MVCRX04GX8UW
prvotní identifikátor

Smlouva

o poskytnutí účelové podpory
na řešení projektu výzkumu, vývoje a inovací s názvem

„Nástroje pro simulaci útoků a emulaci průniku do kritické informační infrastruktury“

VI20202022133

uzavřená mezi smluvními stranami

Česká republika – Ministerstvo vnitra

a

Masarykova univerzita

Č.j. MV- 56066-5/OBVV-2019
Počet stran:14
Přílohy: 2

Smluvní strany

Česká republika – Ministerstvo vnitra

se sídlem: Nad Štolou 936/3, 170 34 Praha 7
IČ: 00007064
DIČ: CZ00007064
zastoupená ředitelem odboru bezpečnostního výzkumu a policejního vzdělávání JUDr. Petrem Novákem, Ph.D.
číslo bankovního účtu: 3605881/0710
adresa pro doručování: Ministerstvo vnitra, odbor bezpečnostního výzkumu a policejního vzdělávání (gesční útvar MV ČR pro oblast bezpečnostního výzkumu), Nad Štolou 936/3,
170 34 Praha 7, tel.: 974 832 746, e-mail: obv@mvcr.cz

(dále jen „**poskytovatel**“)

a

Masarykova univerzita, Ústav výpočetní techniky

se sídlem Žerotínovo náměstí 617/9, 601 77 Brno
IČ: 00216224
DIČ: CZ00216224
Statutární zástupce: doc. PhDr. Mikuláš Bek, Ph.D., rektor
veřejná vysoká škola uvedená v příloze č. 1 zákona č. 111/1998 Sb., o vysokých školách

adresa pro doručování: sídlo příjemce

kontaktní osoba: manažer projektu

(dále jen „**příjemce**“)

uzavírají v rámci Programu bezpečnostního výzkumu České republiky v letech 2015 - 2022 (BV III/1 – VS), na základě § 9 zákona č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a o změně některých souvisejících zákonů ve znění pozdějších předpisů (dále jen „zákon č. 130/2002 Sb.“) a v souladu se zákonem č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník“) tuto

Smlouvu o poskytnutí účelové podpory
na řešení projektu výzkumu, vývoje a inovací
(dále jen „Smlouva“)

Článek 1
Předmět Smlouvy

1) Předmětem této Smlouvy je závazek příjemce řešit projekt výzkumu, vývoje a inovací s názvem **„Nástroje pro simulaci útoků a emulaci průniku do kritické informační infrastruktury“** a identifikačním kódem **„VI20202022133“** a závazek poskytovatele poskytnout příjemci na tento projekt účelovou podporu z veřejných prostředků (dále jen ”podpora”) v rozsahu a za podmínek stanovených Smlouvou.

2) Předmětem řešení projektu je experimentální vývoj zaměřený vytvoření sady nástrojů, které umožní částečně nahradit experty na penetrační testování. Díky zaměření se na automatizaci statického i dynamického testování kyberbezpečnosti poskytne prostředky pro nepřetržité monitorování a vyhodnocování zabezpečení cílové infrastruktury, pro realizaci kyberbezpečnostních cvičení a poslouží jako podklad pro bezpečnostní certifikaci. Svým důrazem na automatizaci výrazně sníží požadavky na množství a expertízu personálu bezpečnostních týmů.

3) Cíle projektu, předpokládané výsledky, rozpočet a harmonogram projektu, včetně dalších údajů jsou uvedeny ve schváleném projektu, který je přílohou č. 1 Smlouvy (dále jen „Projekt“).

Článek 2
Administrátor Projektu

1) Administrátor Projektu je zaměstnanec gesčního útvaru pro oblast bezpečnostního výzkumu určený poskytovatelem, který je odpovědný za spolupráci a komunikaci s příjemcem ve všech záležitostech věcného plnění Projektu a finančního využití poskytnuté podpory.

2) Jméno a kontaktní údaje administrátora projektu budou příjemci sděleny při předání Smlouvy.

Článek 3
Manažer Projektu

Manažer Projektu určený příjemcem je odpovědný za řízení Projektu, včetně finančního řízení, za spolupráci a komunikaci s poskytovatelem.

Článek 4
Hlavní řešitel Projektu

Za odbornou úroveň Projektu dle § 9 odst. 1 písm. e) zákona č. 130/2002 Sb. je příjemci odpovědný [redacted]

Článek 5
Doba řešení Projektu

1) Příjemce je povinen zahájit řešení Projektu dne 1. 1. 2020.

2) Příjemce je povinen ukončit řešení Projektu nejpozději ke dni 31. 12. 2022.

Článek 6
Uznané náklady, výše podpory a platební podmínky

1) Uznané náklady[1] na řešení Projektu se stanovují ve výši **9 679 618,- Kč** (slovy: devetmilionůšestsetsedmdesátdevěttisícšestsetosmnáctkorunčeských). Tato částka zahrnuje podporu ve výši **9 679 618,- Kč** (slovy: devetmilionůšestsetsedmdesátdevěttisícšestsetosmnáctkorunčeských), která je poskytovaná formou dotace z rozpočtové kapitoly Ministerstva vnitra.

2) Členění uznaných nákladů na jednotlivé položky a pro jednotlivé roky řešení Projektu je uvedeno v rozpočtu Projektu.

[1] Uznané náklady jsou takové způsobilé náklady, které poskytovatel schválil a které jsou zdůvodněné.

3) Nedojde-li v důsledku rozpočtového provizoria podle zákona č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů (dále jen „zákon o rozpočtových pravidlech“) k regulaci čerpání rozpočtu, poskytovatel poskytne podporu příjemci v prvním roce řešení Projektu ve lhůtě do 60 kalendářních dnů ode dne nabytí účinnosti Smlouvy. V dalších letech řešení poskytovatel poskytne podporu do 60 kalendářních dnů od začátku kalendářního roku za podmínky, že jsou splněny závazky příjemce vyplývající ze Smlouvy, zejména, že příjemce předložil roční zprávu včetně vyúčtování poskytnutých finančních prostředků, a tato zpráva byla schválena poskytovatelem, a že jsou zařazeny údaje do informačního systému výzkumu, vývoje a inovací v souladu se zákonem č. 130/2002 Sb., Nařízením vlády č. 397/2009 Sb., o informačním systému výzkumu, experimentálního vývoje a inovací (dále jen „NV č. 397/2009 Sb.“) a se zvláštním právním předpisem (zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů).

4) Pokud v průběhu řešení Projektu dojde ke snížení plánovaných finančních prostředků na výzkum a vývoj poskytovatele v rámci státního rozpočtu, je poskytovatel oprávněn jednostranně snížit podporu uvedenou v odstavci 1 tohoto článku a bude uzavřen písemný dodatek ke Smlouvě, v němž se vymezí související úpravy Projektu.

5) Podpora bude poskytována v souladu s rozpočtem bezhotovostním převodem z bankovního účtu poskytovatele na běžný korunový bankovní účet příjemce.

6) Příjemce má povinnost provést audit celého Projektu. Auditorskou zprávu předloží příjemce poskytovateli spolu se závěrečným vyúčtováním Projektu. Audit se týká všech nákladů Projektu. Do uznaných nákladů lze zahrnout pouze náklady na provedení auditu v závislosti na době realizace a účetní náročnosti Projektu až do výše 100 000,- Kč.

Článek 7
Změny Rozpočtu

1) Podstatnou změnou rozpočtu, pro jejíž provedení je nutný předchozí souhlas poskytovatele se rozumí:

   a) zdůvodněná změna celkové výše rozpočtu příjemce,

   b) zdůvodněný přesun uvnitř rozpočtové skupiny mezi položkami přesahující 10 % celkových nákladů této skupiny v rámci rozpočtu příjemce v daném kalendářním roce,

   c) zdůvodněný přesun mezi rozpočtovými skupinami přesahující 10 % celkového rozpočtu příjemce v daném kalendářním roce.

   d) zdůvodněný přesun finančních prostředků z jiných rozpočtových skupin do rozpočtové skupiny osobní náklady a zdůvodněný přesun finančních prostředků mezi jednotlivými položkami v rámci rozpočtové skupiny osobní náklady přesahující 10 % celkových nákladů této skupiny.

2) Ostatní změny rozpočtu musí být se zdůvodněním oznámeny poskytovateli do 7 pracovních dnů od jejich provedení. Dojde-li k ostatní změně rozpočtu v měsíci prosinci, oznámí ji příjemce v roční zprávě za příslušný rok za dodržení podmínek podle Článku 12 odst. 2 Smlouvy.

3) V případě, že součet objemu jednotlivých změn rozpočtu dle odstavce 2 tohoto článku v daném kalendářním roce dosáhne hranice stanovené v odstavci 1 písm. b) nebo c) tohoto článku, podléhá každá další změna rozpočtu předchozímu souhlasu poskytovatele.

4) Pokud příjemce neobdrží stanovisko poskytovatele do 15 pracovních dnů ode dne odeslání informace o podstatné změně rozpočtu dle odstavce 1 tohoto článku nebo o změně dle odstavce 3 tohoto článku, považuje se změna rozpočtu za schválenou poskytovatelem, pokud není stanoveno jinak. Poskytovatel může lhůtu prodloužit o 15 pracovních dnů; je však povinen o prodloužení lhůty příjemce písemně informovat.

5) V případě změny celkové výše rozpočtu, při které dochází k navýšení podpory podle Článku 7 odst. 1 Smlouvy lze tuto změnu realizovat pouze uzavřením dodatku k této Smlouvě.

6) Žádosti příjemce o předchozí souhlas poskytovatele podle odstavce 1 a 3 tohoto článku i oznámení změny rozpočtu podle odstavce 2 tohoto článku předává příjemce prostřednictvím formuláře zveřejněného na webových stránkách Ministerstva vnitra včetně nové verze rozpočtu a komentáře popisujícího jeho změny.

Článek 8
Intenzita podpory

1) Intenzitou podpory se rozumí v procentech vyjádřený podíl výše podpory k uznaným nákladům příjemce v daném roce řešení Projektu.

2) Maximální povolená výše intenzity podpory činí 100 %.

Článek 9
Subdodávky

1) V rámci řešení Projektu nebudou realizovány subdodávky.

2) Pokud se v průběhu řešení Projektu vyskytne potřeba realizace subdodávky, postupuje příjemce podle zákona č. 134/2016 Sb. o zadávání veřejných zakázek (dále jen „zákon č. 134/2016 Sb.).

3) Subdodávky je příjemce povinen pořizovat za tržní ceny (tj. cena v místě a čase obvyklá). Toto je příjemce povinen poskytovateli doložit.

4) Subdodávky na výzkum nebo experimentální vývoj mohou být realizovány maximálně do výše 20 % celkových uznaných nákladů Projektu.

5) Nové subdodávky musí být předem odsouhlaseny poskytovatelem a upraveny písemným dodatkem ke Smlouvě.

6) Je-li subdodavatelem veřejně financovaná výzkumná organizace, mohou být předmětem subdodávek pouze výzkum nebo experimentální vývoj za těchto podmínek:

   a) výzkumná organizace poskytuje danou výzkumnou službu nebo provádí smluvní výzkum za tržní cenu nebo

   b) nelze-li určit tržní cenu, výzkumná organizace poskytne danou výzkumnou službu nebo provede smluvní výzkum za cenu, která zahrnuje plné náklady a přiměřený zisk.

7) Je-li příjemce výzkumnou organizací, může pořizovat subdodávky pouze od jiné výzkumné organizace.

8) Při pořízení subdodávek v rozporu s tímto článkem bude postupováno dle Článku 20 Smlouvy.

