výše uvedené agendy je nutné kapacitu NÚKIB v této oblasti posílit.

6.1.6 Kybernetické bezpečnostní politiky

6.1.6.1 Národní kybernetické bezpečnostní politiky

Vzhledem k tomu, že kybernetická a informační bezpečnost prostupuje množstvím různých oborů a sektorů, je nutné zajistit řádnou koordinaci. Zároveň lze identifikovat trend, kdy dříve nezávislé sektory vyžadují od NÚKIB koordinaci v těch případech, kdy se sektorová problematika prolíná s kybernetickou bezpečností. To však znamená značný nárůst vstupů, podnětů a žádostí o konzultaci

či koordinaci ze strany NÚKIB. Klade to také vysoké nároky na pracovníky, kteří musí mít všeobecný odborný přehled od technické stránky fungování kyberprostoru, přes právní a regulační mechanismy, sektorová specifika, až po oblast geopolitiky a mezinárodních vztahů.

Vzhledem k významu výše uvedené agendy je nutné kapacitu NÚKIB v této oblasti posílit.

6.1.6.2 Mezinárodní kybernetické bezpečnostní politiky

V případě mezinárodní spolupráce v oblasti kybernetické bezpečnosti lze taktéž pozorovat silný narůstající trend v počtu nutných či potřebných aktivit. Zatímco ještě v roce 2015 byla aktivita na mezinárodní či evropské úrovni spíše menší, v současné době se kybernetická bezpečnost řeší na značném počtu platforem a mezinárodních organizací. Z nich vycházejí normy a standardy, které mají zásadní dopad na koncepci a finanční náklady zajištění kybernetické bezpečnosti v ČR. Příkladem lze uvést evropskou směrnici NIS nebo uplatňování stávajícího mezinárodního práva veřejného v oblasti kybernetické bezpečnosti. V případě úspěšných vyjednávání lze tyto iniciativy ovlivnit ještě v průběhu jejich tvorby a promítnout tak do nich české pozice, případně zabránit finančně nákladným opatřením, která by byla nevhodná v prostředí ČR.

V současné době jsou kapacity pro tvorbu a udržování českých pozic v zahraničí rozděleny mezi vícero organizačních částí NÚKIB, přičemž i nadále platí, že hlavní koordinační roli v mezinárodních aktivitách sehrává Ministerstvo zahraničních věcí. Organizační části NÚKIB jsou odpovědné zejména za (i) věcnou přípravu pozic a zastupování NÚKIB, potažmo ČR, na odborných skupinách a dále se orientují na (ii) zastupování NÚKIB přímo v zahraničí a prosazování definovaných pozic k bilaterální spolupráci mezi NÚKIB a zahraničními partnerskými institucemi.

Vzhledem k současné zátěži (i s ohledem na chystané předsednictví ČR v Radě EU, kde bude kybernetická bezpečnost jedním z důležitých témat) je do roku 2027 potřebné tuto kapacitu dále posílit.

6.1.7 Analytika

Robustní analytické kapacity jsou předpokladem efektivního plnění kompetencí NÚKIB. Jedná se o kapacity, které slouží k (i) udržování a získávání poznatků o současných či nových kybernetických hrozbách, (ii) kontextualizaci řešených incidentů, (iii) informování partnerů a nadřízených orgánů, (iv) řádné tvorbě politik a návrhů změn legislativy založených na faktech a analýzách. Za stavu zahlcení veřejného prostoru informacemi jsou velmi důležité vlastní kapacity, které pomohou vstupní data zpracovat tak, aby na jejich základě bylo možné činit rozhodnutí.

Aby byl NÚKIB dále schopen data přijímat, analyzovat a řádně vyhodnocovat, je nutné analytickou kapacitu posílit.

6.1.8 Prověřování služeb cloudových dodavatelů

Na základě aktuálně platného znění zákona č. 365/2005 Sb., o informačních systémech veřejné správy se předpokládá, že NÚKIB bude posuzovat bezpečnostní požadavky na poskytovatele cloudových služeb, kteří budou dodávat služby poskytovatelům informačních systémů veřejné správy (dále jen „ISVS“).

Prověřování bude vyžadovat nejen pracovníky s technickou specializací, ale také pracovníky se znalostí technických a právních norem a dále analytické pracovníky pro sběr a korelaci veřejně dostupných informací pro řádné ověření prověřovaných údajů.

Chybné vyhodnocení bezpečnostní způsobilosti dodavatele cloudové služby může znamenat vážné ohrožení bezpečnosti státních systémů, tudíž nelze tuto velmi komplexní problematiku podceňovat. V tomto ohledu bude nutné posílit kapacity NÚKIB k prověřování bezpečnostní způsobilosti dle nastavených parametrů celého procesu.

6.1.9 Efektivní vymáhání plnění zákonných povinností

Navazující činností na výše uvedené oblasti kybernetické bezpečnosti a ochrany utajovaných informací je provádění kontrolní činnosti. Jejím cílem je zvyšování kybernetické bezpečnosti a identifikace nedostatků při plnění zákonných povinností, které je nutno efektivně vymáhat, k čemuž může sloužit mimo jiné pravomoc úřadu pokutovat přestupky.

Ustanovení zákona o přestupcích obsahuje jak ZKB, tak ZoUI. Vzhledem k tomu, že NÚKIB spravuje celou oblast vymezenou v ZKB, týká se jeho působnost i celé přestupkové agendy definované tímto zákonem. V rámci ZoUI je dozorová činnost dělena mezi NÚKIB a NBÚ. V souladu s tímto rozdělením pak NÚKIB projednává přestupky týkající se nakládání s utajovanými informacemi v informačních a komunikačních systémech a záležitosti kryptografické ochrany.

V návaznosti na rozvoj kapacit v oblasti kybernetické bezpečnosti, zejména na úseku regulace a kontroly, se předpokládá nárůst počtu prováděných kontrol a s tím související nárůst počtu kontrolních zjištění a možných porušení zákona. V současné době je agenda přestupků vykonávána pracovníky odboru právního, kteří zajišťují i další činnosti nezbytné pro chod NÚKIB. S ohledem na vývoj a požadavky kladené na NÚKIB v rámci této agendy je vhodné ji kapacitně posílit.

6.1.10 Vzdělávání

V oblasti vzdělávání vykonává NÚKIB aktivity, které mají přispívat k postupnému navyšování povědomí o problematice kybernetické bezpečnosti, a to jak z běžného uživatelského hlediska, tak z hlediska odborných znalostí. Doposud se NÚKIB soustředil zejména na rozvoj vlastních vzdělávacích projektů a osvětových kampaní.

Agenda vzdělávání je NÚKIB svěřena zákonem o kybernetické bezpečnosti. I s ohledem na vyvíjející se hrozby, které z velké části využívají právě omezených znalostí problematiky běžnými uživateli, se jedná o jednu ze zásadních strategických činností, které v dlouhodobém horizontu mohou mít znatelný dopad na celou kybernetickou bezpečnost České republiky.

NÚKIB by měl své současné know-how dále co nejefektivněji využít, ať již formou vylepšování on-line kurzů a zlepšování existujícího vzdělávacího portálu, podpory vzdělávacích institucí při vytváření oborů zaměřených na kybernetickou a informační bezpečnost a dalších vzdělávacích projektů. S tím souvisí i dostatečná spolupráce a podpora na osvětových akcích a kampaních v této oblasti, zejména těch, které jsou pořádány partnery a dalšími třetími stranami.

S ohledem na vývoj a požadavky kladené na NÚKIB v rámci této agendy (koncepční, komunikační, pedagogické i vývojové) je vhodné ji kapacitně posílit.

6.1.11 Výzkum

NÚKIB má dle ZKB také zajišťovat výzkum a vývoj v oblasti kybernetické a informační bezpečnosti. Úkol zabývat se vědou a výzkumem vyplývá jak ze zákona, tak z příslušných bodů schváleného Akčního plánu k Národní strategii kybernetické bezpečnosti. Po relativně dlouhé období byla tato agenda z důvodu nedostatku kapacit pouze udržována a nebyla rozvíjena tak, jak bylo při přijímání ZKB původně zamýšleno.

V uplynulém období však úřad vytvořil základní kapacity pro řešení agendy vědy a výzkumu a jejich koordinaci na národní i mezinárodní úrovni a vypracoval *Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti* tak, aby se koncentrovaly veřejné výzkumné prostředky do reálně uplatnitelných produktů kybernetické bezpečnosti s vysokou přidanou hodnotou. NÚKIB tak převzal aktivnější roli v této agendě, bude dále prosazovat prioritní výzkumná témata určená Národním plánem a informovat o výzkumu a vývoji v kybernetické a informační bezpečnosti jak firmy, tak akademická pracoviště a veřejnou správu. NÚKIB také aktivně propojuje potenciální partnery na národní i evropské úrovni, organizuje zahraniční výzkumné mise, informuje o jednotlivých výzkumných výzvách a vysvětluje, jak se do nich zapojit.

V rámci připravovaného unijního nařízení o Evropském centru kompetence kybernetické bezpečnosti bude NÚKIB plnit roli Národního koordinačního centra, zapojovat soukromý i veřejný sektor do mezinárodních výzkumných a inovačních projektů či rozdělovat granty v rámci programů Horizont Evropa (plánovaných 100 mld. EUR) a Digitální Evropa (plánovaných 8,2 mld. EUR).[15]

Z výše uvedených důvodů je důležité kapacitu NÚKIB v této oblasti posílit.

6.1.12 Certifikace

V souvislosti s blížící se účinností nařízení EU Cyber Security Act, které mimo jiné zavádí systém evropských certifikací kybernetické bezpečnosti produktů, procesů a služeb, bude NÚKIB zastávat roli vnitrostátního orgánu certifikace kybernetické bezpečnosti. Do roku 2025 chce v této oblasti napomoci vzniku sítě českých komerčně úspěšných středisek nalézání shody (*CAB – Conformity Assesment Bodies*), u kterých si budou zákazníci objednávat vydání různých druhů EU bezpečnostních certifikací. Certifikovat se budou výrobky, služby a procesy kybernetické bezpečnosti. Z toho plyne, že CAB se může stát široké spektrum českých institucí od právních pracovišť až po technicky orientované laboratoře.

Z výše uvedených důvodů je nutné kapacitu NÚKIB v této oblasti posílit.

6.1.13 Činnost kabinetu ředitele

Kabinet ředitele NÚKIB má ve své gesci legislativní, vládní a parlamentní agendu, agendu související s činností Bezpečnostní rady státu (BRS) a jejími stálými pracovními výbory, agendu komunikace, mezinárodní spolupráci a řízení kybernetických přidělenců[16] a pracovníků úřadu, kteří byli vysláni jako národní experti do mezinárodních organizací.[17] Zároveň zajišťuje funkci sekretariátu Výboru pro kybernetickou bezpečnost (stálý pracovní výbor BRS) a dále Rady pro kybernetickou bezpečnost (poradní orgán předsedy vlády pro otázky kybernetické bezpečnosti).

[15] "Horizon Europe - the next research and innovation framework programme." European Commission - European Commission, 1. března 2018, ec.europa.eu/info/horizon-europe-next-research-and-innovation-

[16] Kybernetičtí přidělenci jsou pracovníci úřadu, kteří jsou na základě dohody mezi NÚKIB a MZV vysíláni na zastupitelské úřady ČR.

[17] V současné době úřad vyslal své zástupce do NATO Cooperative Cyber Defence Center of Excellence v Tallinu a do Evropské agentury kybernetické bezpečnosti ENISA.

6.1.13.1 Mezinárodní spolupráce a kybernetičtí přidělenci

V mezinárodní oblasti vykonává NÚKIB vedle tvorby politik a pozic také role spojené s vedením bilaterální a multilaterální spolupráce s partnerskými úřady, s kontakty se zahraničními zastupitelskými úřady a se zajišťováním působení pracovníků NÚKIB v zahraničí v rámci krátkodobých i dlouhodobých výjezdů.

Intenzita a význam mezinárodní spolupráce v poslední době výrazně narůstají (ať již ve formě (i) navázaných pracovních vztahů, díky nimž dostává NÚKIB včas informace o kybernetických hrozbách, které jsou dále analyzovány a předávány na národní úrovni, nebo také (ii) schopnosti ovlivnit tvorbu mezinárodních norem, standardů dle zájmů České republiky).

S tím souvisí také činnost kybernetických přidělenců a pracovníků vyslaných na pozici národních expertů do mezinárodních organizací. Tento koncept se ukázal jako přínosný. S ohledem na skutečnost, že spolupráce v oblasti kybernetické bezpečnosti se dynamicky rozvíjí i s dalšími státy, by bylo vhodné vytvořit pozici kybernetických přidělenců i na dalších zastupitelských úřadech.

Vysíláním národních expertů do mezinárodních organizací úřad s těmito sdílí svoji expertízu a znalost. Zároveň má možnost prostřednictvím svých pracovníků činnost těchto organizací ovlivnit a získávat poznatky důležité pro činnost NÚKIB.

6.1.13.2 Legislativa a vládní agenda

Pro NÚKIB vyplývají povinnosti z jeho členství ve stálých pracovních výborech Bezpečnostní rady státu a povinnosti související s komunikací s dalšími vládními a zákonodárnými platformami. Aktivita a komunikace v rámci těchto platforem v poslední době značně narůstá, a to zejména s růstem důležitosti problematiky kybernetické bezpečnosti, větším počtem kybernetických hrozeb, incidentů a zájmem politické reprezentace o toto téma.

Narůstá množství zákonných úprav, které se dotýkají problematiky kybernetické a informační bezpečnosti, přičemž lze důvodně očekávat trvání, či dokonce posílení tohoto trendu. Tento nárůst je navíc patrný jak na národní úrovni, tak i na úrovni Evropské unie. Důsledkem tohoto vývoje je zvýšený počet legislativních návrhů, které musí NÚKIB vytvářet nebo se k nim vyjadřovat a pracovat s nimi.

S ohledem na výše zmíněné je nutné oddělení posílit.

6.2 Provozní a podpůrné agendy

6.2.1 Interní informační a komunikační infrastruktura

Nároky kladené na interní informační a komunikační infrastrukturu jsou a budou u instituce typu NÚKIB vysoké. Interní infrastruktura musí poskytnout dostatečně robustní prostředí pro zabezpečení různorodých činností, které NÚKIB vykonává. Nároky kladené na infrastrukturu nebudou pramenit pouze z její komplexity, ale s ohledem na citlivou povahu informací, které pracovníci zpracovávají a komunikují, také ze zvýšených nároků na bezpečnost. Primárním cílem v této oblasti bude dobudovat základní infrastrukturu úřadu.

Pro dobudování NÚKIB je nutné doplnit pracovníky zabývající se interní informační a komunikační infrastrukturou.

6.2.2 Bezpečnost

Bezpečnost je klíčovým předpokladem činnosti NÚKIB. V rámci prováděných aktivit dochází ke sběru, vytváření, zpracovávání i komunikaci značného počtu informací citlivé povahy a informací utajovaných, které jsou pro některé celky běžnou denní agendou.

Vedle fyzické, personální, administrativní a informační bezpečnosti v oblasti utajovaných informací je nutným předpokladem pro řádné dobudování kapacit i nutnost zajistit dostatečné plnění rolí v oblasti kybernetické bezpečnosti. NÚKIB musí jít příkladem, pokud jde o kybernetickou a informační bezpečnost.

Při současných kapacitách a nárocích, které jsou dále ztíženy i roztříštěností lokalit a v některých případech i neodpovídajícím zázemím, je zajišťování bezpečnosti NÚKIB komplikované.

I z těchto důvodů je nutné podpořit tuto činnost posílením personálních i technologických kapacit.

6.2.3 Personalistika a vnitřní organizace

S ohledem na vývoj v oblasti kybernetické a informační bezpečnosti a na velmi omezený počet odborníků na trhu práce je personální a náborová politika zásadní výzvou pro budoucí fungování NÚKIB.

Aby bylo možné dobudovat kapacity pro výkon potřebných kompetencí a činností, je nutné umět získat a udržet příslušné odborníky, ale také mít schopnost a možnost pracovníky vzdělávat, trénovat a školit. Bez těchto předpokladů nebude NÚKIB schopen vykonávat jemu svěřené úkoly ani v případě plného tabulkového naplnění.

Z výše uvedených důvodů je klíčové vytvořit dostatečné kapacity náboru, které budou schopny proaktivně zajišťovat nábor pracovníků, včetně činností, jako je komunikace s vysokými školami, zajišťování stáží, aktivita v rámci personalistických platforem a veletrhů atd., což jsou v současnosti nezbytné aktivity pro získání nových pracovníků.

6.2.3.1 Interní vzdělávání

Nad rámec výše uvedeného je nutné vytvořit kapacity, které budou koordinovat vzdělávání, trénink a další rozvoj pracovníků. NÚKIB by měl disponovat schopností své zaměstnance interně vzdělávat.

Aktuální působnost NÚKIB jde napříč mnoha agendami, což vede k pestré skladbě činností, jež úřad vykonává. Tyto činnosti jsou přitom často navzájem provázány a k jejich vykonávání jsou nutné znalosti a dovednosti jak v technických, tak netechnických oborech. Pracovníci také potřebují mít povědomí a udržovat si často hluboké porozumění činnostem vykonávaných svými kolegy na jiných celcích. NÚKIB v současnosti disponuje řadou úzce zaměřených specialistů, kteří k udržení svých kompetencí potřebují kontinuální odborné vzdělávání. Lze předpokládat, že i v budoucnu bude nutné těmto pracovníkům zajišťovat domácí i zahraniční školení.

6.2.4 Ekonomika

Posílení kapacit k plnění současných kompetencí a úkolů se nutně dotkne také hospodaření NÚKIB.

S tím bude souviset i posílení kapacit vykonávajících ekonomické agendy, na které bude růst celého úřadu taktéž dopadat.

6.2.5 Právní podpora

Pro fungování NÚKIB je klíčová i řada provozních právních agend, například administrace zadávacích řízení v režimu zákona o zadávání veřejných zakázek či postupů pod tento zákon nespadajících.

Dále se jedná o oblast smluvního zajištění veškerých projektů v rámci NÚKIB. Vedle smluv obchodního charakteru se jedná o úzkou spolupráci v pracovněprávní agendě, řešení problematiky ochrany osobních údajů (GDPR) ve spolupráci s pověřencem pro ochranu osobních údajů, přípravu memorand i jiných mimosmluvních dokumentů, zastoupení v projektových týmech úřadu i zpracovávání interních předpisů úřadu a podpůrnou a metodickou činnost pro ostatní organizační celky. NÚKIB dále vyřizuje žádosti o informace podle zákona č. 106/1999 Sb. a další podání občanů, vč. uplatnění nároku na náhradu škody dle zák. č. 82/1998 Sb. V neposlední řadě je součástí agendy zastupování NÚKIB v řízeních před soudem a jinými orgány státu v občanskoprávním, správním nebo trestním řízení.

S ohledem na vývoj a požadavky kladené na NÚKIB v rámci této agendy je vhodné ji posílit.

6.2.6 Komunikace s veřejností

NÚKIB průběžně komunikuje při výkonu své činnosti jak se svými národními či mezinárodními partnery, tak také s povinnými subjekty, médii, veřejností či dalšími organizacemi. Kvalitní interní i externí komunikace představuje základ při budování důvěry a udržení prestiže u široké i odborné veřejnosti. Komunikace se také významnou měrou podílí na náboru nových pracovníků úřadu a má přesah i do dalších oblastí činnosti, například při vysvětlování konkrétních kroků úřadu.