Článek 10
Vedení účetnictví o uznaných nákladech Projektu

1) O vynaložených nákladech Projektu je příjemce povinen po celou dobu řešení Projektu vést v účetnictví oddělenou evidenci podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů v souladu s § 8 odst. 1 zákona č. 130/2002 Sb.

2) Nezpůsobilými náklady projektu jsou zejména:
   - zisk,
   - daň z přidané hodnoty (u příjemců, kteří jsou plátci této daně a kteří uplatňují její odpočet nebo odpočet její poměrné části)[2],
   - jiné daně (silniční daň, daň z nemovitosti, daň darovací, dědická, apod.),
   - náklady na marketing, prodej a distribuci výrobků,
   - úroky z dluhů,

[2] Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů

- náklady na finanční pronájem a pronájem s následnou koupí (např. leasing, aj.),
- manka a škody,
- náklady na pohoštění, dary a reprezentaci,
- náklady na vydání periodických publikací, učebnic a skript,
- náklady/výdaje na pořízení budov a pozemků,
- opravy nebo údržba místností, stavby, rekonstrukce budov nebo místností, nábytek či zařízení, která nejsou pevnou součástí místností, a další náklady, které bezprostředně nesouvisejí s předmětem řešení projektu,
- správní poplatky,
- výdaje související s likvidací příjemce, nedobytné pohledávky,
- platby příspěvků do soukromých penzijních fondů,
- peněžitá pomoc v mateřství,
- ostatní sociální výdaje na zaměstnance, které nejsou zaměstnavatelé povinni odvádět dle zvláštních předpisů (např. dary k životním jubileím, příspěvky na rekreaci, příspěvky na penzijní připojištění, životní pojištění apod.),
- odstupné,
- nájemné, kdy příjemce je vlastníkem nemovitosti nebo ji užívá zdarma,
- výdaje na školení a vzdělávání personálu (pokud se nejedná o odborné akce přímo související s řešením projektu).

3) Do uznaných nákladů na pořízení hmotného a nehmotného majetku lze zahrnout pouze část ceny majetku, která odpovídá podílu užití majetku na řešení Projektu.

4) Příjemce účtuje doplňkové náklady související s Projektem **metodou kalkulace úplných nákladů (FC - Full Costs).**

5) V případě, že příjemce předpokládá nevyčerpání finančních prostředků daného kalendářního roku, ale využil by je v rámci projektu v roce následujícím, je povinen požádat poskytovatele o schválení využití těchto nespotřebovaných finančních prostředků, a to do 15. listopadu daného kalendářního roku cestou změnového řízení. V případě, že bude jeho žádost poskytovatelem schválena, ponechá si příjemce tyto nespotřebované finanční prostředky na svém účtu. V případě, že žádost nebude poskytovatelem schválena, příjemce tyto nespotřebované finanční prostředky převede obratem na bankovní účet poskytovatele číslo [redacted] při převodu finančních prostředků příjemce uvede do Zprávy pro příjemce: VRATKA-NESPOTŘEBOVANÉ PROSTŘEDKY, kód projektu, svůj název).

6) Je-li příjemce veřejnou výzkumnou institucí nebo veřejnou vysokou školou, může finanční prostředky, které nemohly být efektivně použity v roce, ve kterém byly poskytnuty, nad rámec odstavce 5 tohoto článku, převést do fondu účelově určených prostředků, a to do výše 5 % objemu těchto prostředků poskytnutých na Projekt v daném kalendářním roce. Takto převedené prostředky mohou být použity pouze k účelu, ke kterému byly poskytnuty.[3] Převod musí příjemce písemně prokazatelně oznámit poskytovateli a odůvodnit.

7) Příjemce finanční prostředky daného kalendářního roku, u kterých předpokládá jejich nevyčerpání v daném kalendářním roce a nepostupuje-li dle odstavce 5 a 6 tohoto článku, převede nejpozději do konce listopadu daného kalendářního roku na bankovní účet poskytovatele číslo [redacted] při převodu finančních prostředků příjemce uvede do Zprávy pro příjemce: VRATKA-NESPOTŘEBOVANÉ PROSTŘEDKY, kód projektu, svůj název).

8) V případě, že příjemci zůstanou nevyužité finanční prostředky daného kalendářního roku, s výjimkou postupu podle odstavce 5 až 7 tohoto článku, je povinen tyto prostředky poskytovateli vrátit do 15. února následujícího roku převedením na bankovní účet poskytovatele číslo [redacted] při převodu finančních prostředků příjemce

[3] § 18 odst. 9, 10, 11 zákona č. 111/1998 Sb., o vysokých školách; § 26 zákona č. 341/2005 Sb., o veřejných výzkumných institucích;

uvede do Zprávy pro příjemce: VRATKA-NEVYUŽITÉ PROSTŘEDKY, kód projektu, svůj název). Tyto prostředky budou poskytovatelem odvedeny do státního rozpočtu.

9) V případě, že příjemci v letech následujících po prvním roce řešení zůstanou nevyužité finanční prostředky, které si ponechal na svém účtu podle odstavce 5 tohoto článku, je povinen tyto prostředky poskytovateli vrátit do 15. února následujícího roku převedením na bankovní účet poskytovatele číslo [redacted] (při převodu finančních prostředků příjemce uvede do Zprávy pro příjemce: VRATKA-NEVYUŽITÉ PROSTŘEDKY, kód projektu, svůj název). Tyto prostředky budou poskytovatelem odvedeny do státního rozpočtu.

10) V posledním roce řešení převede příjemce finanční prostředky daného kalendářního roku, které předpokládá nevyčerpat do konce řešení projektu, nejpozději do 15. prosince daného kalendářního roku na bankovní účet poskytovatele číslo [redacted] (při převodu finančních prostředků příjemce uvede do Zprávy pro příjemce: VRATKA-KONEČNÉ NESPOTŘEBOVANÉ PROSTŘEDKY, kód projektu, svůj název).

11) V případě, že zůstanou na účtu příjemce ke dni 31. prosince daného kalendářního roku, který je posledním rokem řešení projektu, nějaké nevyužité finanční prostředky daného kalendářního roku a nevyužité finanční prostředky, které si ponechal na svém účtu podle odstavce 5 a 6 tohoto článku, je povinen tyto prostředky poskytovateli vrátit do 31. ledna následujícího roku převedením na bankovní účet poskytovatele číslo [redacted] při převodu finančních prostředků příjemce uvede do Zprávy pro příjemce: VRATKA-KONEČNÉ NEVYUŽITÉ PROSTŘEDKY, kód projektu, svůj název) a provést finanční vypořádání podpory se státním rozpočtem dle Článku 11 odst. 4 Smlouvy.

12) Nebude-li příjemce postupovat dle povinností uvedených v odstavci 5 až 11, může poskytovatel postupovat dle Článku 20 odst. 3 Smlouvy.

13) Pokud příjemce uplatňuje rozdílný hospodářský rok, provádí vyúčtování nákladů na Projekt a poskytnuté podpory k 31. prosinci daného kalendářního roku a při uzávěrce hospodářského roku provede kontrolu tohoto vyúčtování a o výsledku písemně informuje poskytovatele.

Článek 11
Povinnosti příjemce

1) Příjemce je povinen postupovat při řešení Projektu v souladu s Projektem a dalšími podmínkami uvedenými ve Smlouvě.

2) Příjemce je povinen použít podporu v souladu s podmínkami, účelem a způsobem stanovenými Smlouvou. Použije-li příjemce podporu v rozporu s podmínkami stanovenými Smlouvou na jiný účel nebo jiným způsobem, závažným způsobem poruší povinnosti stanovené Smlouvou. V takovém případě bude postupováno dle Článku 20 odst. 4 Smlouvy.

3) Příjemce je povinen dodržovat podmínky uvedené v Projektu, na jejichž základě byla stanovena maximální povolená výše míry podpory. Porušení této povinnosti se pokládá za závažné porušení povinnosti a bude postupováno dle Článku 20 odst. 4 Smlouvy.

4) Příjemce je povinen provést finanční vypořádání poskytnuté dotace v souladu s § 14 odst. 10 a § 75 zákona o rozpočtových pravidlech a příslušnými předpisy pro zúčtování se státním rozpočtem platnými pro daný rok. Finanční vypořádání zpracuje příjemce za období týkající se celé doby trvání Projektu podle stavu k 31. prosinci roku, v němž bylo ukončeno financování Projektu. Příjemce předloží poskytovateli podklady pro finanční vypořádání dotace do 15. února roku následujícího po roce ukončení Projektu na tiskopisu, jehož vzor je uveden v přílohách příslušných předpisů pro zúčtování se státním rozpočtem platných pro daný rok.

5) Příjemce je povinen písemně informovat poskytovatele o veškerých podstatných skutečnostech, které by mohly mít vliv na průběh a výsledek řešení Projektu

a které nastaly v době ode dne nabytí platnosti a účinnosti Smlouvy, a to ve lhůtě do 15 kalendářních dnů ode dne, kdy se o takové skutečnosti dozvěděl.

6) Podstatnou změnou, pro jejíž provedení je nutný předchozí souhlas poskytovatele je změna harmonogramu projektu, změna výsledků projektu, změna data ukončení řešení projektu, změna manažera Projektu a změna hlavního řešitele Projektu. Pokud příjemce neobdrží stanovisko poskytovatele do 15 pracovních dnů ode dne odeslání informace o podstatné změně, považuje se podstatná změna za schválenou poskytovatelem. Poskytovatel může lhůtu prodloužit o 15 pracovních dnů; je však povinen o prodloužení lhůty příjemce písemně informovat. Formulář pro změnové řízení dle tohoto ustanovení je zveřejněn na webových stránkách Ministerstva vnitra. Při postupu příjemce v rozporu s tímto ustanovením, bude postupováno dle ustanovení Článku 20 odst. 3 Smlouvy.

7) Změny členů řešitelského týmu je příjemce povinen se zdůvodněním oznámit poskytovateli do 7 pracovních dnů od jejich provedení. Pokud by změnou ve složení řešitelského týmu mělo dojít k přesunu finančních prostředků mezi jednotlivými položkami v rámci rozpočtové skupiny osobní náklady, je příjemce povinen postupovat dle Článku 7 odst. 1 písm. d) Smlouvy. Oznámení o změně řešitelského týmu musí obsahovat formulář čerpání osobních nákladů, který je s formulářem pro personální změnu zveřejněn na webových stránkách Ministerstva vnitra. Při postupu příjemce v rozporu s tímto ustanovením, bude postupováno dle ustanovení Článku 20 odst. 3 Smlouvy.

8) O ostatních změnách informuje příjemce poskytovatele průběžně, nejpozději v roční zprávě dle Článku 12 odst. 2 Smlouvy.

9) Příjemce je povinen každou zahraniční pracovní cestu, jejíž náklady přesáhnou 100 000,- Kč, předložit s předstihem nejméně 30 kalendářních dní před zahájením zahraniční pracovní cesty se zdůvodněním poskytovateli ke schválení. Nejpozději do 30 kalendářních dní po ukončení cesty je příjemce povinen předložit poskytovateli podrobnou zprávu o jejím průběhu a výsledcích ve vztahu k řešení Projektu.

10) Veškerá oznámení dle tohoto článku předává příjemce formou a ve lhůtách, které jsou uvedeny ve Smlouvě.

11) Příjemce je povinen poskytnout i další údaje požadované poskytovatelem pro věcné a finanční řízení Projektu, a to v termínech stanovených poskytovatelem.

Článek 12
Zprávy

1) Příjemce předkládá poskytovateli ke schválení v průběhu řešení Projektu zprávy o průběhu řešení Projektu (roční zprávy, mimořádné zprávy). Po ukončení řešení Projektu příjemce předloží poskytovateli závěrečnou zprávu.