Vzhledem k permanentnímu nárůstu objemu agendy NÚKIB bude nevyhnutelně narůstat i objem práce oddělení komunikace, které k jejímu výkonu bude potřebovat adekvátní personální i materiální zajištění.

Z těchto důvodů je potřebné posílit kapacity NÚKIB i v této agendě.

6.2.7 Projektové řízení

Mnohé aktivity úřadu jsou natolik komplexní a unikátní, že dochází k jejich realizaci formou projektů. Jedná se kupříkladu o potenciální stavbu nového sídla, budování a obnovu infrastruktury, projekt Honeypot nebo analýzy síťového provozu prostřednictvím sond. Vzhledem k významu, složitosti a nutnosti spolupráce více organizačních celků je u podobných projektů žádoucí, aby byly řízeny kvalitními projektovými manažery s potřebnou kvalifikací a zkušenostmi. Tito budou sdruženi v projektové kanceláři úřadu. Pokud by projekty byly vedeny nekvalitně, dojde k ohrožení jejich termínů, kvality nebo dohodnutých nákladů. NÚKIB v současnosti disponuje několika projektovými manažery, kteří řídí jeho projekty a prokazují opodstatněnost a efektivnost své specializace. Vzhledem k plánovanému nárůstu činností NÚKIB lze očekávat i nárůst počtu projektů – je tedy vhodné adekvátně navýšit kapacity projektového řízení a poskytnout jim potřebná školení, projektový software a další nástroje.

V návaznosti na výše uvedené je nutné posílit počet pracovníků v této agendě.

7 SMĚR DALŠÍHO ROZVOJE

Vedle posílení kapacit současných činností je nutné i nastolit směr dalšího rozvoje činnosti NÚKIB. Jedná se o aktivity či projekty, které bude nezbytné v budoucnu dále posilovat a rozvíjet mimo jiné z hlediska (i) nových či očekávaných kompetencí, či z hlediska (ii) řádného výkonu státní správy a s cílem co nejefektivněji čelit výzvám, které Českou republiku na poli kybernetické a informační bezpečnosti čekají.

Rozvoj těchto aktivit či projektů jde nad rámec výše uvedených činností. Jejich realizace bude závislá na dostupných personálních a finančních zdrojích.

Zatímco některé z uvedených činností bude možné rozvíjet v rámci kapacit vybudovaných do roku 2027, jiné je nutné spíš považovat za výhled činností přesahující stanovený rámec.

7.1 Kapacity pro řešení nových hrozeb

Kdy: průběžně od 2022

Požadavky: personální kapacity v podobě vyhrazených pracovníků, technické zázemí pro testování, funkční kooperaci zejména s akademickým a soukromým sektorem

Kybernetická bezpečnost a oblast informačních technologií obecně je silně dynamický obor. Již od svého počátku je charakteristický neustále se vynořujícími novými trendy a technologiemi. Ty mají mnohdy zásadní vliv na celý obor a mají potenciál ho do značné míry proměnit. V současnosti se jedná kupříkladu o:

a. umělou inteligenci;
b. kvantové počítače a s tím související post-kvantovou kryptografii a kvantovou komunikační infrastrukturu;
c. bio-technologie;
d. bio-hacking;
e. bezpečnostní systémy založené na umělé inteligenci a strojovém učení;
f. drony a další robotická, autonomní zařízení;
g. rozšířenou realitu;
h. smart („chytré“) technologie a jejich bezpečnostní protokoly;
i. používání a bezpečnost senzorových sítí;
j. nové metody kybernetického válčení;
k. problematiku digitálních měn apod.

Tyto technologie a trendy s sebou přinášejí nové hrozby, vůči nimž stávající přístupy a zabezpečení nemusí být dostačující či dokonce funkční jako takové. **Je žádoucí a nutné nastupující trendy a technologie identifikovat a následně jim důkladně porozumět a připravit případné nezbytné kroky. To umožní NÚKIB zvolit postupy, jež si udrží efektivnost v dynamickém prostředí kybernetické bezpečnosti.**

7.2 Tvorba a ovlivňování mezinárodních norem a standardů

Kdy: průběžně již od 2020

Požadavky: personální kapacity v podobě vyhrazených pracovníků, sektorové specializace, koordinační kapacity s ostatními regulátory a akademickými pracovišti

Mezinárodní dění ovlivňuje kybernetickou bezpečnost státu zásadním způsobem. Jednou z cest je podílet se na nastavování mezinárodních či nadnárodních pravidel či norem, které mají přímý dopad na ČR, popřípadě na jednotlivé subjekty.

Obdobný dopad mají i mezinárodní standardy, a to ať technologického rázu, které určitým způsobem definují bezpečnostní aspekty produktů, nebo tzv. governance standardy týkající se fungování mezinárodních platforem či projektů. Příkladem může být vliv např. ITU či odborných standardizačních skupin na oblast fungování a bezpečnost telekomunikací, nebo vliv ICANN na fungování a možnou budoucí podobu Internetu.

Ze zkušeností pracovníků NÚKIB přitom lze v těchto oblastech předejít naprosto zásadním bezpečnostním dopadům. Správně nasazené kapacity NÚKIB pro řešení standardů fungování technologií, platforem a procesů mezinárodního charakteru dokážou skrze prosazování zájmů ČR ve svém důsledku přinést zásadní pozitivní efekty, a to jak v oblasti zvýšení bezpečnosti fungování kyberprostoru, tak u nákladů a ekonomických dopadů spojených se zaváděním nových standardů. Poměr přidané hodnoty a ceny za tuto aktivitu je v této oblasti významně výhodný.

7.3 Kontinuální budování školících kapacit

Kdy: v roce 2023 provést revizi koncepce a plánů a zahájit přípravu školícího pracoviště

Požadavky: adekvátní prostory a personální kapacity

Jedním z klíčových elementů, ne-li tím zcela nejpodstatnějším, je v kybernetické a informační bezpečnosti vzdělaný a motivovaný personál. Dynamický vývoj v oblasti kybernetické a informační bezpečnosti navíc klade na lidský element vysoké nároky a vyžaduje kontinuální vzdělávání. Ačkoliv NÚKIB je národní autoritou ve své působnosti, nedokáže sám efektivně zajistit požadovanou úroveň bezpečnosti a jediným účinným přístupem je komplexní přístup, který ale vyžaduje vzdělaný personál na straně partnerů úřadu i povinných subjektů. **Je tak žádoucí, aby se NÚKIB zasadil o systematické a dlouhodobé vzdělávání zaměřené primárně na povinné osoby dle ZKB, ale i zaměstnance partnerských organizací z ČR i zahraničí.**

Obdobně jako mají vlastní tréninkové kapacity armádní, policejní, hasičské či jiné bezpečnostní složky, bude stejně zásadní vytvořit tréninkové kapacity státu pro oblast kybernetické a informační bezpečnosti. NÚKIB musí mít schopnost zajistit odpovídající školení svým expertům a pracovníkům, kteří tvoří první linii v boji s kybernetickými hrozbami.

Cílem pak bude vytvořit školicí středisko, které bude fungovat jako hub pro vzdělávání, osvětu a trénink, zejména vůči specialistům, kteří vykonávají role u jednotlivých správců důležitých informačních systémů, provozovatelů kryptografických prostředků, popřípadě pro experty z příbuzných institucí.

Školicí středisko by mělo nabídnout z první ruky informace, jak přistupovat k zajišťování kybernetické a informační bezpečnosti v souladu s požadavky státu, mělo by umožnit bezprostřední zpětnou vazbu

ze strany regulovaných subjektů. V neposlední řadě jde o důležitý krok k vytváření komunity specialistů státu na kybernetickou a informační bezpečnost.

Středisko by nemělo plně nahrazovat školení nabízená soukromým sektorem, mělo by však vytvářet vlastní trénink obdobně jako u jiných bezpečnostních oblastí. Tento postup je považován za ideální hned z několika důvodů:

(i) Úřad bude mít pod kontrolou kvalitu nabízených aktivit. Pro povinné osoby bude vždy existovat kvalitní vzdělávací aktivita.
(ii) Jde o finančně výhodnější variantu než budování duplicitních kapacit u více institucí či složek nebo se spoléhat jen na nabídku komerčních subjektů.
(iii) Bude zajištěno, že na potřebné vzdělávací aktivity dosáhnou i organizace, které si z finančních důvodů nemohou komerční produkt dovolit, což by mohlo vést k vytvoření slabého místa v kybernetické bezpečnosti ČR.
(iv) Vzdělávací aktivity mohou odhalit informace citlivé povahy, které by v nepovolaných rukou či při nezabezpečeném nakládání s nimi mohly posloužit i ke škodlivé činnosti namířené na kritické systémy a instituce ČR.
(v) Pravidelná školení přispějí ke zvýšenému povědomí o stavu zajišťování kybernetické bezpečnosti u subjektů v působnosti NÚKIB, což usnadní identifikaci nedostatků a slabých míst, na něž je v budoucnu vhodné se zaměřit.
(vi) Vytvoření vlastního školicího střediska NÚKIB umožní řešit vzdělávání komplexně a dlouhodobě. Úřad bude schopen zajistit návaznost a doplňování aktivit způsobem, jenž přispěje ke vzdělaným a uvědomělým pracovníkům zodpovídajícím za zabezpečení systémů nezbytných pro chod ČR.

7.4 Sektorové specializace

Kdy: postupně od 2021; celá šíře specializací dle kapacit od 2028 dále

Požadavky: především personální kapacity, zajištění vzdělávacích aktivit nutných pro specializaci na jednotlivé sektory

Kybernetická bezpečnost je zajišťována v mnoha sektorech, které přitom mají svá specifika a jsou do značné míry heterogenní a unikátní. Kupříkladu jen u kritické informační infrastruktury je nyní v ČR rozlišováno devět odvětví:

- energetika
- vodní hospodářství
- potravinářství a zemědělství
- zdravotnictví
- doprava
- telekomunikace
- finanční trh a měna
- nouzové služby
- veřejná správa

Další odlišné sektory mohou být identifikovány například v rámci provozovatelů základních služeb či významných informačních systémů dle ZKB.