2) Roční zprávu je příjemce povinen předložit poskytovateli za každý rok řešení Projektu vždy ve lhůtě do 15. ledna následujícího kalendářního roku, nestanoví-li poskytovatel písemně jinak. Roční zpráva obsahuje zejména informace o postupu řešení Projektu, o dosažených výsledcích a způsobu jejich využití v uplynulém roce. V roční zprávě zároveň příjemce upřesní postup řešení Projektu na další rok a předloží aktuální verzi harmonogramu. Samostatnou částí roční zprávy je vyúčtování nákladů na Projekt a poskytnuté podpory za uplynulý rok ve struktuře Rozpočtu a aktuální verze rozpočtu. Roční zprávu podle první věty je příjemce povinen předložit rovněž za poslední rok řešení projektu. V případě oznámení změn v roční zprávě podle Článku 7 odst. 2 a Článku 11 odst. 8 Smlouvy je povinností příjemce k roční zprávě přiložit příslušný formulář pro změnové řízení zveřejněný na webových stránkách Ministerstva vnitra.

3) Mimořádnou zprávu předkládá příjemce poskytovateli v průběhu řešení Projektu na vyžádání poskytovatele, který zároveň stanoví předmět zprávy a termín jejího předložení.

4) Závěrečnou zprávu z řešení Projektu předloží příjemce do 30 kalendářních dnů ode dne ukončení řešení Projektu uvedeného v Článku 5 Smlouvy. Závěrečná zpráva z řešení Projektu zahrnuje zejména informaci o dosažených cílech, výsledcích, způsobu jejich využití a výstupech Projektu. Součástí závěrečné zprávy je vyúčtování nákladů na

Projekt a poskytnuté podpory za celé období řešení Projektu ve struktuře Rozpočtu. Přílohou závěrečné zprávy jsou materiály, kterými příjemce dokládá, že výsledky existují a jejich funkčnost, jako jsou například technická dokumentace, rozhodnutí nebo certifikace výsledků.

5) Příjemce je povinen předkládat poskytovateli zprávu o využití výsledků Projektu v souladu s Popisem výsledků projektu a plánem jejich využití, který je přílohou č. 2 Smlouvy, a to každoročně po dobu 5 let ode dne ukončení Smlouvy, vždy ve lhůtě do 20. ledna následujícího kalendářního roku.

6) U Projektů obsahujících utajované informace budou zprávy uvedené v tomto článku zpracovávány v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon č. 412/2005 Sb.“).

7) Poskytovatel stanoví rozsah, strukturu a formu zpráv uvedených v tomto článku.

8) Poskytovatel schvaluje roční a mimořádné zprávy nejpozději do 30 kalendářních dnů ode dne jejich doručení nebo v této lhůtě uplatní písemné připomínky a stanoví lhůtu pro jejich vypořádání příjemcem.

9) Pokud příjemce nepředloží zprávy uvedené v odstavci 1 až 4 tohoto článku, bude postupováno dle Článku 20 odst. 3 Smlouvy.

Článek 13
Kontroly

1) Poskytovatel je oprávněn ve smyslu § 13 zákona č. 130/2002 Sb. provádět u příjemce kontrolu plnění cílů Projektu, včetně kontroly čerpání a využívání podpory a účelnosti vynaložených prostředků podle této Smlouvy.

2) Poskytovatel je oprávněn provádět finanční kontrolu v souladu se zákonem č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů a provádět kontrolu podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád).

3) Příjemce je povinen umožnit poskytovateli provedení všech kontrol uvedených v odstavci 1 a 2 tohoto článku a poskytnout mu při nich potřebnou součinnost, zejména poskytnout na pracovištích příjemce volný přístup k osobám podílejícím se na řešení Projektu, ke všem dokumentům, počítačovým záznamům a zařízením, která přísluší k řešení Projektu.

4) Příjemce je povinen předložit na žádost poskytovatele pro potřeby kontroly Projektu originály veškerých účetních dokladů vztahujících se k Projektu.

5) Příjemce je povinen předkládat poskytovateli na vyžádání přehledy jakýchkoliv účetních záznamů vztahujících se k Projektu.

6) Osoby provádějící kontrolu jsou povinny předložit příjemci písemné pověření ředitele věcně příslušného odboru poskytovatele k provedení kontroly.

7) Kontrolu je poskytovatel oprávněn provést kdykoliv v době řešení Projektu a následně ve lhůtě do 5 let ode dne ukončení Smlouvy. Příjemce je povinen po celou tuto dobu uchovávat veškeré doklady týkající se Projektu.

Článek 14
Nákup a vlastnictví majetku pořízeného pro řešení Projektu

1) V rámci řešení Projektu příjemce nebude pořizovat hmotný a nehmotný majetek.

2) Pokud se v průběhu řešení Projektu vyskytne potřeba pořídit hmotný a nehmotný majetek, postupuje se podle zákona č. 134/2016 Sb.

3) Hmotný a nehmotný majetek je příjemce povinen pořizovat za tržní ceny (tj. cena v místě a čase obvyklá). Toto je příjemce povinen poskytovateli doložit.

4) Vlastníkem majetku, pořízeného z poskytnuté podpory je ve smyslu ustanovení § 15 odst. 1 zákona č. 130/2002 Sb. příjemce.

5) Při pořízení majetku v rozporu s tímto článkem bude postupováno dle Článku 20 Smlouvy.

Článek 15
Práva k výsledkům Projektu a jejich využití

1) Práva k výsledkům Projektu patří příjemci.

2) Při využití výsledků Projektu je příjemce povinen postupovat v souladu s ustanovením § 16 odst. 4 zákona č. 130/2002 Sb. a Popisem výsledků projektu a plánem jejich využití.

Článek 16
Poskytování informací

1) Příjemce je povinen předávat poskytovateli veškeré informace o Projektu pro účely jejich předání do informačního systému výzkumu, experimentálního vývoje a inovací ve formě a termínech stanovených poskytovatelem v souladu se zákonem č. 130/2002 Sb. a NV č. 397/2009 Sb., a další informace stanovené poskytovatelem.

2) Při jakémkoliv předávání nebo zveřejňování informací týkajících se Projektu a výsledků Projektu, včetně konferencí, je příjemce povinen zveřejnit informaci o poskytnuté podpoře poskytovatelem na základě Smlouvy a o příslušnosti k programu výzkumu a vývoje poskytovatele.

3) Pokud je předmět řešení Projektu utajovanou informací podle zákona č. 412/2005 Sb., je příjemce povinen uvést stupeň důvěrnosti těchto údajů podle zákona č. 412/2005 Sb., a poskytnout poskytovateli konkrétní informace o Projektu a jeho výsledcích postupem podle zákona č. 130/2002 Sb.

4) Příjemce je povinen při změně Smlouvy předat poskytovateli informace o změně údajů zveřejňovaných v informačním systému výzkumu, experimentálního vývoje a inovací, pokud k takovéto změně v důsledku změny Smlouvy dojde.

Článek 17
Povinnost mlčenlivosti

1) Poskytovatel a příjemce jsou povinni zajistit mlčenlivost o všech informacích, které jim jako důvěrné byly poskytnuty a jejichž předání dalším subjektům by mohlo poškodit práva toho, kdo je poskytl.

2) V případě, že jsou poskytovatel a příjemce na základě Smlouvy oprávněni poskytovat informace třetím stranám, jsou povinni zajistit, aby tyto třetí strany zachovávaly mlčenlivost o těchto informacích, které jim byly poskytnuty jako důvěrné, a používaly je jen k účelům, k nimž jim byly předány.

3) Poskytovatel a příjemce jsou zproštěni povinnosti zachovávat mlčenlivost v případě:

   a) že se obsah informací, které jim byly poskytnuty jako důvěrné, stane veřejně přístupným, a to na základě jiných činností prováděných mimo rámec Smlouvy nebo na základě opatření, která nesouvisí s řešením Projektu;

   b) že byl požadavek zachovávat mlčenlivost odvolán těmi, v jejichž prospěch byla tato povinnost stanovena.

Článek 18
Odpovědnost za škodu

1) Odpovědnost za škodu se řídí ustanoveními občanského zákoníku.

2) Poskytovatel neodpovídá za jednání nebo za nečinnost příjemce. Poskytovatel neodpovídá za nedostatky výrobků vytvořených nebo služeb poskytnutých na základě výsledků Projektu.

3) Příjemce se zavazuje, že odškodní třetí strany v případě uplatnění požadavku na náhradu škody, která vznikla jednáním nebo nečinností příjemce nebo která souvisí s nedostatky výrobků vytvořených nebo služeb poskytnutých na základě výsledků Projektu, pokud neprokáže, že za tyto neodpovídá.

4) Prokáže-li třetí strana své nároky spojené s prováděním Smlouvy vůči poskytovateli, je příjemce povinen poskytovateli poskytnout pomoc.

Článek 19
Odstoupení od Smlouvy

1) Poskytovatel je oprávněn od Smlouvy odstoupit v případě, že:

   a) příjemce uvedl neúplné, nesprávné nebo nepravdivé údaje a skutečnosti ve veřejné soutěži nebo při uzavření Smlouvy;

   b) příjemce nesplnil povinnosti nebo jiné podmínky stanovené Smlouvou ani poté, co jej poskytovatel k tomu písemně vyzval a stanovil mu náhradní dobu k jejich splnění; náhradní doba k plnění nesmí být kratší než 30 kalendářních dnů;

   c) příjemce vstoupil do likvidace nebo na něho byla vyhlášena nucená správa, vůči majetku příjemce probíhá insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh nebyl zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení, nebo nebyl konkurs zrušen proto, že majetek byl zcela nepostačující, byla povolena reorganizace nebo byl nařízen výkon rozhodnutí prodejem podniku, pokud by tato skutečnost mohla dle názoru poskytovatele ovlivnit řešení Projektu nebo zájmy poskytovatele;

   d) dojde ke vzniku závažných ekonomických nebo technických důvodů, které podstatně ovlivní řešení Projektu, nebo se výrazně sníží možnost využití poznatků Projektu;

   e) z důvodu podstatného porušení Smlouvy podle § 2002 odst. 1 občanského zákoníku.

2) Odstoupení od Smlouvy musí být odůvodněno a nabývá účinnosti dnem jeho doručení příjemci.

Článek 20
Vrácení podpory a sankce

1) V případě odstoupení od Smlouvy podle ustanovení Článku 19 odst. 1 písm. a), b) a e) Smlouvy je příjemce povinen vrátit poskytnutou podporu poskytovateli v plné výši. K vrácené podpoře je příjemce povinen zaplatit smluvní pokutu ve výši 0,1 % z částky podpory uvedené v Projektu pro rok, v němž vznikl důvod k odstoupení od Smlouvy, a to za každý den za dobu ode dne připsání poskytnuté podpory, která má být vrácena, na bankovní účet příjemce do dne jejího připsání na účet poskytovatele.

2) V případě odstoupení od Smlouvy podle ustanovení Článku 19 odst. 1 písm. c) a d) Smlouvy a v případě uzavření dohody o ukončení Smlouvy je příjemce povinen vrátit poskytnutou podporu v poměrné výši, stanovené poskytovatelem, a to ve lhůtě do 30 kalendářních dnů ode dne doručení sdělení o odstoupení od Smlouvy nebo ode dne nabytí účinnosti dohody o ukončení Smlouvy. Z poskytnuté podpory mohou být uhrazeny jen uznané náklady Projektu použité příjemcem na poskytovatelem schválené výstupy z Projektu, kterých bylo dosaženo do okamžiku odstoupení od Smlouvy, případně ukončení Smlouvy dohodou.