Lze přitom očekávat, že v budoucnu počet regulovaných odvětví vzroste spolu s tím, jak bude digitalizace prostupovat českou společností. Každý z těchto sektorů je do značné míry specifický, pokud jde o využívané systémy, jejich roli a tím například i typy možných útoků. Tyto důvody vedou ke vzrůstající nutnosti disponovat pracovníky s expertními znalostmi na poli jednotlivých odvětví. Nejedná se přitom jen o vědomosti technické povahy, ale i netechnické (například právní, krizového řízení, hospodaření s majetkem státu a veřejných zakázek, znalost aktérů působících v daném sektoru atd.). Vybudování expertízy v jednotlivých sektorech umožní úřadu vykonávat zejména následující činnosti:

- poskytování kvalitnější pomoci jednotlivým subjektům na míru například v případě kybernetického incidentu;
- plnění role expertní instituce, na kterou je možné se obracet kupříkladu s žádostmi o konzultace, a to jak ze strany povinných subjektů, tak i ze strany jiných státních organizací;
- umožnění postupného sjednocování a koordinace sektorových regulací kybernetické bezpečnosti ve spolupráci se sektorovými regulátory;
- provádění efektivnější komplexní kontroly, auditu či metodické podpory u povinných subjektů díky podrobné znalosti sektoru, v němž působí;
- nastavování kvalitnějších standardů a pravidel respektujících specifika jednotlivých sektorů;
- tvorba kvalitnějších školení a cvičení na míru pro jednotlivé subjekty či celé sektory.

S ohledem na rostoucí trend žádostí o konzultace a požadavky plynoucí z jednotlivých sektorů je vhodné, aby si NÚKIB zajistil jistý standard odbornosti v nejdůležitějších sektorech. Schopnost sektorové specializace je rovněž nezbytná pro efektivní vykonávání dalších činností NÚKIB.

7.5 Komplexní kontrola

Kdy: průběžně

Požadavky: posílení agendy kontroly, sektorové specializace, posílení CERT kapacit služeb subjektům

Kontrola je jedna ze zásadních agend NÚKIB v oblasti kybernetické a informační bezpečnosti. Obdobně jako u jiných oblastí, které stát reguluje, se jedná o činnost státu směřující ke zjištění, zdali subjekty naplňují zákonné požadavky a řádně zabezpečují své komunikační a informační systémy.

Kapacity k provádění kontroly je v první řadě nutné doplnit tak, aby bylo možné zajistit základní plnění zákonných povinností. V souvislosti s nárůstem počtu kontrol a zajištění personálního a odborného zázemí pro jejich provádění je však vhodné podobu kontroly posunout i po stránce kvality a vytvořit z ní službu pro kontrolované subjekty s vysokou přidanou hodnotou.

Cílem je vybudovat kapacity schopné tzv. komplexní kontroly či auditu. Kontrola ze strany NÚKIB tak nebude zahrnovat pouze klasické zjišťování shod a neshod, ale její součástí může být také:

- provedení penetračního testování, včetně phishingové kampaně, pro zjištění slabých míst zabezpečení instituce a konkrétních informačních a komunikačních systémů;
- analýza případů týkajících se kybernetické bezpečnosti kontrolovaného subjektu;
- provedení kontroly kybernetické a informační bezpečnosti s plným penzem informací o stavu zabezpečení kontrolovaných systémů;
- následná metodická pomoc a podpora při implementaci nápravných či doplňujících opatření.

Cílem je také lépe a pravidelně spolupracovat s dalšími odvětvovými regulátory (např. civilní letectví, energetika, telekomunikace aj.) tak, aby (i) byla služba ze strany státu vůči regulovaným subjektům co nejkomplexnější a (ii) aby byly související kontroly provedeny pokud možno koordinovaně tak, aby byly subjekty co nejméně zatěžovány individuálními kontrolami jednotlivých regulátorů.

7.6 Zesílená metodická pomoc

Kdy: dle dostupných kapacit, předpoklad zahájení pilotního poskytování služby od 2021

Požadavky: týmy zaměřené na metodickou pomoc technického i netechnického zaměření; sektorové specializace

Systém zajišťování kybernetické bezpečnosti v ČR deleguje část odpovědnosti za bezpečnost kyberprostoru na každý subjekt využívající tento prostor. Středobodem celého přístupu je pak bezpečnost informací, která vychází z jejich hodnoty. Tuto hodnotu pak vždy musí znát subjekt, který data využívá a zpracovává, tzv. správce. Proto je nutné, aby kybernetická bezpečnost informačních a komunikačních systémů byla primárně odpovědností správce.

Jelikož se jedná o komplexní a dynamicky se vyvíjející oblast, jsou kladené nároky na jednotlivé správce značné. Z tohoto důvodu musí být NÚKIB připraven poskytovat metodickou podporu a pomoc správcům k co nejlepšímu zabezpečení jejich systémů. Tato pomoc by se měla odehrávat jak skrze individuální konzultace, tak také pomocí přípravy postupů a metodik k nastavení vlastních bezpečnostních opatření dle aktuálního znění vyhlášky o kybernetické bezpečnosti a nejlepší praxe. Samotná práce musí být vždy provedena na straně jednotlivých správců, avšak se silnou metodickou podporou a pomocí lze překlenout některé výzvy, ať již nedostatek odborníků na pracovním trhu nebo nedostatečnou podporu problematiky kybernetické bezpečnosti v některých organizacích, či dynamický vývoj kybernetických hrozeb a další.

7.7 Tvorba technických a procedurálních standardů

Kdy: od 2027 dále

Požadavky: sektoroví odborníci, koordinační tým pro standardy

V nadcházejícím období je vhodné, aby NÚKIB začal připravovat standardy kybernetické bezpečnosti jak technické, tak i standardy tzv. governance nejen pro povinné osoby, ale také pro jednotlivé sektory či subjekty, poskytující v těchto sektorech služby.

Cílem je pak co nejefektivněji podpořit subjekty zabezpečující své informační a komunikační systémy v jejich snaze a stanovit potřebná kritéria pro hodnocení kvality či vyzrálosti některých opatření či procesů.

7.8 Týmy rychlé reakce (angl. Rapid Response Team – RRT)

Kdy: zahájení od roku 2022, plný rozvoj předpokládán od roku 2027

Požadavky: personální kapacity, technická vybavenost

Při závažných incidentech se ukázalo jako efektivní, a také často nezbytné, vyslat k napadenému subjektu tým expertů s cílem asistovat napadené organizaci při řešení incidentu. V současné době jsou vysílaní pracovníci vyčleňováni z jednotlivých oddělení pracoviště Vládního CERT. Vzhledem k trvajícímu trendu nárůstu počtu a závažnosti incidentů bude vhodné vybudovat samostatnou kapacitu určenou pro okamžitou asistenci napadenému subjektu, a to většinou fyzickým vysláním. Jedná se primárně o technické kapacity, nicméně ad hoc mohou být posíleny i netechnickými specialisty (např. analytiky, právníky či pracovníky komunikace). Vybudované týmy rychlé reakce by pak měly splňovat dvě zásadní kritéria:

1. jejich vysláním nedojde automaticky k oslabení pracoviště Vládního CERT v jiných oblastech expertízy. Pokud by vyslání týmu omezilo jiné činnosti CERT, znamenalo by to ve světle trendu nárůstu počtu závažných útoků dlouhodobé omezení kapacit pracoviště, které není žádoucí, a negativně by ovlivnilo další významné činnosti a projekty;
2. členové týmu musí mít adekvátní vzdělání a specializaci pro svoji činnost. Například jde o znalost práce Policie ČR v oblasti zajišťování důkazů či sektorovou specializaci díky různorodosti subjektů, k nimž mohou být vysláni.

Tým rychlé reakce by měl být připraven k okamžitému vyslání. K dispozici mu také musí být specializovaná technika, kterou je možné snadno přepravovat a nasadit v rozličné infrastruktuře. Nemělo by se jednat o technické vybavení, jehož absence by omezila vykonávání běžné činnosti úřadu.

7.9 Bezpečnostní operační středisko Vládního CERT

Kdy: v závislosti na potřebě a stavu připravenosti partnerů; předpoklad nejdříve od 2026.

Požadavky: personální posílení, technické vybavení

V současné době funguje Vládní CERT jako hlavní koordinační orgán pro případy kybernetických bezpečnostních incidentů na národní úrovni a hlavní kontaktní bod pro řešení přeshraničních incidentů pro mezinárodní partnery.

Vládní CERT má v současné době vybudované kapacity pro tzv. incident handling, čímž se rozumí kapacity pro koordinační a metodickou pomoc subjektům při řešení vlastních incidentů a událostí.

S tím také souvisí vybudování tzv. bezpečnostního operačního střediska, které pak umožní nejen reagovat na podněty jednotlivých správců regulovaných systémů, ale i samostatně pružně odhalovat některé hrozby a útoky a včas na ně reagovat.

Vytvořené kapacity by následně mohly podporovat i agendu ochrany utajovaných informací v informačních a komunikačních systémech, kde by bylo vhodné vyhradit část takového střediska pro hlášení incidentů u systémů nakládajících s utajovanými informacemi a následnou podporu k jejich řešení.

7.10 Rozšíření technických služeb CERT

Kdy: dle jednotlivých projektů

Požadavky: dle jednotlivých projektů

Součástí služeb, jež poskytují pracoviště typu CERT, by měly být v budoucnosti i takové, které slouží k intenzivnější prevenci kybernetických incidentů, případně efektivnější reakci na ně.

Během následujících let se jedná zejména o následující služby:

- **Pokročilé penetrační testování**
  Techniky penetračního testování je nutné dále vyvíjet a posouvat tak, aby reflektovaly aktuální postupy a nástroje, které jinak využívají útočníci v kybernetickém prostoru. Cílem NÚKIB je posouvat aktuální kapacity i v kvalitativní rovině a nabízet tak komplexní sadu služeb.