3) V případě, že příjemce neinformuje poskytovatele dle Článku 7, Článku 10 odst. 5 až 11, Článku 11 odst. 6 a 7, Článku 12 odst. 1 až 4 této Smlouvy, poskytovatel uloží příjemci smluvní pokutu ve výši 2 % z částky podpory uvedené v Projektu pro rok, v němž vznikl důvod k uložení smluvní pokuty. Podpora pro následující kalendářní rok bude příjemci poskytnuta ve výši, snížené o uplatněnou smluvní pokutu.

4) V případě, že příjemce použije poskytnutou podporu nebo část poskytnuté podpory v rozporu s podmínkami, účelem nebo způsobem stanovenými touto Smlouvou, je poskytovatel oprávněn požadovat od příjemce vrácení takto použitých prostředků.

Příjemce je povinen tyto prostředky převést na účet poskytovatele, a to ve lhůtě do 30 kalendářních dnů ode dne, kdy byl tento požadavek poskytovatele písemně doručen příjemci.

5) V případě, že příjemce nevyužije výsledky Projektu nebo neumožní jejich využití dle § 16 odst. 4 zákona č. 130/2002 Sb., vrátí poskytovateli poskytnutou podporu v plné výši.

6) V případě, že u příjemce byly po ukončení Smlouvy zjištěny na základě provedené kontroly závažné finanční nesrovnalosti nebo podvod, může poskytovatel od příjemce písemně požadovat vrácení poskytnuté podpory v celé výši. K vrácené podpoře je příjemce povinen zaplatit smluvní pokutu ve výši 0,1 % z poskytnuté podpory za každý den, a to za dobu ode dne připsání poskytnuté podpory, která má být vrácena, na bankovní účet příjemce do dne jejího připsání na účet poskytovatele.

7) Poskytnutá podpora nebo její poměrná část se vrací a smluvní pokuta se platí připsáním na bankovní účet poskytovatele, který bude příjemci poskytovatelem sdělen.

8) Neoprávněné použití nebo zadržení podpory se posuzuje jako porušení rozpočtové kázně podle zákona o rozpočtových pravidlech.

9) Poskytovatel je oprávněn přerušit nebo zastavit poskytování podpory příjemci, pokud jsou naplněny skutkové podstaty, pro které může být Smlouva ukončena v souladu s ustanovením Článku 19 odst. 1 Smlouvy. Ustanovením tohoto odstavce nejsou dotčena práva poskytovatele stanovená Smlouvou. Příjemci nenáleží náhrada škody, která mu vznikne v důsledku přerušení nebo zastavení poskytování podpory.

10) Tímto článkem není dotčen nárok poskytovatele na náhradu škody, která mu vznikne v důsledku neplnění Smlouvy příjemcem.

Článek 21
Ukončení řešení Projektu a ukončení Smlouvy

1) Příjemce je povinen řešení Projektu ukončit nejpozději ke dni uvedenému v Článku 5 Smlouvy. Řešení Projektu se považuje za ukončené rovněž v případě předčasného zastavení řešení Projektu v souvislosti s ukončením Smlouvy v souladu s ustanovením tohoto článku odstavec 4 písm. b) a c) Smlouvy.

2) Po ukončení řešení Projektu poskytovatel provede závěrečné hodnocení Projektu, zejména zhodnocení plnění cílů Projektu, včetně kontroly čerpání a využívání podpory, účelnosti vynaložených prostředků Projektu podle Smlouvy a dále provede závěrečné zhodnocení dosažených výsledků Projektu a jejich vztah k cílům Projektu.

3) Smlouva je splněna dnem schválení závěrečné zprávy poskytovatelem a úspěšným závěrečným hodnocením Projektu poskytovatelem v souladu s § 13 odst. 4 zákona č. 130/2002 Sb.

4) Smlouva je ukončena:

   a) dnem ukončení Smlouvy stanoveným ve Smlouvě v Článku 25 odst. 2,

   b) dnem doručení písemného odstoupení od Smlouvy poskytovatelem,

   c) dnem nabytí účinnosti dohody smluvních stran o ukončení Smlouvy.

5) Po ukončení Smlouvy je poskytovatel oprávněn podle § 9 odst. 1 písm. k) zákona č. 130/2002 Sb. provádět u příjemce kontrolu využití výsledků Projektu v souladu s § 16 zákona č. 130/2002 Sb., Popisem výsledků projektu a plánem jejich využití, a to ve lhůtě do 5 let ode dne ukončení Smlouvy.

Článek 22
Doručování písemností

1) Písemnosti dle Smlouvy se doručují na adresu poskytovatele nebo příjemce uvedenou v této Smlouvě. V případě doručování prostřednictvím provozovatele poštovní služby je náhradní doručení uložením zásilky možné. V takovém případě se považuje písemnost za doručenou 10. kalendářní den ode dne oznámení o uložení zásilky na poště.
2) Písemnosti v elektronické formě lze doručovat do datové schránky poskytovatele nebo příjemce podle zvláštního zákona[4], s výjimkou ustanovení Článku 12 odst. 6 Smlouvy. Písemnost se považuje za doručenou nejpozději 10. kalendářní den ode dne, kdy byl dokument dodán do datové schránky.

Článek 23
Spory smluvních stran

Spory smluvních stran vznikající ze Smlouvy nebo v souvislosti s ní, budou řešeny příslušným soudem.

Článek 24
Závěrečná ustanovení

1) Smlouva, včetně příloh, může být doplňována, upravována a měněna pouze písemnými, po sobě číslovanými dodatky ke Smlouvě, podepsanými smluvními stranami.
2) Nestanoví-li Smlouva jinak, návrh posledního dodatku ke Smlouvě lze doručit druhé smluvní straně nejpozději 60 kalendářních dnů přede dnem ukončení řešení Projektu uvedeným v Článku 5 Smlouvy.
3) Smlouva se řídí právním řádem České republiky.
4) Vztahy neupravené Smlouvou se řídí především zákonem č. 130/2002 Sb. a občanským zákoníkem.
5) Základní ustanovení Smlouvy (Články 1 až 25 Smlouvy) mají v případě rozporu přednost před ustanoveními Projektu.
6) Nedílnou součástí Smlouvy jsou:
   a) Příloha č. 1 - Projekt,
   b) Příloha č. 2 - Popis výsledků projektu a plán jejich využití.
7) Smlouva se vyhotovuje ve dvou stejnopisech, z nichž poskytovatel i příjemce obdrží po jejich podpisu jedno vyhotovení.
8) Smluvní strany prohlašují a podpisem Smlouvy stvrzují, že jimi uvedené údaje, na jejichž základě je uzavřena Smlouva a poskytnuta podpora poskytovatelem, jsou správné, úplné a pravdivé.
9) Smluvní strany prohlašují, že si tuto Smlouvu přečetly, s jejím obsahem souhlasí a že byla sepsána na základě jejich pravé a svobodné vůle, a na důkaz toho připojují své podpisy.

[4] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

Článek 25
Platnost a účinnost Smlouvy

1) Smlouva se uzavírá na dobu určitou a nabývá platnosti dnem podpisu obou smluvních stran a účinnosti od 1. 7. 2019, pokud právní předpis nestanoví jinak.
2) Smlouva je ukončena dnem 29. 6. 2023.
3) Ukončení Smlouvy před datem uvedeným v odstavci 2 tohoto článku je upraveno v ustanovení Článku 21 odst. 4 písm. b) a c) Smlouvy.

Za poskytovatele:	Za příjemce:
JUDr. Petr Novák, Ph.D.	doc. PhDr. Mikuláš Bek, Ph.D.
V Praze dne:	V dne:

Nástroje pro simulaci útoků a emulaci průniku do kritické informační infrastruktury

Program: **BV III/1-VS**

Uchazeč: **Masarykova univerzita**

Další účastníci: **0**

Hlavní obor: **IN - Informatika**

Vedlejší obor: **JC - Počítačový hardware a software**

Stupeň důvěrnosti údajů: **S - údaje jsou zveřejnitelné a odpovídají skutečnosti**

1. Identifikační údaje Programu a vyhlášení veřejné soutěže

1.1 Kód Programu

Kód Programu
VI

1.2 Název Programu

Název Programu
Program bezpečnostního výzkumu České republiky 2015-2022

1.3 Dílčí cíl, který nejvíce odpovídá zamýšlené oblasti uplatnění výsledků

Název tematické oblasti v rámci daného dílčího cíle Programu, která bude projektem řešena
2d) Účinná detekce a identifikace hrozeb kritické infrastruktury

1.4 Číslo a datum vyhlášení

Číslo a datum vyhlášení
Vyhlášení třetí VS z 23.08.2018.

2. Identifikace projektu

2.1 Název projektu

Název projektu

Nástroje pro simulaci útoků a emulaci průniku do kritické informační infrastruktury

2.2 Název projektu anglicky

Název projektu anglicky

Breach Emulation and Attack Simulation Toolkit

2.3 Anotace projektu

Anotace projektu

Cílem projektu je vytvoření sady nástrojů, které umožní částečně nahradit experty na penetrační testování. Díky zaměření se na automatizaci statického i dynamického testování kyberbezpečnosti poskytne prostředky pro nepřetržité monitorování a vyhodnocování zabezpečení cílové infrastruktury, pro realizaci kyberbezpečnostních cvičení a poslouží jako podklad pro bezpečnostní certifikaci. Svým důrazem na automatizaci výrazně sníží požadavky na množství a expertízu personálu bezpečnostních týmů.

2.4 Anotace projektu anglicky

Anotace projektu anglicky

The aim of this project is creating a toolkit to partially replace penetration testing experts. By focusing on automation of static and dynamic testing of cybersecurity, it will provide means for continuous monitoring and security evaluation of target infrastructure, for implementation of cyber defense exercises, and will serve as a basis for security certification. Its emphasis on automation will significantly lower requirements on the number and expertise of security teams' personnel.

2.5 Kategorie činnosti

Kategorie činnosti

experimentální vývoj

2.6 Předpokládané datum zahájení projektu

Předpokládané datum zahájení projektu

01.01.2020

2.7 Datum ukončení projektu

Datum ukončení projektu

31.12.2022

2.8 Projekt má více uchazečů

Projekt má více uchazečů

NE

2.9 Klíčová slova

Klíčová slova

Kyberbezpečnost; penetrační testování; automatizace; kontinuální testování; BAS; kyberbezpečnostní cvičení; CDX; KII; VIS;

2.10 Klíčová slova anglicky

Klíčová slova anglicky

Cybersecurity; penetration testing; automation; continuous testing; BAS; cyber defense exercise; CDX; KII; VIS;

3. Identifikace uchazeče

3.1 Název uchazeče

Název uchazeče
Masarykova univerzita
Organizační jednotka
14610 - Ústav výpočetní techniky

3.2 Právní forma

Právní forma
VVS - veřejná nebo státní vysoká škola (zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů)

3.3 IČ

IČ
00216224

3.4 DIČ

DIČ
CZ00216224

3.5 Sídlo uchazeče

Státní příslušnost			
CZ - Česká republika			
Kraj	Obec		
Jihomoravský	Brno		
Ulice	Č. popisné	Č. orientační	PSČ
Žerotínovo náměstí	617	9	60177
Telefon	E-mail		
+420549491011	info@rect.muni.cz		
Web stránka			
www.muni.cz			

3.7 Statutární zástupce/zástupci uchazeče

Titul před jménem	Jméno	Příjmení	Titul za jménem
doc. PhDr.	Mikuláš	Bek	Ph.D.
Pracovní pozice osoby na pracovišti			
rektor			
Telefon	Fax	E-mail	
+420549491001	+420549491070	rektor@muni.cz	

3.8 Kategorie uchazeče

Kategorie uchazeče
VO - výzkumná organizace

3.9 Popis předchozích zkušeností uchazeče v oblasti výzkumu a vývoje za posledních 5 let

Popis předchozích zkušeností uchazeče v oblasti výzkumu a vývoje za posledních 5 let

Masarykova univerzita (MU) je pravidelným úspěšným uchazečem o projekty výzkumu a vývoje napříč programovými rámci vyhlašovanými v ČR i v zahraničí. MU spolupracuje s partnery z komerční i neziskové sféry. Řešitelský tým má dlouholeté zkušenosti v oblasti základního i aplikačně orientovaného výzkumu a vývoje a uplatnění dosažených výsledků do praxe. Subjekty využívající dosažené výsledky jsou podniky a státní organizace (NÚKIB, Policie ČR, Armáda ČR).