  Příkladem může být využívání technik sociálního inženýrství či phishingové kampaně. V současné době je z pohledu útočníků nejslabším místem vhodným k útoku běžný uživatel, jenž má o kybernetické bezpečnosti mnohdy minimální či žádné povědomí. Nejčastější vektor útoku představuje zasílání phishingových (či spear-phishingových) e-mailů. Mimo nepřetržité vzdělávání uživatelů je další osvědčenou metodou vedení tréninkových phishingových kampaní. Ty umožňují bezpečnou cestou simulovat aktivitu útočníků a ukázat samotným uživatelům, jak by tento útok mohl vypadat. Pravidelné vedení těchto kampaní také představuje možnost, jak mapovat úspěšné vzdělávání uživatelů a poskytovat zpětnou vazbu.

- **Hledání zranitelností**
  Jedná se o plošné skenování infrastruktury povinných subjektů vystavené do Internetu s cílem odhalit možná slabá místa. Tato metoda se od penetračního testování liší plošným použitím i povrchnějším přístupem, přičemž u této metody nedochází k pokusům o překonání bezpečnostních opatření daného systému.

- **Systém vyhledávání hrozeb**
  Ze zkušeností z metodických podpor, kontrol a analýz incidentů NÚKIB zjistil, že velké množství institucí nemá možnost, jak efektivně zajistit kontrolu vlastních systémů proti nalezeným indikátorům kompromitace (škodlivé procesy, škodlivé soubory, jejich kontrolních součtů, IP adres, domén apod.), které jim NÚKIB zaslal na základě analýz kybernetického bezpečnostního incidentu z otevřených zdrojů nebo které obdržel od svých partnerů. Tuto situaci je potřeba řešit a nabídnout možnost využít některý z připravených skriptů, návodů, případně open source nástrojů.

7.11 Kapacita pro řešení nadresortních projektů

Kdy: rozvoj projektů dle následných koordinovaných koncepcí

Požadavky: v přípravné fázi specializovaný projektový tým složený z technických, regulačních, koncepčních a projektových odborností; další kapacity v návaznosti na konečné podobě řešení a zabezpečení projektů

Rozvoj státní komunikační infrastruktury a rozvoj eGovernmentu s sebou přináší řadu bezpečnostních výzev. Tyto výzvy jsou pak společné pro vícero institucí státní správy, přičemž řešení některých z nich a na ně návazné projekty ještě nemají určeného gestora. Již v této fázi je však potřebné mít dostatečné technické, právní i koncepční kapacity, které budou schopny s partnery tyto projekty řešit a dovést do stavu realizace.

Jako příklad lze uvést následující projekty:

- **Využití české .gov domény**
  Mnohé země během postupu digitalizace státní správy zavedly unikátní doménu druhého řádu (např. ".gov.cz"). Použití tohoto doménového jména je obecně vyhrazeno pro státní instituce a vládní organizace. Jeho další užití, např. pro místní úřady či samosprávy, závisí na zvolené registrační politice. Cílem projektu je zavedení této domény včetně dalších poskytovaných služeb zvyšujících bezpečnost.

- **Vytvoření společného přístupového místa pro státní správu**
  Cílem je vytvoření jednotného přístupového místa pro státní správu do sítě Internet. Díky tomu bude možné daleko lépe čelit kybernetickým útokům a ochránit zásadní systémy pro fungování státní správy.

7.12 Navýšení počtu a kvality cvičení

Kdy: počínaje rokem 2021 a poté pozvolný růst; plný rozvoj po dobudování nového pracoviště a potřebných prostor

Požadavky: personální zajištění (netechničtí i techničtí specialisté), akvizice, rozvoj a údržba software i hardware potřebných k efektivnímu vedení veškerých typů cvičení, vlastní prostory vhodné pro vedení vlastních cvičení, rozvoj ostatních kapacit NÚKIB (sektorové specializace, penetrační testy atd.) majících zásadní dopad na kvalitu cvičení

Cvičení kybernetické bezpečnosti představují jeden z klíčových nástrojů, které přispívají k navyšování kybernetické bezpečnosti ČR. Umožňují cvičícím organizacím i jednotlivcům projít si tzv. „nanečisto“ simulovanou krizovou situací, což je základem kvalitní připravenosti na případný incident a reakci na něj. Cvičení pak nepřipravuje pouze samotné pracovníky, ale také včas odhaluje nedostatky v nastavených procesech a postupech a umožňuje je napravit v době mimo krizi.

NÚKIB nyní sám pořádá, nebo se aktivně podílí na přípravě široké palety cvičení od technických, přes procesní a table-top až po hybridní cvičení. Je žádoucí, aby byly i nadále realizovány rozličné typy cvičení, které jsou vytvořeny na míru pro různá cílová publika a účely. Přitom je potřebné nadále zvyšovat jejich kvalitu například akvizicí a rozvíjením vhodného hardware i software, tvorbou vlastních hybridních (komplexních) cvičení či rozvíjením sektorových cvičení.

Veškerá pořádaná cvičení vyžadují technické zajištění, přičemž realizace specializovaných technických cvičení vyžaduje značné kapacity ze strany technických pracovníků Vládního CERT. I tato agenda tedy musí disponovat vzdělanými zaměstnanci, zejména pro přípravu a vývoj technických cvičení, případně správu dalších nástrojů využívaných i při jiných typech cvičení.

7.13 Širší rozvoj kapacit v oblasti bezpečnosti průmyslových a řídicích systémů

Kdy: navyšování kapacit průběžně od 2021

Požadavky: navýšení personálních kapacit pro specialisty na průmyslové systémy, vybudování a provoz nové specializované laboratoře

Průmyslové a řídicí systémy představují oblast velmi odlišnou od světa informačních a komunikačních technologií. Zároveň jde o pole, kde se nachází systémy a technologie, které plní kritické funkce a zajišťují chod moderní společnosti, jak ji známe – například provoz elektráren a přenosové soustavy, továren nebo úpravu pitné vody. Díky významu a zaměření této oblasti není možné, aby ji pokrývali pracovníci řešící problematiku klasických informačních a komunikačních systémů – je potřebné disponovat specializovanými pracovníky a dalšími kapacitami. Jde tedy zejména o následující:

1. vybudování celku zaměřeného na tuto oblast s dostatkem kapacit, například i pro řešení incidentů v průmyslových systémech. Jelikož jde o velice specifické prostředí, odpovídá tomu i charakter incidentů, které jsou schopni efektivně řešit pouze specialisté;
2. vybudování technického zázemí, zejména potom laboratoře, kde by docházelo k testování kybernetické bezpečnosti průmyslových systémů a procesů. Laboratoř bude také využívána ke školení, cvičení, vývoji a výzkumu v oblasti kybernetické bezpečnosti průmyslových řídicích systémů.

S ohledem na dynamický rozvoj v oblasti kybernetické bezpečnosti průmyslových a řídicích systémů a souvisejících přidružených oblastí je potřeba se této problematice věnovat.

7.14 Kapacity pro budoucí rozvoj současných projektů

Kdy: liší se dle jednotlivých projektů

Požadavky: liší se dle jednotlivých projektů

NÚKIB již v minulosti zahájil několik projektů, jejichž cílem je přispět k navýšení kybernetické a informační bezpečnosti ČR. Nicméně vzhledem k omezeným kapacitám úřadu došlo u některých projektů ke zpoždění realizace či jejich pozastavení. Jedná se zejména o následující projekty:

1. **Kyberliga**
   Cílem je umožnit, systematizovat a nastavit využívání dobrovolnických kapacit pro potřeby státu. Projekt má značný potenciál, jelikož kapacity a expertíza soukromého nebo akademického sektoru v některých oblastech mnohdy překonávají ty státní. Již v počáteční fázi projektu byl rovněž odhalen zájem o vstup do kyberligy ze strany odborné komunity. Případné zapojení dobrovolníků z těchto sektorů může výrazně zvýšit kapacity státu v mnoha oblastech.
2. **Projekt honeypoty**[18]
   Vytvářením a správou honeypot senzorů dokáže NÚKIB získat cenná data o útocích a útočnících, kteří by mohli cílit i na systémy důležité pro chod ČR. Získaná data mohou být následně efektivně využita v identifikaci trendů a právě probíhajících útoků, u včasného varování povinných subjektů i partnerů a případně i předejití úspěšným útokům. Projekt se nyní nachází v pilotní fázi.

[18] Honeypot je technická návnada lákající útočníka k provedení útoku. Po zachycení potenciálně nebezpečného software dochází k jeho automatizované analýze.

V budoucnu je počítáno s rozvojem projektu do fáze, kdy budou nasazeny senzory implementující specifické služby partnerů.

3. **Projekt sondy**[19]
   NÚKIB realizoval projekt s názvem „Systém detekce kybernetických bezpečnostních událostí ve vybraných ISVS“. Jeho cílem je pomocí rozmístěných síťových sond usnadnit administrátorům těchto klíčových státních institucí nalezení případného útočníka a lépe je chránit. V rámci projektu došlo k nasazení sond u 20 partnerů z řad státní správy a vyškolení místních správců. Do budoucna je žádoucí projekt rozšiřovat o další organizace.

Jelikož se jedná o významné a žádoucí projekty, jeví se jako vhodné a potřebné pokračovat v jejich realizaci.

7.15 Budování netechnických kapacit v oblasti ochrany utajovaných informací

Kdy: průběžně

Požadavky: posílit koncepční a právní kapacity v této oblasti

Ochrana utajovaných informací v informačních systémech je v současné době zajišťována zejména technickými odbornými pracovníky působícími v oblasti (i) kryptologie, (ii) certifikace informačních a komunikačních systémů pro utajované informace, (iii) certifikace kryptografických prostředků a pracovišť, (iv) TEMPEST a (v) šifrové služby.

Všechny tyto agendy v sobě nesou i nutnost vykonávat další aktivity, zejména v koncepční oblasti, tzn. schopnost upravovat koncepci státu v oblasti ochrany utajovaných informací v informačních a komunikačních systémech dle aktuálních potřeb. Dále pak schopnost případné změny reflektovat v právních předpisech a také schopnost reagovat a prosazovat české zájmy na mezinárodních platformách majících přímý dopad na tuto agendu.

7.16 Dosažení plných operačních schopností PRS

Kdy: dosažení počátečních operačních schopností do konce 2021, následně dosažení plných operačních schopností

Požadavky: personální posílení a vybudování potřebné infrastruktury

PRS je exkluzivní služba poskytovaná systémem Galileo autorizovaným uživatelům, která vyžaduje dodržování přesně definovaných pravidel pro řízení a kontrolu přístupu k této službě. Jednou z podmínek je i vybudování a nepřetržitý provoz dohledového centra PRS a nastavení národních pravidel použití PRS včetně kontroly jejich dodržování, zabezpečení autorizace subjektů pro přístup k PRS informacím a kontrolu exportu a importu PRS zařízení.

[19] Sondy jsou zařízení, která pomohou upozornit na podezřelá datová spojení, anomální objemy dat opouštějící konkrétní síť, rozpoznají „oťukávání“ sítě zvnějšku a slouží i jako nástroj včasného varování před blížícími se útoky. Tato zařízení mají také schopnost získávat a uchovávat popisná data o provozu a vytvořit tak auditní stopu pro pozdější zkoumání.

8 VYPLÝVAJÍCÍ POŽADAVKY

Jak vyplývá z výše uvedeného, NÚKIB potřebuje primárně **stabilizovat**, **dobudovat** a dále **rozvíjet** své schopnosti a kapacity.

S vědomím dříve schválených materiálů, zejména vládním usnesením z roku 2016 o *Návrhu rozvoje kapacit a schopností Národního centra kybernetické bezpečnosti do roku 2025,* které stanovovaly vybudování potřebného zázemí, infrastruktury a doplnění personálních kapacit až do počtu 400, **a s vědomím současné ekonomické situace a reálných možností státu**, pak potřebuje:

(i) potřebnou **nemovitou infrastrukturu**, (ii) adekvátní personální kapacity a (iii) tomu odpovídající **finanční prostředky**.

8.1 Nemovitosti

V prvé řadě potřebuje NÚKIB zajistit vhodné lokality pro své fungování a další rozvoj. Jedná se o zázemí v Brně a v Praze.

8.1.1 Brno

Brno je sídlem NÚKIB a v současné době je zde umístěna primárně Sekce NCKB, Sekce provozně právní a části Sekce informační bezpečnosti.

Zejména pro tyto organizační celky je nutné vybudovat nové zázemí. V současnosti je připraven projekt Černá Pole, který je nejsnazší a nejefektivnější cestou k vyřešení současného nevyhovujícího stavu. Jeho ukončení je plánováno v průběhu roku 2026.

8.1.1.1 Mezičas

V mezičase je potřebné nalézt prostory, které v Brně pojmou nárůst kapacit, jež NÚKIB vyžaduje k dobudování. Jako nejvýhodnější způsob zajištění prostorových kapacit v mezičase se jeví rekonstrukce a úpravy již existujících objektů v majetku státu.

8.1.2 Praha

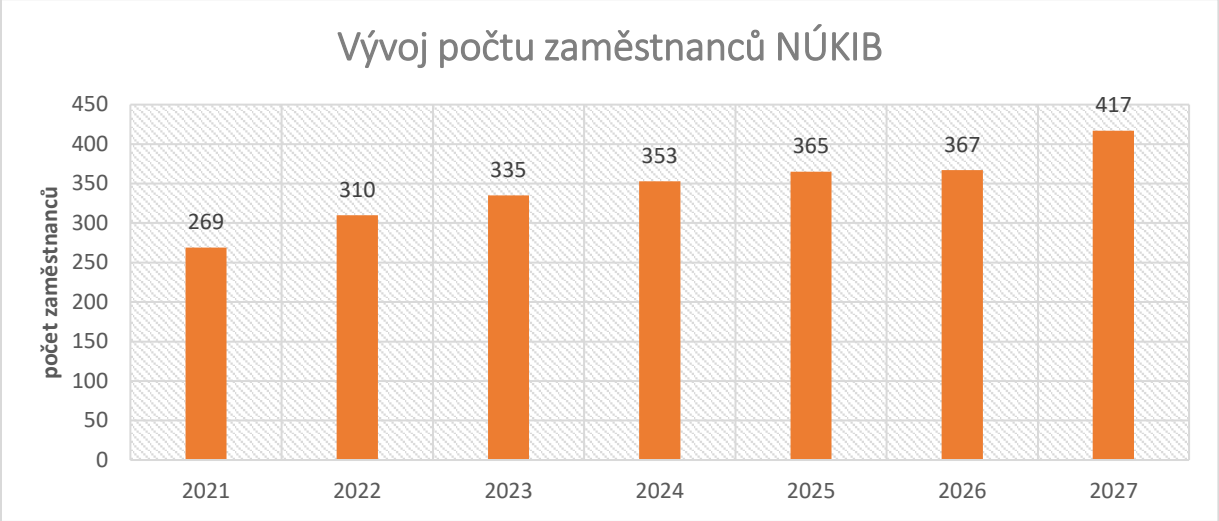
V Praze jsou umístěny prostory odboru Kabinetu ředitele, stejně jako část NÚKIB věnující se ochraně utajovaných informací, část věnující se Galileo PRS a některé části agendy kybernetické bezpečnosti; ty zde budou v dalším období posíleny.

V průběhu této koncepce bude dokončena komplexní delimitace od Národního bezpečnostního úřadu, k čemuž bude nutné vybudování adekvátních prostor, které budou splňovat zejména přísné nároky na bezpečnost.

8.2 Personál

Klíčovým předpokladem pro zachování funkčnosti NÚKIB je personální posílení zejména v nejkritičtějších oblastech a tam, kde neexistuje řádná zastupitelnost pracovníků a existuje vysoké riziko ztráty expertízy a schopností státu.

Tabulka níže znázorňuje vývoj počtu personálu v jednotlivých letech:[20]



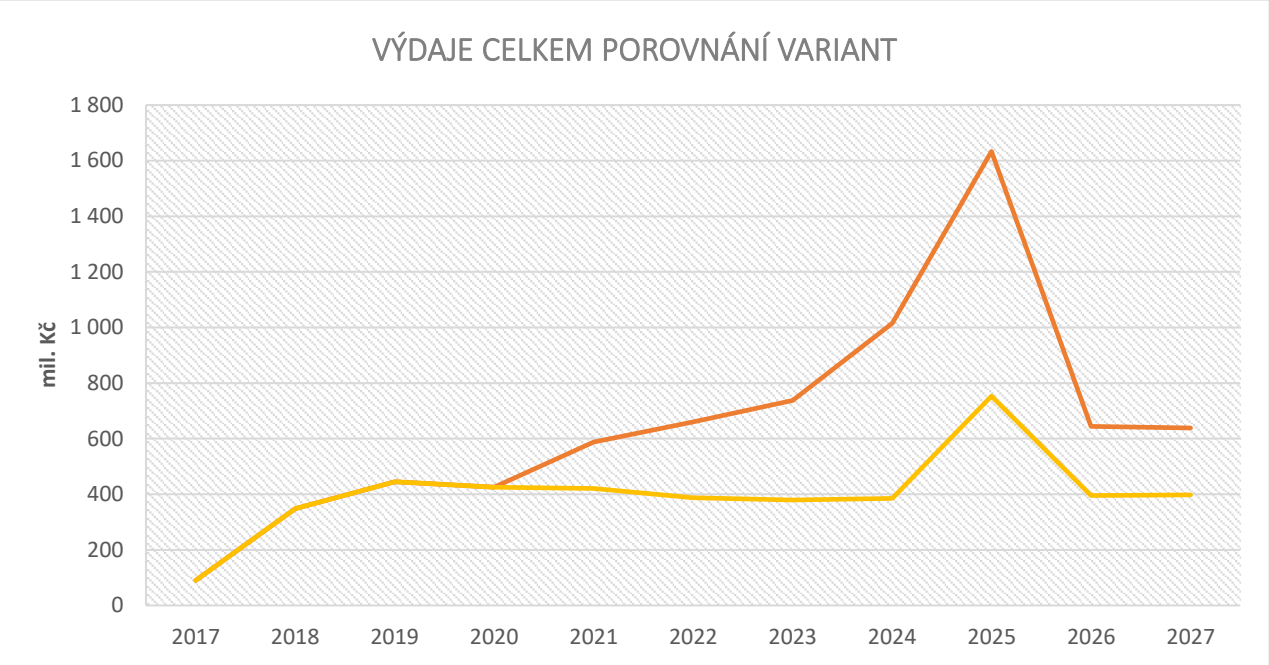
8.3 Celkové náklady

Celkově se jedná o následující náklady v jednotlivých letech.

PLÁN NA DOBUDOVÁNÍ A NÁSLEDNÝ ROZVOJ NÚKIB

	2020	2021	2022	2023	2024	2025	2026	2027
počet pracovníků	221	269	310	335	353	365	367	417
náklady personál	189 mil.	230 mil.	265 mil.	287 mil.	302 mil.	312 mil.	314 mil.	356 mil.
náklady investice	98 mil.	198 mil.	217 mil.	276 mil.	532 mil.	1060 mil.	125 mil.	75 mil.
náklady provoz	138 mil.	160 mil.	178 mil.	174 mil.	181 mil.	261 mil.	205 mil.	207 mil.
celkem	**425 mil.**	**588 mil.**	**660 mil.**	**737 mil.**	**1015 mil.**	**1633 mil.**	**644 mil.**	**638 mil.**

[20] Pokud do roku 2027 nedojde k nepředvídatelným okolnostem (jako např.: rozšíření zákonné působnosti o nové povinnosti), NÚKIB nebude v uvedených letech požadovat další posilování personálních kapacit nad rámec požadavků předložených v tomto dokumentu. Případné posilování souvisejících prostředků na platy (např.: v souvislosti s plošným růstem platů ve státní správě) bude předmětem projednávání požadavků na státní rozpočet v jednotlivých letech.