V rámci programu Bezpečnostního výzkumu řešila MU projekt VG20132015103, který vytvořil software pro unikátní prostředí Kybernetického polygonu (KYPO). Projekt byl oceněn Cenou ministra vnitra za mimořádné výsledky v oblasti bezpečnostního výzkumu v roce 2016. Na projekt KYPO navázal projekt Simulace, detekce a potlačení kybernetických hrozeb ohrožujících kritickou infrastrukturu (VI20162019014). Výsledky obou projektů jsou úspěšně používány při realizaci národních technických cvičení Cyber Czech. Další řešené projekty Bezpečnostního výzkumu jsou např. VI20172020070, VI20162019029 a VF20132015031 a zaměřují se na vývoj technologií určených pro ochranu kritických informačních infrastruktur.

Špičkový základní výzkum uchazeče reprezentuje projekt Centra excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur (C4e), který se zaměřuje na výzkum komplexních problémů kyberprostoru. Mezinárodní přesah prováděného bezpečnostního výzkumu potvrzuje získání H2020 projektu Cyber security competence for research and innovation (830927).

Popis předchozích zkušeností uchazeče v oblasti výzkumu a vývoje za posledních 5 let

Výzkum a vývoj pro komerční sektor (společnosti AXENTA, ČEPS, ČEZ, Flowmon Networks aj.) zahrnuje poskytování znalostí formou smluvního výzkumu, inovačních voucherů a projektů aplikovaného výzkumu a experimentálního vývoje TA ČR (TA04010062, TH02010185).

3.10 Úspěšně vyřešené projekty uchazeče v oblasti výzkumu a vývoje v posledních deseti letech

Identifikátor	Název
OVMASUN200801	CYBER – Bezpečnost informačních a komunikačních systémů AČR – on line monitorování, vizualizace a filtrace paketů. Rozvoj schopností Computer Incident Response Capability v prostředí Cyber Defence.

Oblast výzkumu a vývoje

Výzkum a vývoj v oblasti ochrany informačních a komunikačních systémů proti kybernetickým útokům. Analýza jednotlivých druhů hrozeb (vzorů chování) a specifikace postupů a metodik, jak naplnění těchto hrozeb odhalit a bránit se jim.

Výsledky evidované v RIV

D – Článek ve sborníku – Čeleda, P. et al. Revealing and Analysing Modem Malware. 2012. (RIV/00216224:14610/12:00058686).
D – Článek ve sborníku – Čeleda, P. et al. Flow-Based Security Issue Detection in Building Automation and Control Networks. 2012. (RIV/00216224:14610/12:00058685).
D – Článek ve sborníku – Vykopal, J. et al. Network-based Dictionary Attack Detection. 2009. (RIV/00216224:14610/09:00040909).

Identifikátor	Název
VG20132015103	Kybernetický polygon

Oblast výzkumu a vývoje

Výzkum a vývoj unikátního prostředí pro analýzu hrozeb ohrožujících bezpečnost kritických informačních infrastruktur. V prostředí polygonu lze provádět komplexní scénáře útoků vedených proti kritickým infrastrukturám a analyzovat jejich průběh.

Výsledky evidované v RIV

D – Článek ve sborníku – Čeleda, P. et al. KYPO – A Platform for Cyber Defence Exercises. 2015. (RIV/00216224:14610/15:00080539).
D – Článek ve sborníku – Kouřil, D. et al. Cloud-based Testbed for Simulation of Cyber Attacks. 2014. (RIV/00216224:14610/14:00073216).
D – Článek ve sborníku – Jirsík, T.; Husák, M. et al. Cloud-based Security Research Testbed: A DDoS Use Case. 2014. (RIV/00216224:14610/14:00073217).

Identifikátor	Název
TA04010062	Technologie pro zpracování a analýzu síťových dat velkého rozsahu

Oblast výzkumu a vývoje

Výzkum a vývoj řešení pro zpracování a analýzu dat velkého rozsahu. Vyvinuté řešení umožňuje zpracování a analýzu extrémního objemu dat v reálném čase. V rámci projektu byl vyvinut nástroj Stream4Flow pro proudové zpracování síťových dat v reálném čase.

Výsledky evidované v RIV

J – Článek v odborném periodiku – Jirsík, T. et al. Toward Stream-Based IP Flow Analysis. 2017. (RIV/00216224:14610/17:00094364).
D – Článek ve sborníku – Čermák, M. et al. A Performance Benchmark of NetFlow Data Analysis on Distributed Stream Processing Systems. 2016. (RIV/00216224:14610/16:00087595).
R – Software – Jirsík, T. et al. Stream4Flow: Software for mining and analysis of the large volumes of network traffic. 2016. (RIV/00216224:14610/16:00087653).

3.11 Výsledky projektů výzkumu a vývoje uchazeče, které byly nebo jsou prokazatelně úspěšně využívány komerčně

Identifikátor	Název
CAMNEP	Multiagentní systém pro detekci anomálního chování v provozu počítačové sítě

Kým a po jakou dobu komerčně využíván, případně číslo patentu nebo jiného typu právní ochrany

Výstupy projektů pro Armádu Spojených států amerických (N62558-07-C-0001 a W911NF-08-1-0250) které řešilo ČVUT (příjemce) společně s MU (další řešitel) převedlo ČVUT v roce 2010 do své technologické spin-off společnosti Cognitive Security s.r.o. (www.cognitivesecurity.cz), kterou později koupila společnost Cisco (2013). Výsledek byl předán na základě licenční dohody mezi ČVUT se společností Cognitive Security s.r.o. Součástí převodu bylo i programové vybavení vytvořené Masarykovou univerzitou pro sběr a předzpracování síťových dat pro multiagentní systém. U převedených výsledků došlo ke komerčnímu dokončení, zahájení výroby na nich postavených produktů a prodeji v ČR a zahraničí.

Identifikátor	Název
LIBEROUTER	Programovatelný hardware pro monitorování vysokorychlostních sítí s hardwarově akcelerovanými funkcemi

Kým a po jakou dobu komerčně využíván, případně číslo patentu nebo jiného typu právní ochrany

Převod výsledků vědy a výzkumu sdružení CESNET, MU a VUT (projekty MŠM 6383917201, GÉANT2 No. 511082, SCAMPI IST-2001-32404, 6NET IST-2001-32603) aktivita Programovatelný hardware (www.liberouter.org) do technologického spin-offu MU a VUT společnosti INVEA-TE-CH (od roku 2015 rozdělena na společnosti Flowmon Networks a.s. a Netcope Technologies, a.s.). Výsledek byl licencován na základě Smlouvy o poskytnutí výsledků výzkumu ze dne 9. 5. 2007 a následné Smlouvy o spolupráci a smlouvy licenční z 16. 4. 2008 společnosti INVEA-TECH a.s. Nejvýznamnější převedené výsledky jsou:

- COMBO - rodina akceleračních karet COMBO využívající hradlových polí (FPGA) pro bezeztrátové zpracování síťového provozu ve vysokorychlostních sítích.
- NetCOPE - vývojová platforma NetCOPE pro návrh firmwaru vysokorychlostních síťových aplikací využívajících hradlových polí.
- FlowMon - hardwarově akcelerovaná sonda FlowMon pro monitorování IP toků na počítačové síti využívající platformy PC a hardwarových akcelerátorů COMBO.

Kým a po jakou dobu komerčně využíván, případně číslo patentu nebo jiného typu právní ochrany

U převedených výsledků došlo ke komerčnímu dokončení, zahájení výroby na nich postavených produktů a prodeji v ČR a zahraničí. Společnost INVEA-TECH se opakovaně umístila v žebříčku Deloitte nejrychleji rostoucích technologických firem Deloitte CE Technology Fast 50.

Identifikátor	Název
KYBERCVIČENÍ	Technické cvičení kybernetické bezpečnosti

Kým a po jakou dobu komerčně využíván, případně číslo patentu nebo jiného typu právní ochrany

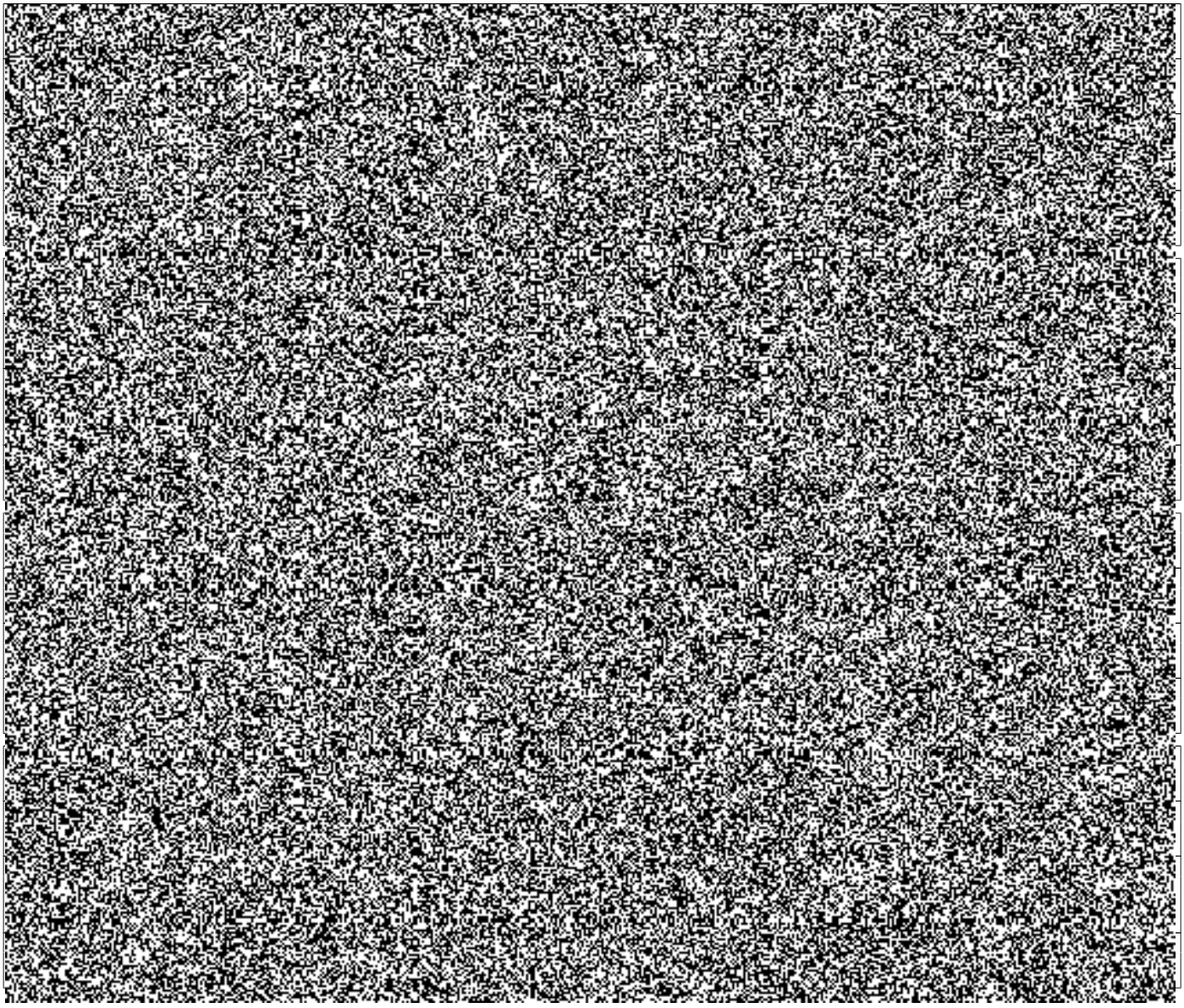
Výstupem projektu KYPO (VG20132015103) je software umožňující vytvářet a provádět technická cvičení kybernetické bezpečnosti. První cvičení pod názvem Cyber Czech bylo realizováno v roce 2015 ve spolupráci s Národním bezpečnostním úřadem (od roku 2017 NÚKIB). Jednalo se o první komplexní technické cvičení v České republice. Od té doby jsou cvičení pořádána pravidelně pro účastníky z České republiky i zahraničí. Dosud bylo realizováno osm rozsáhlých cvičení pro státní instituce a dvě cvičení pro komerčního partnera z energetického sektoru.

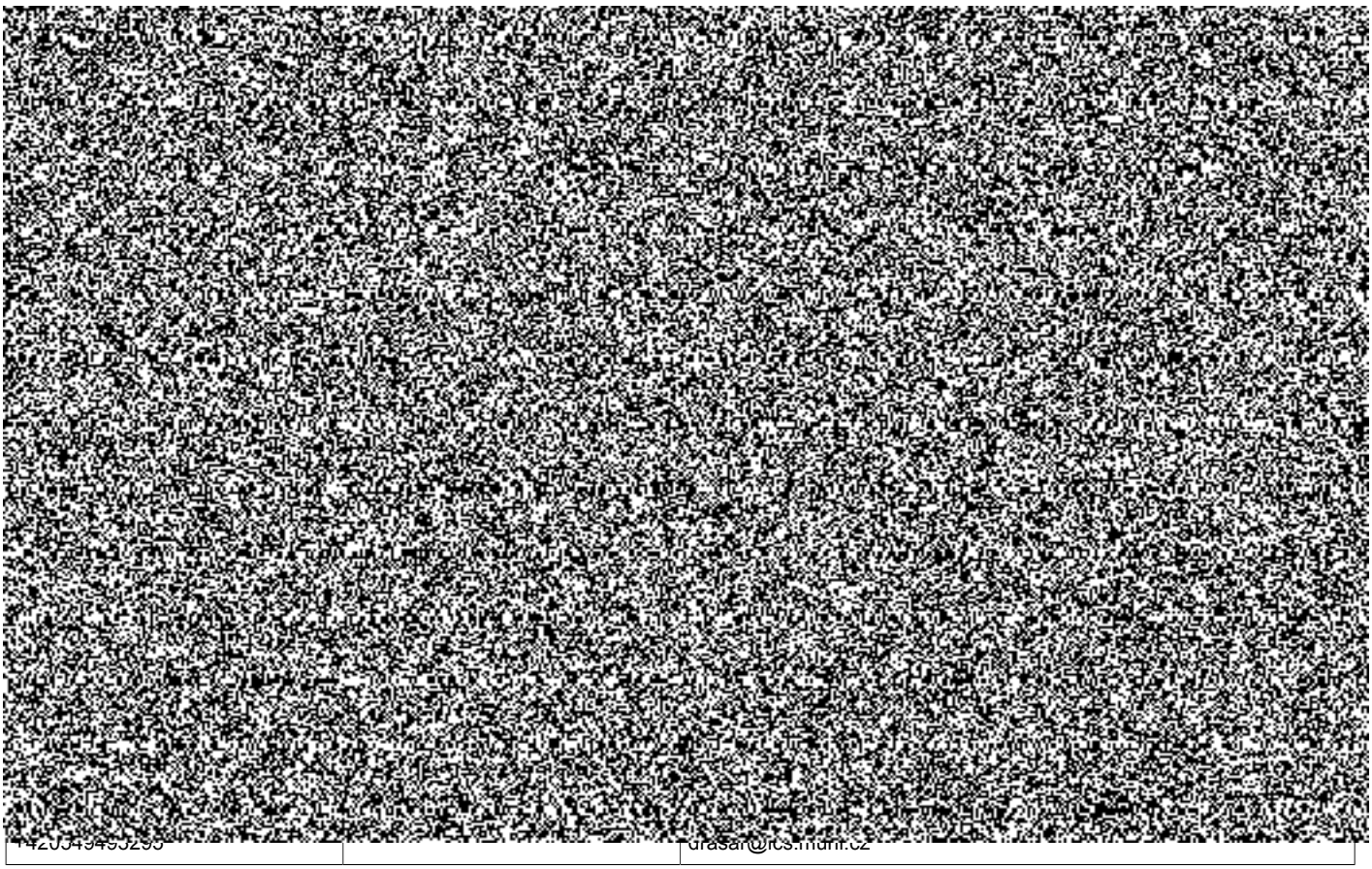
Identifikátor	Název
AXENTA	Vývoj simulačního prostředí pro analýzu kyberútoků

Kým a po jakou dobu komerčně využíván, případně číslo patentu nebo jiného typu právní ochrany

Výstupy projektu (CZ.01.1.02/0.0/0.0/16_045/0007358) byly v roce 2017 předány společnosti AXENTA a.s. (www.axenta.cz) v souladu s podmínkami projektové výzvy. Společnost výstupy projektu v současné době využívá pro demonstraci svých nástrojů a školení technického personálu v oblasti reakce bezpečnostního týmu na kyberútoky.

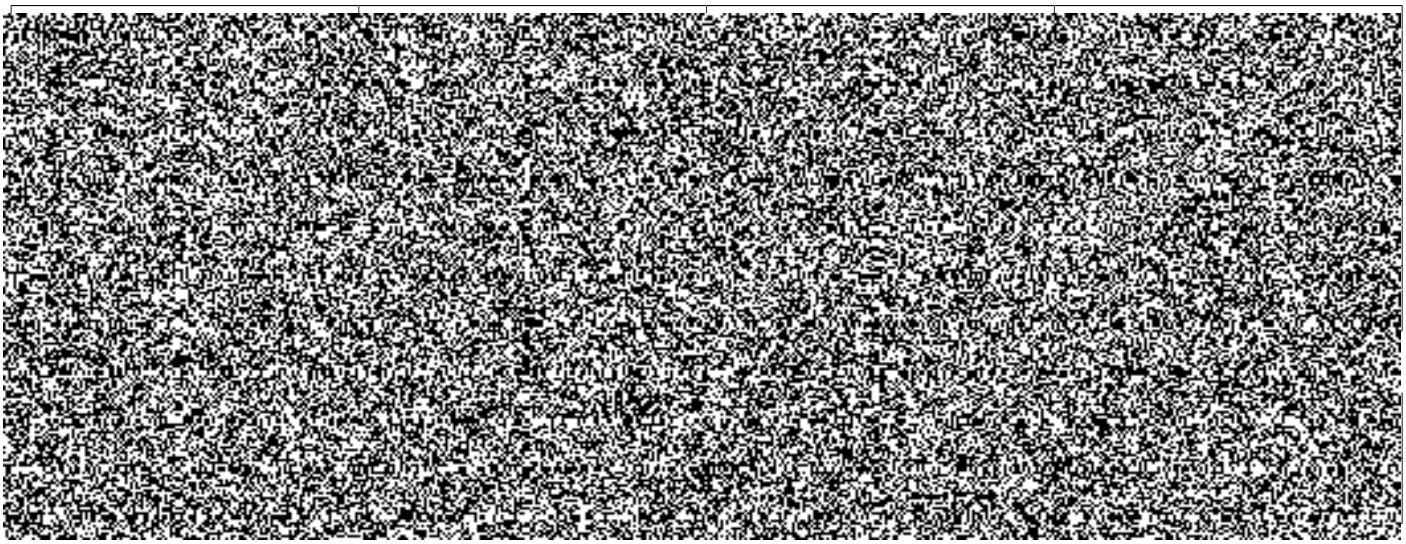
3.12 Řešitelský tým projektu





+420549493293		drasar@rcs.muni.cz

3.14 Další pracovníci projektového týmu



5. Popis projektu

5.1 Hlavní cíl projektu a jeho charakteristika

Hlavní cíl projektu a jeho charakteristika

Hlavním cílem projektu je vytvořit prostředky pro automatizaci činností penetračního testování a posloužit tak provozovatelům KII a VIS v zajištění adekvátní úrovně zabezpečení, navzdory nedostatku kvalifikovaného personálu a neustále se měnícím hrozbám. Za tím účelem budou vyvinuty nástroje pro efektivní orchestraci existujících nástrojů ofenzivní bezpečnosti, pro automatickou realizaci komplexních scénářů penetračního testování a pro automatickou dynamickou analýzu zabezpečení cílové infrastruktury.
K dosažení stanoveného cíle budou zanalyzovány nástroje ofenzivní bezpečnosti, komplexní systémy simulace průniku (breach and attack simulation) a budou zkoumány mechanismy automatizace scénářů penetračního testování a hledání optimálních metod průniku do cílové infrastruktury. Na základě těchto činností bude implementována a otestována otevřená a snadno rozšiřitelná sada nástrojů, která umožní zastoupit většinu činností expertů na penetrační testování. Na rozdíl od stávajících řešení bude zaměřena na realizaci všech typů útoků, včetně bezpečnostního testování samotných nástrojů pro detekci a prevenci průniku a bude klást důraz na snadnou ovladatelnost, aby její využití nebylo podmíněno hlubokými znalostmi v oblasti kyberbezpečnosti.
Předložený projekt umožní snížit požadavky na množství a expertízu členů bezpečnostních týmů provozovatelů KII a VIS, otevře cestu pro zavedení procesů kontinuálního testování infrastruktury, umožní i ICT expertům bez specializace na kyberbezpečnost provádět hloubkové penetrační testováni infrastruktury a poslouží jako prostředek snížení nákladů na realizaci kyberbezpečnostních cvičení. Přispěje tak k navýšení odolnosti kritické IT infrastruktury a posílí schopnost dotčených subjektů reagovat na hrozby v kyberprostoru.

5.2 Dílčí cíle projektu

Dílčí cíle projektu

K naplnění hlavního cíle projektu byly stanoveny následující dílčí cíle, které pokrývají tři hlavní komponenty komplexního penetračního testování:

- Analýza nástrojů ofenzivní bezpečnosti a vytvoření mechanismu jejich orchestrace - tento cíl se zabývá výzkumem a vytvořením mechanismu pro jednotné ovládání nástrojů ofenzivní bezpečnosti a jednotného popisu jejich výstupů, aby bylo možné tyto nástroje mezi sebou propojovat a jejich výstupy konzistentně zpracovávat.
- Vytvoření mechanismu popisu a realizace komplexních scénářů penetračního testování - penetrační testování může zahrnovat celou řadu různých úkonů s netriviálními závislostmi. Dílčí cíl se proto bude věnovat výzkumu a vývoji popisných nástrojů pro specifikaci a opakovanou automatickou realizaci penetračních testů podle daného scénáře.
- Návrh metod pro automatizaci dynamického penetračního testování - tento cíl zahrnuje výzkum a vývoj metod automatické kombinace objevených zranitelností pro dosažení stanoveného cíle penetračního testu a přizpůsobování běhu testu dynamickým obranným mechanismům testovaného systému.