Výdaje bez rozvoje celkem od roku 2021	3 118 mil. Kč
Cena rozvoje od roku 2021 (Plán na dobudování a následný rozvoj NÚKIB)	+ 2 797 mil. Kč

Poznámky:

- **Výrazný růst nákladů v roce 2025 v obou případech je způsoben mimo jiné nutností periodické obnovy technické infrastruktury.**
- **Provozní a investiční výdaje reflektují inflační koeficient 3 % (netýká se investiční akce Černá pole).**
- **Při výpočtu personálních nákladů se vychází z aktuálního stavu platů. Personální náklady také nereflektují nutné navýšení platů některých specializací k udržení konkurenceschopnosti.**

PŘÍLOHA Č. 1 AGENDY VYKONÁVANÉ NÚKIB

Kategorie činností	Činnost	Předpis
KYBERNETICKÁ BEZPEČNOST		
Tvorba bezpečnostních politik	Příprava a vyhodnocování strategie ČR v oblasti KB	§ 22 písm. q) ZKB
	Vyhodnocování Akčního plánu	usnesení vlády č. 382/2015
	Návrhy úpravy politiky ČR v oblasti KB	obecné principy činnosti ÚSÚ
	Návrhy úpravy širší legislativy	obecné principy činnosti ÚSÚ
Regulace	Určování KII a PZS	§ 22 písm. n) a p) ZKB
	Vedení evidence KII, VIS a PZS a udržování aktuálnosti	§ 22 písm. o) ZKB
	Stanovování bezpečnostních opatření	§ 22 písm. a) ZKB
	Vydávání opatření	§ 22 písm. b) ZKB
	Úprava regulačních předpisů	obecné principy činnosti ÚSÚ
	Zajišťování metodické podpory	§ 22 písm. j) ZKB
	Poskytování konzultací	D.4.01 AP
	Vytváření doporučení i pro nepovinné subjekty ze ZKB	C.3.02 AP
	Koordinace regulačních rámců kybernetické bezpečnosti napříč sektory	obecné principy činnosti ÚSÚ
Výkon kontroly	Výkon kontroly podle zákona o kybernetické bezpečnosti	§ 23 ZKB
	Metodické audity podle usnesení vlády	usnesení vlády 607/2017
	Přijímání podnětů k zahájení správního řízení (porušení povinností podle zákona o kybernetické bezpečnosti)	§ 42 správního řádu
	Návrhy nápravných opatření či sankcí a kontrola jejich dodržování	§ 24 ZKB

Vládní CERT	Provozování Vládního CERT	§ 20 ZKB
	Incident handling	§ 20 písm. b) až e), l) ZKB
	Přijímání podnětů od povinných osob a dalších osob a jejich vyhodnocování	§ 20 písm. f) ZKB
	Spolupráce s Národním CERTem a dalšími CERT či obdobnými institucemi	§ 20 písm. g) až i) ZKB
	Hodnocení zranitelností	§ 20 písm. j) ZKB
	Plnění role týmy CSIRT dle NIS směrnice	§ 20 písm. m) ZKB
	Vedení evidence dle § 9 ZKB	§ 9 ZKB
Vládní CERT	Monitorování a analýza síťového provozu	C.3.07, C.4.02 AP
	Honeypot projekt	C.3.06 AP; § 22 písm. j)
	Penetrační testování	C.3.10, C.8.01 AP; zákl. kompetence v § 22 písm. j) (prevence) a § 20 písm. j);
	Forenzní laboratoř, analýza malware	C.3.08 AP; § 22 písm. j) (prevence) a § 20 písm. u)
	Vývoj vlastních nástrojů a řešení GovCERT	§ 20 ZKB
	Vytváření expertízy v nejvyužívanějších oblastech KB (ICS/SCADA, různé operační systémy, analýza síťového provozu, mobilní zařízení aj.)	§ 20 ZKB
Analytika	Provádění analýzy a monitoringu kybernetických hrozeb a rizik	§ 22 písm. u) ZKB
	Vybudování a provoz detekčního systému včasného varování	C.6.04
	Analytická podpora organizačních částí a vedení NÚKIB	§ 22 písm. u) ZKB
	Vytváření zprávy o stavu kybernetické bezpečnosti	usnesení vlády č. 105/2015
Krizové řízení	Krizové řízení na úrovni státu; plnění role koordinačního orgánu za stavu kybernetického nebezpečí	§ 22 písm. f) ZKB, C.12.01

Národní spolupráce	Obecná povinnost	§ 22 písm. g) ZKB
	Koordinace s dalšími subjekty státní správy	obecné principy činnosti ÚSÚ
	Koordinace a harmonizace pozic v mezinárodních organizacích s ostatními rezorty	A.4.02 AP
	Aktivní zapojení do diskuzí se soukromým sektorem	D.1.01 AP
	Vytvoření platformy na sdílení informací o kybernetických hrozbách a zranitelnostech	D.5.05 AP
Mezinárodní spolupráce	Obecná povinnost	§ 22 písm. h), i) ZKB
	Aktivní účast na jednáních v EU, NATO	AP (B.1.01, B.1.02)
	Aktivní účast na jednáních v NATO	AP (B.1.05, B.1.06 a další)
	Aktivní účast na jednáních v OBSE	B.1.04 AP
	Aktivní účast na jednáních v OSN a dalších	B.1.07, B.7.01 aj. AP
	Participace v CCDCOE	B.1.09 AP
	Spolupráce v rámci Středoevropské platformy (CECSP)	B.2.01 AP
Mezinárodní spolupráce	Plnění role jednotného kontaktního místa pro zajištění přeshraniční spolupráce v rámci EU	§ 22 písm. r) ZKB
	Zastupování ČR ve skupině pro spolupráci dle NIS směrnice	§ 22 písm. s) ZKB
	Podílení se na činnosti ENISA	B.1.03 AP
Cvičení	Provádění technických cvičení	A.1.03 AP
	Provádění netechnických cvičení	A.1.03 AP
	Příprava, zajišťování a koordinace mezinárodních cvičení	B.4.01 AP

Vzdělávání a osvěta	Zajišťování prevence a vzdělávání Pořádání konferencí a osvětových akcí Provoz e-learningového vzdělávacího portálu Modernizace vzdělávacích programů o téma KB Spolupráce s VŠ: přehled oborů se zaměřením na KB, stáže, vedení diplomových prací Vytváření metodických materiálů pro učitele atd.	§ 22 písm. j) ZKB D.4.01, F.1.01, F.2.05 AP F.1.03, F.3.01-04 AP F.2.01,F.2.02 AP F.2.04,F.2.06-08, E.4.02 AP F.2.03 AP
Výzkum	Zajišťování a koordinace výzkumu v oblasti KB Aktualizace Národního plánu výzkumu v KB Aktualizace interního plánu výzkumných aktivit NÚKIB Databáze výzkumných projektů v oblasti KB Tvorba a účast ve výzkumných konsorciích v oblasti KB	§ 22 písm. k) ZKB E.1.01-02,E.2.02 AP E.1.03 AP E.2.01 AP E.3.01,E.4.01 AP
EU certifikace produktů a služeb	Plnění role vnitrostátního orgánu certifikace kybernetické bezpečnosti dle Nařízení Cyber Security Act (kyberbalíček)	čl. 58 CSA, D.2.02 AP
Projektová kancelář	Jednotlivé projekty jsou navázány na APOD.	Např. Systém detekce (sondy) - C.4.02 AP

Galileo PRS		
Výkon příslušného orgánu PRS (dále jen CPA)	Správa utajovaných informací PRS a klíčů k PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Řízení přístupu k informacím PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Řízení bezpečnostních rizik uživatelů PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Organizace skupin uživatelů PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Vymezení a správa přístupových práv pro uživatele PRS a komunity uživatelů PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Distribuce přístupových klíčů k PRS a souvisejících utajovaných informací uživatelům	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Zajištění uplatňování provozních koncepcí a postupů pro používání PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Autorizace subjektů pověřených vývojem nebo výrobou zařízení PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Zabezpečení položek PRS v průběhu výzkumu, vývoje a výroby	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Zajištění dodržování Profilu ochrany pro bezpečnostní moduly PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Zajištění dodržování opatření pro integraci bezpečnostních modulů PRS do ostatních zařízení PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Posouzení splnění podmínek pro vývoz položek PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Zajištění hlasového a datového spojení pro přenos klíčů k PRS a souvisejících utajovaných informací mezi bezpečnostním střediskem a CPA	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Posouzení splnění podmínek pro přepravu položek PRS	§ 22 písm. v) ZKB, 1104/2011/EU, CMS
	Zastupování ČR ve výborech a pracovních skupinách Evropské komise a Agentury pro evropský GNSS (budoucí Agentury Evropské unie pro kosmický program) řešících problematiku PRS a bezpečnosti kosmického programu	§ 22 písm. v) ZKB

Ochrana utajovaných informací v informačních a komunikačních systémech		
Kryptologie	Aplikovaný výzkum a vývoj kryptografických prostředků	§ 137a písm. f) ZOUI
	Analýzy a hodnocení šifrových systémů a krypto algoritmů	§ 137a písm. g) ZOUI
	Vývoj nových technologií a výrobních zařízení na výrobu klíčových materiálů kryptografických prostředků	§ 137a písm. f) ZOUI
	Výzkum v oblasti matematické kryptologie	§ 137a písm. g) ZOUI
	Vývoj a schvalování národních šifrových algoritmů	§ 137a písm. g) ZOUI
	Vývoj a schvalování národních kryptografických schémat	§ 137a písm. g) ZOUI
Certifikace IS a KS pro UI	Výkon funkce Národního střediska pro bezpečnost IS	§ 137a písm. d) ZOUI
	Certifikace informačních a komunikačních systémů	§ 137a písm. e) ZOUI
	Schvalování projektů bezpečnosti KS	§ 137a písm. e) ZOUI
	Evidence certifikovaných IS, kontrola dodržování podmínek a schvalování změn	§ 138 ZOUI
	Bezpečnostní akreditace IS pro NATO a EU	§ 137a písm. b) ZOUI
	Výzkumně-vývojové práce pro bezpečnostní funkce IS a KS	§ 137a písm. l) ZOUI
	Konzultační činnost	§ 137a písm. c) ZOUI
Certifikace kryptografických prostředků a pracovišť	Certifikace kryptografických prostředků	§ 137a písm. e) ZOUI
	Stanovování bezpečnostních standardů pro KP	§ 137a písm. j) ZOUI
	Konzultace k certifikačním řízením	§ 137a písm. c) ZOUI
	Vedení seznamu NÚKIB materiálu kategorie CCI	§ 37 odst. 3 ZOUI
	Schvalování způsobilosti materiálu k zabezpečení funkce kryptografických prostředků	§ 137a písm. e) ZOUI
	Schvalování projektů zástavby KP do mobilních systémů	§ 137a písm. l) ZOUI
	Spolupráce v rámci NATO a EU pro zajištění mezinárodní certifikace kryptografických prostředků	§ 137a písm. b) ZOUI
	Metodická činnost v příslušných oblastech ochrany UI	§ 137a písm. c) ZOUI
	Státní dozor, kontrola	§ 143 odst. 6 ZOUI

TEMPEST (měření kompromitujícího elektromagnetického vyzařování)	Výkon role Národního střediska pro TEMPEST	§ 137a písm. d) ZOUI
	Vývoj metod a postupů pro hodnocení elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu z hlediska úniku UI prostřednictvím kompromitujícího vyzařování	§ 137a písm. c) ZOUI
	Konzultace k certifikaci IS a KS	§ 137a písm. c) ZOUI
	Školení k problematice TEMPEST	§ 137a písm. c) ZOUI
	Vytváření analýz a hodnocení elektrických a elektronických zařízení a kryptografických prostředků	§ 137a písm. h) ZOUI
	Zajišťování zónových hodnocení prostor a certifikace stínících komor určených pro zpracování UI	§ 137a písm. h) ZOUI
Šifrová služba	Výkon role Národního střediska pro distribuci kryptografického materiálu	§ 137a písm. d) ZOUI
	Provádění zkoušek zvláštní odborné způsobilosti pracovníků kryptografické ochrany	§ 137a písm. a) ZOUI
	Evidence KP, dokumentů, klíčových a heslových materiálů a pracovníků kryptografické ochrany	§ 137a písm. d) ZOUI
	Výroba klíčových materiálů pro provoz KP	§ 137a písm. d) ZOUI
	Distribuce klíčových materiálů pro provoz KP	§ 137a písm. d) ZOUI
	Servis a údržba	§ 137a písm. d) ZOUI

Věcně-podpůrné činnosti		
PR a tiskové záležitosti	Styk s veřejností	obecné principy činnosti ÚSÚ
	Styk s médii	obecné principy činnosti ÚSÚ
	Zajištění webové prezentace úřadu	obecné principy činnosti ÚSÚ
	Zajišťování propagace úřadu (sociální sítě aj.)	obecné principy činnosti ÚSÚ
Vládní a parlamentní agenda	Připomínková řízení materiálů před projednáním vládou	obecné principy činnosti ÚSÚ
	Příprava návrhů právních předpisů v působnosti úřadu	obecné principy činnosti ÚSÚ
	Příprava materiálů do určených k projednání vládou, BRS a jejích pracovních výborů (VVB, VKZBP, VOP)	obecné principy činnosti ÚSÚ
	Plánování legislativních a nelegislativních prací	obecné principy činnosti ÚSÚ
	Agenda aproximace práva EU	obecné principy činnosti ÚSÚ
	Koordinace součinnosti s jinými orgány ve věcech legislativy a vládní agendy, včetně poskytování pomoci s přípravou právních předpisů z oblasti informačních a komunikačních technologií	obecné principy činnosti ÚSÚ
	Komunikace s PSP a Senátem PČR (SK NÚKIB, VB, VZOB)	obecné principy činnosti ÚSÚ
	Zajišťování činnosti sekretariátu Rady pro kybernetickou bezpečnost	Statut RKB
	Zajišťování činnosti sekretariátu Výboru pro kybernetickou bezpečnost	Statut VKB
Mezinárodní spolupráce	Zajišťování zahraničních pracovních cest pracovníků úřadu	obecné principy činnosti ÚSÚ
	Zajišťování incomingových návštěv	obecné principy činnosti ÚSÚ
	Rozvoj mezinárodní spolupráce úřadu	obecné principy činnosti ÚSÚ
	Aktivní účast na jednáních v EU a NATO (kybernetická bezpečnost, bezpečnost informačních systémů, PRS Galileo) Výkon činnosti cyber attaché Zastupování ČR v NATO Cooperative Cyber Defence Centre of Excellence v Talinnu	§ 22 písm. h) ZKB

Provozní a podpůrné činnosti		
Bezpečnost	Krizové řízení úřadu BOZP, požární ochrana Fyzická bezpečnost Řízení přístupů na lokalitách Interní protikorupční program úřadu Zajištění ochrany utajovaných informací (personální, fyzická a administrativní bezpečnost) včetně školení Zastupování úřadu ve VCNP Zajištění kybernetické bezpečnosti na úrovni úřadu	Usnesení vlády ČR ze dne 17. prosince 2018 č. 855 (Vládní koncepce boje s korupcí na léta 2018 až 2022) ZOUI
Spisová služba	Zajišťování spisové služby, činnosti registru, správního archivu úřadu Metodické třídění a zpracování archivních svazků (převz. z NBÚ)	Zákon o archivnictví a spisové službě
Registr	Zajištění činnosti registru UI NATO, EU a OCM v prostředí úřadu	ZOUI

IT provoz	Návrh a výstavba neutajované ICT infrastruktury úřadu ve všech lokalitách Návrh a výstavba utajované ICT infrastruktury úřadu ve všech lokalitách Rozvoj, provoz a údržba neutajované ICT infrastruktury úřadu ve všech lokalitách Rozvoj, provoz a údržba utajované ICT infrastruktury úřadu ve všech lokalitách Kompletní zajištění provozu a technické podpory uživatelů a koncových bodů utajované infrastruktury ve všech lokalitách úřadu Kompletní zajištění provozu a technické podpory uživatelů a koncových bodů neutajované infrastruktury ve všech lokalitách úřadu Rozvoj, provoz a údržba neutajované informační a komunikační infrastruktury s externím prostředím a externími subjekty Dohled, monitoring a zabezpečení ICT úřadu a jeho interních i hraničních prvků Návrh, výstavba, rozvoj, provoz systému TIGER včetně podpory koncových uživatelů Zajištění provozu a obsluhy CRONOS, VEGA-T, VEGA-D	
	Příprava a koordinace nákupů ICT úřadu dle ZZVZ a jeho realizace Tvorba a vedení ICT dokumentace Rozvoj, provoz a údržba aplikační platformy úřadu Administrativní, evidenční a majetkové činnosti související s procesem evidence, nákupů a životního cyklu ICT prostředků úřadu	
IT provoz - analytika	Zajištění služeb datové analytiky NÚKIB Projekt monitoringu zranitelností Vývoj nových služeb datové analytiky	§ 22 písm. u) ZKB § 20 písm. j) a § 22 písm. u) ZKB § 22 písm. u) ZKB

Provozní agenda	Správa a údržba majetku, inventarizace BOZP a požární ochrana Provoz služebních automobilů Materiálně-technické zabezpečení úřadu	
Ekonomická agenda	Příprava návrhu rozpočtu úřadu a střednědobý výhled, čerpání rozpočtu, rozpočtová opatření Účetní výstupy, účetní závěrky Vyúčtování tuzemských a zahraničních pracovních cest Chod pokladny	
Personální agenda	Vytváření a analýza pracovních míst Plánování a získávání zaměstnanců Výběrová řízení a přijímání zaměstnanců Vzdělávání, osobnostní a profesní rozvoj, hodnocení Platová agenda Pracovní vztahy a komunikace s odbory Péče o zaměstnance, FKSP	

Právní agenda a veřejné zakázky	Přestupky podle zákona o kybernetické bezpečnosti a zákona o ochraně osobních údajů Zadávání veřejných zakázek Agenda obchodních a dalších smluvních ujednání, registr smluv	
	Zajišťuje výkon komplexních právních činností v celém oboru působnosti úřadu, zpracování stanovisek a INA Zastupuje úřad v řízení před soudem a jinými orgány státu Činnost rozkladové komise úřadu Povinnosti úřadu ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, zákona č. 110/2019 Sb., o zpracování osobních údajů, a GDPR Zpracovává stanoviska z oblasti kybernetické bezpečnosti a vybraných oblastí ochrany utajovaných informací Posuzuje návrhy smluv o zajištění činnosti, veřejnoprávních smluv, opatření obecné povahy a rozhodnutí podle zákona o kybernetické bezpečnosti před jejich uzavřením nebo uložením Podílí se na zpracování návrhů právních úprav, připomínkování právních předpisů a materiálů nelegislativní povahy předkládaných vládě České republiky a jejím orgánům	
Interní audit	Provádění interních auditů, mapování rizik Provádění následných finančních kontrol, poradenská a konzultační činnost Zpracování Roční zprávy o výsledcích finančních kontrol pro Ministerstvo financí Prověřování kvality a účinnosti vnitřního kontrolního systému úřadu, tvorba INA	
Investice a rozvoj	Příprava investičních záměrů Příprava a realizace investičních akcí Komplexní inženýrská činnost Opravy, rekonstrukce	