5.3 Hlavní výsledky projektu

Kód	Druh výsledku	Počet
R	software	3

5.4 Vedlejší výsledky projektu

Kód	Druh výsledku	Počet
D	článek ve sborníku	2

5.5 Popis současného stavu problematiky řešené oblasti

Popis současného stavu problematiky řešené oblasti

Automatizace a kontinuální testování jsou hodnoceny analytiky jako jedna z oblastí, jež bude mít v blízké době velmi významný dopad na kyberbezpečnost (viz např. analýza společnosti Gartner k tématu Breach and Attack Simulation). Nástroje automatizace statického a dynamického bezpečnostního testování jsou vyvíjeny v komerční, open-source i výzkumné sféře. Největšími zástupci komerčních nástrojů jsou FireDrill, Cymulate, SafeBreach a ThreatCare. Představiteli open-source nástrojů jsou AutoTTP, Metta a DumpsterFire. Výzkumnými projekty využívanými v praxi při automatizaci útočných scénářů v bezpečnostních cvičeních jsou Sved, vyvíjený ve švédské agentuře obranného výzkumu (FOI), a Cryton, vyvíjený uchazečem jako součást projektu KYPO II (VI20162019014).

Schopnosti komerčních nástrojů sahají od provádění kontinuálního testování na základě předem vytvořených scénářů (FireDrill) po laterální pohyb testovanou infrastrukturou a simulaci přítomnosti útočníků v infrastruktuře (Cymulate, SafeBreach). Tyto nástroje jsou dostupné jako lokálně provozovaný SW nebo v režimu Security as a Service (SaaS), kdy je veškerá útočná infrastruktura spravována provozovatelem nástroje.

Open-source nástroje poskytují proti těm komerčním omezenou funkcionalitu. Zaměřují se více na simulaci aktivit napadeného stroje, což nachází využití při testování nasazených bezpečnostních detekčních nástrojů. Tyto nástroje se starají buď pouze o orchestraci útočných nástrojů (AutoTTP, DumpsterFire), nebo o vytvoření celého virtualizovaného prostředí, ve kterém následně vykoná popsaný útočný scénář (Metta).

V akademické sféře jsou nejvýznamnější dva nástroje: Sved a Cryton. Sved poskytuje rozhraní pro definici útočných scénářů pomocí útočných grafů, v kterých je cesta volená na základě úspěchu jednotlivých útočných kroků. Používá pravděpodobnostní model s pravděpodobnostmi stanovenými na základě analýzy existujících infrastruktur a reálných případů penetračního testování. Cryton poskytuje prostředky pro orchestraci útočných nástrojů a pro vykonávání jednotlivých kroků útoku v daném čase a za daných podmínek. Nástroj je ve stádiu prototypu a vyvíjí se převážně jako prostředek realizace kyberbezpečnostních cvičení.

Emulace reálných útoků a pohybu útočníka infrastrukturou vyžaduje existenci modelu zranitelností cílového systému. Těchto modelů byla vytvořena celá řada. Ačkoliv je jejich původním účelem vyhodnocení zranitelnosti cílových systémů nebo infrastruktur, představuje plánování útoků duální problém, který lze řešit stejnými prostředky. Příkladem těchto modelů jsou útočné grafy, obranné grafy, Markovovy procesy řízené

Popis současného stavu problematiky řešené oblasti

Booleovskou logikou, CORAS framework, nebo Secure Tropos. Tyto modely jsou povětšinou omezené tím, že vyžadují specifikaci závislostí mezi jednotlivými komponentami posuzované infrastruktury, stanovení pravděpodobnosti napadení a závažnost jednotlivých zranitelností. V principu tedy nemohou být využívány nikým jiným než experty na kyberbezpečnost. Navzdory těmto omezením vznikly nástroje, které tyto modely využívají a zároveň se dotazují externích zdrojů informací o zranitelnostech, aby zredukovali množství informací, které musí uživatelé vyplnit. Jde o nástroje NETSPA, GARNET, NAVIGATOR, MulVAL a TVA-tool. Tyto nástroje však mají velká omezení týkající se rozsahu posuzovaných zranitelností - primárně se zaměřují na zneužívání zranitelností a neumožňují např. modelovat dopady slovníkových útoků.

Nejdále v modelování útoků a jejich následné realizaci je nástroj Sved, který staví na vlastním jazyku pro modelováni kyberbezpečnosti (CySeMoL). U něj jsou pravděpodobnosti úspěchu různých typů útoků experimentálně ověřeny a stanoveny na základě expertních hodnocení a na základě výsledků penetračních testování a kyberbezpečnostních cvičení, nevyžaduje tedy tak hluboké znalosti pro úspěšnou analýzu průniku. Zároveň tento jazyk umožňuje modelovat mnohem širší množinu typů útoků. Hlavní slabinou tohoto nástroje je binárnost rozhodování o úspěchu jednotlivých kroků, která znemožňuje přípravu komplexnějších scénářů.

Aby mohl předkládaný projekt naplnit stanovené cíle, bude potřeba adresovat následující oblasti, jejichž řešení je stále otevřené:

- Efektivní integraci nástrojů ofenzivní bezpečnosti a jejich propojení, aby bylo možné nástroje vhodně kombinovat a eliminovat false positives.
- Rozšíření modelů zranitelností, aby pokrývaly framework MITRE ATT&CK.
- Vytvoření mechanismů popisu jednotlivých kroků útoku k popisu komplexních scénářů.
- Propojení nástroje s infrastrukturou, aby bylo možné simulovat činnost útočníků vevnitř infrastruktury.

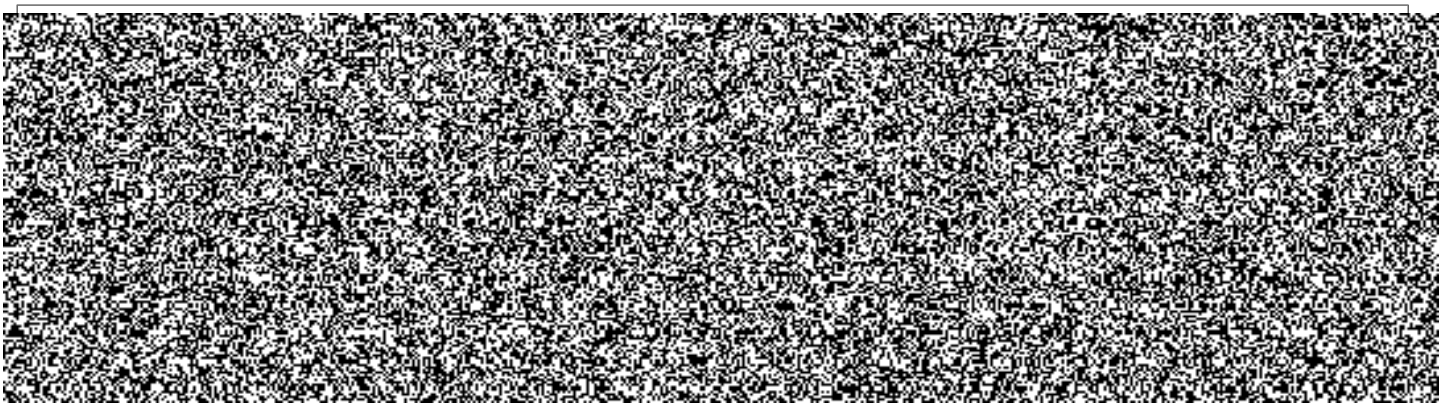
5.6 Přínosy a dopady projektu v oblasti bezpečnosti a cílů stanovených Programem

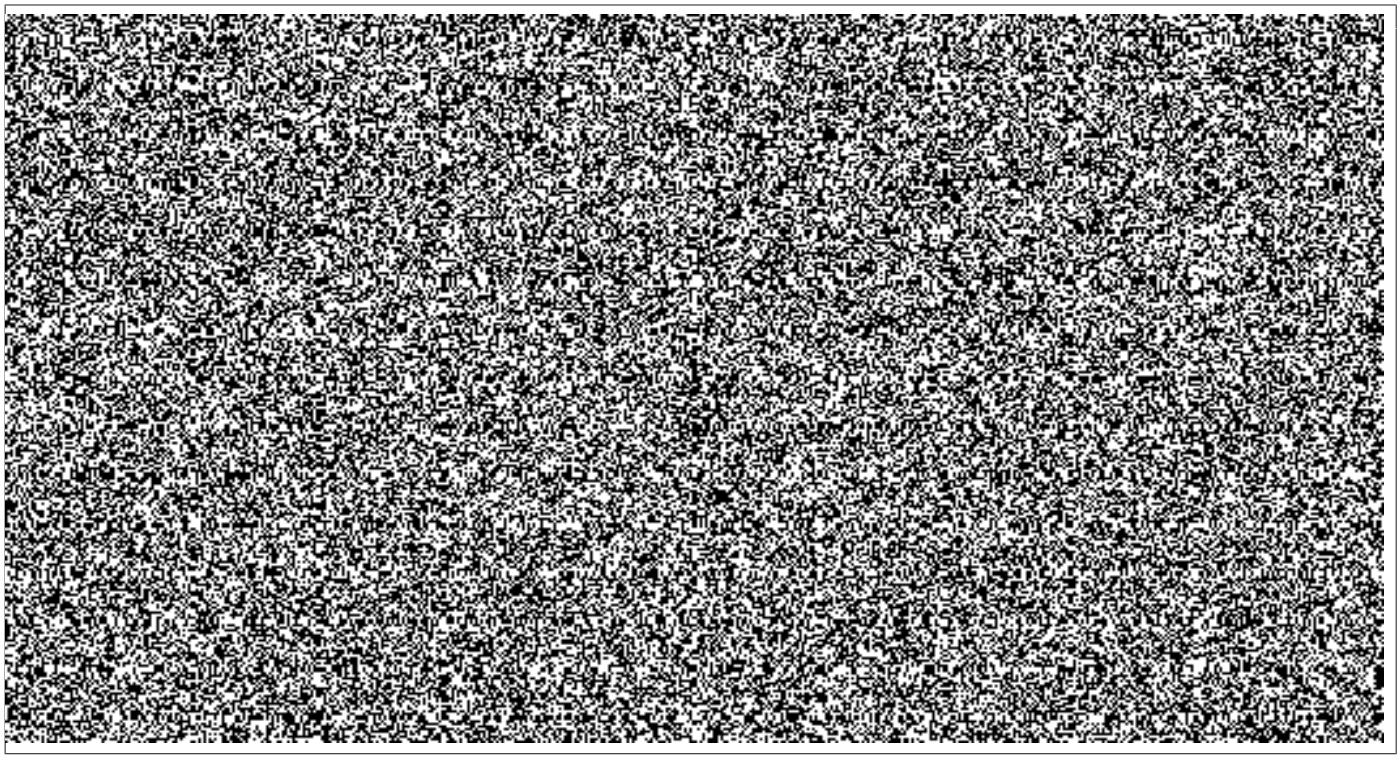
Přínosy a dopady projektu v oblasti bezpečnosti a cílů stanovených Programem

Realizace projektu bude mít přímý vliv na bezpečnostní praxi v kontextu závazků a úkolů, které plynou ze strategických cílů EU v oblasti kybernetické bezpečnosti, Strategie České republiky pro oblast kybernetické bezpečnosti, Zákona č. 181/2014 Sb. o kybernetické bezpečnosti a souvisejících prováděcích právních předpisů a výsledků Auditu národní bezpečnosti v oblasti hrozeb v kyberprostoru. Výstupy projektu přispějí k plnění cílů tematické oblasti Bezpečnost kritických infrastruktur a zdrojů Programu. Mezi konkrétní přínosy a praktické dopady projektu v oblasti bezpečnosti patří:

- Zpřístupnění široké škály nástrojů ofenzivní bezpečnosti expertům. Pro specialisty na kyberbezpečnost je k dispozici nepřeberné množství různých ofenzivních nástrojů, jež jsou mnohdy využitelné pouze pro jeden konkrétní útok nebo omezenou sadu akcí. Ačkoliv existují výjimky, jako např. Metasploit, provádění efektivních útoků vyžaduje znalost celé řady těchto nástrojů, které se však liší svým ovládáním i prezentací a dalším zpracováním výstupů. Díky sjednocení ovládání a zpracování výstupů těchto nástrojů se bude možné při výcviku bezpečnostních expertů více zaměřit na samotné koncepty, než na konkrétní nástroje, což usnadní a urychlí jejich vzdělávání. Toto sjednocení zároveň umožní efektivně porovnávat výstupy různých nástrojů, čímž přispěje ke snazší identifikaci false positives a zefektivnění činnosti bezpečnostních týmů. V neposlední řadě poskytne sjednocení prostředky pro jednotné programové ovládání různých nástrojů a dá tak bezpečnostním expertům do rukou prostředek pro širší automatizaci jejich práce.
- Omezení požadavků na počet a expertízu členů bezpečnostních týmů a tedy i jejich snadnější personální zajištění. Každý z plánovaných výsledků projektu přispěje k automatizaci procesů penetračního testování a zredukuje požadavky na potřebné specifické znalosti. Tím dojde ke zpřístupnění těchto procesů i specialistům mimo obor kyberbezpečnosti. Týmy, které se potýkají s nedostatkem personálu budou jednak potřebovat méně expertů a také budou moct delegovat část role kyberbezpečnostních expertů např. na IT specialisty z jiné domény, nebo budou moct snížit požadavky na nové zaměstnance, jež bude možné rychleji a levněji zaškolit.
- Výrazné ulehčení zajištění procesu kontinuálního testování pro KII a VIS. Kontinuální testování je nezbytným předpokladem pro zajištění optimálního zabezpečení za situace, kdy se vyvíjí nejenom hrozby v kyberprostoru, ale i podmínky ve sledované infrastruktuře. V současné době takové testování vyžaduje buď dostatek expertů nebo zakoupení služeb externích penetračních týmů pro každou KII nebo VIS. Nástroje vyvinuté v rámci tohoto projektu umožní centrálně připravit procesy kontinuálního testování a pak je sdílet mezi jednotlivými subjekty. Tím se jednak zajistí shodně vysoká úroveň testování všech zúčastněných a také se dále sníží nároky na expertízu ICT personálu jednotlivých subjektů. Přidanou hodnotou sjednocení testování je vzájemná porovnatelnost úrovně zabezpečení jednotlivých subjektů.
- Sledování vývoje bezpečnosti v čase. Automatizované kontinuální testování spojené s tvorbou auditů umožní vést podrobnou dokumentaci o stavu vývoje zabezpečení v čase. To umožní manažerům bezpečnosti jednotlivých subjektů vyhodnocovat dopad interních a externích změn na zabezpečení organizace. V případě, kdy dojde k narušení zabezpečení některého subjektu, usnadní auditová historie vyšetření incidentu.
- Redukce nákladů pro realizaci bezpečnostních cvičení. Kyberbezpečnostní cvičení imitující reálné infrastruktury a hrozby jsou velmi nákladná na realizaci. Zajištění červeného týmu odpovídající kvalifikace patří mezi jednu z nejvýznamnějších položek. Nástroje vyvinuté v rámci předkládaného projektu umožní výrazně zmenšit velikost týmů útočníků a snížit jejich expertízu, aniž by byla ovlivněna kvalita cvičení. To povede k výrazným úsporám a umožní zajistit cvičení pro širší okruh specialistů.

5.7 Popis realizace projektu (zvolená metodologie, použité metody, technologie a postupy)





5.8 Způsob a podíl zapojení jednotlivých účastníků do realizace projektu

Způsob a podíl zapojení jednotlivých účastníků do realizace projektu

Masarykova univerzita se na řešení projektu podílí sama. Řešitelský tým se skládá z pracovníků Ústavu výpočetní techniky, kteří již mají zkušenosti s problematikou řešení projektů bezpečnostního výzkumu MV ČR a provozem bezpečnostního týmu CSIRT-MU. Na řešení projektu se bude podílet vyvážený tým složený z výzkumníků, jejichž výzkumná témata jsou blízká cílům projektu, a IT specialistů. Vzhledem k nemalému podílu vývojových prací spojených s vytvořením softwarových nástrojů (Výsledek č. 1 až 3), jsou na pozici programátorů do projektu zapojeni také studenti Fakulty informatiky MU.

Masarykova univerzita disponuje potřebným technologickým zázemím pro řešení projektu. V rámci univerzitního centra CERIT Scientific Cloud (CERIT-SC - CZ.1.05/3.2.00/08.0144) bude poskytnuta výpočetní a síťová infrastruktura pro vývoj a testování vytvářeného software. Simulace kritických infrastruktur a bezpečnostních incidentů bude prováděna v prostředí Kybernetického polygonu (VG20132015103) a s využitím SCADA testbedu projektu C4e (CZ.02.1.01/0.0/0.0/16_019/0000822). Pilotní nasazení výsledků projektu bude provedeno řešitelským týmem na síti Masarykovy univerzity. Výsledky projektu budou napojeny na technické a programové vybavení, které využívá bezpečnostní tým CSIRT-MU.

5.9 Intenzita podpory

Intenzita podpory - Masarykova univerzita / Ústav výpočetní techniky

MU je výzkumná organizace a v souladu se zadávací dokumentací uplatňuje úhradu způsobilých nákladů ve výši 100 % způsobilých nákladů projektu. Kalkulace nákladů vychází z cen a mezd v místě a čase obvyklých. Osobní náklady jsou verifikovány osobními průměry a situací v oboru ICT. Cestovné je kalkulováno ve vazbě na počet plánovaných článků. Náklady na služby jsou kalkulovány na základě zkušeností uchazeče a doplňkové režijní náklady vychází z metodiky FullCost MU.

5.10 Předpokládaní uživatelé výsledků

Předpokládaní uživatelé výsledků

Předpokládanými uživateli výsledků projektu jsou především bezpečnostní týmy povinných orgánů a osob (organizací) dle Zákona o kybernetické bezpečnosti č. 181/2014 Sb. Zejména pak Vládní CERT (GovCERT.CZ) a dále pak národní CSIRT ČR, CIRC MO, CESNET-CERTS, CSIRT-MU.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) – vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Mezi jeho hlavní činnosti patří provozování Vládního CERT České republiky, výzkum a vývoj v oblasti kybernetické bezpečnosti a příprava bezpečnostních standardů pro informační systémy KII a VIS. NÚKIB projevil podporu předkládanému projektu formou dopisu uvedeného v příloze 4.3.4. Výsledky projektu budou poskytnuty Vládnímu CERT a jemu podřízeným organizacím a bude je možno využít pro standardizační a certifikační aktivity spojené s provozováním KII a VIS.

Ministerstvo obrany (MO) – v rámci resortu MO vybudovalo Vojenské zpravodajství (VZ) Národní centrum kybernetických operací (NCKO), které formuluje a realizuje strategii kybernetické obrany ČR. Další prvek kybernetické bezpečnosti resortu MO tvoří Centrum CIRC. Jeho úkolem je proaktivní identifikace bezpečnostních hrozeb a incidentů, jejich analýza a následné reportování zjištěných událostí a postupů řešení k relevantním partnerům. Výsledky projektu budou poskytnuty VZ, NCKO a Centru CIRC.

Předpokládaní uživatelé výsledků

Výsledky projektu budou využitelné i dalšími organizacemi a firmami řešícími problematiku udržitelnosti úrovně kybernetické bezpečnosti. Cílem uchazeče je vytvořit a dále rozvíjet plánované výsledky tak, aby mohly být jednoduše využity třetími stranami. Výsledky budou zpřístupněny tak, aby jejich využívání nebylo v rozporu se zájmy České republiky a negativně neovlivňovalo bezpečnost České republiky a jejích občanů.

V neposlední řadě budou výsledky projektu využity bezpečnostním týmem uchazeče (CSIRT-MU), který je použije pro účinné a kontinuální testování zabezpečení infrastruktury Masarykovy univerzity a pro přípravu kyberbezpečnostních cvičení. Výsledky projektu budou rozvíjeny v dalších VaV aktivitách uchazeče a použity pro podporu bezpečnostního vzdělávání členů bezpečnostních týmů a studentů Masarykovy univerzity. Tento krok podpoří výchovu nových bezpečnostních odborníků, kterých je v České republice stále velký nedostatek.

5.11 Projekt počítá se subdodávkami

Projekt počítá se subdodávkami

NE

5.12 Harmonogram projektu

Název činnosti	Uchazeč	0bdobí, kdy je činnost uskutečňována											
		1	2	3	4	5	6	7	8	9	10	11	12
Rok 2020													
1.1 Návrh architektury systému a definice rozhraní Návrh centralizované/distribuované architektury, specifikace univerzálního rozhraní mezi komponentami, specifikace komunikačního protokolu.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x						
1.2 Vývoj a testování SW pro orchestraci nástrojů ofenzivní bezp. Specifikace jednotného rozhraní pro ovládání nástrojů ofenzivní bezpečnosti a pro zpracování a analýzu jejich výstupů. Vývoj SW pro ovládání těchto nástrojů.	Masarykova univerzita / Ústav výpočetní techniky			x	x	x	x	x	x	x	x	x	x
1.3 Vývoj SW pro statickou verifikaci bezpečnostních opatření Příprava modelových scénářu statického penetračního testování, vytvoření jazyka pro popis komplexních útočných scénářů, vývoj SW pro spouštění těchto scénářů.	Masarykova univerzita / Ústav výpočetní techniky							x	x	x	x	x	x
1.4 Integrace nástrojů ofenzivní bezpečnosti: Etapa I Výběr a integrace nástrojů ofenzivní bezpečnosti do Výsledku č. 1, tak aby bylo možné je jednotným způsobem ovládat.	Masarykova univerzita / Ústav výpočetní techniky								x	x	x	x	x
Rok 2021													
2.1 Integrace nástrojů ofenzivní bezpečnosti: Etapa II Výběr a integrace nástrojů ofenzivní bezpečnosti do Výsledku č. 1, tak aby bylo možné je jednotným způsobem ovládat.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x	x	x
2.2 Statická verifikace bezp. opatření zvolených modelových případů Analýza expresivnosti vytvořeného jazyka pro popis komplexních útočných scénářů, vyhodnocení na případu velkých kyberbezpečnostních cvičení.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x	x	x
2.3 Vývoj a testování SW pro st. verifikaci bezp. opatření: Etapa I Vývoj SW pro spouštění komplexních útočných scénářů pro statickou verifikaci bezpečnostních opatření, testování ve virtualizovaném prostředí.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x	x	x
2.4 Vývoj SW pro dynamickou analýzu bezpečnostních opatření Příprava modelových scénářu dynamického penetračního testování, rešerše modelů a jazyků pro popis závislosti bezpečnostních zranitelností, příprava vlastního/upraveného modelu a jazyka, který umožní definovat cíle penetračního testování, implementace SW.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x	x	x
Rok 2022													
3.1 Dynamická analýza bezp. opatření zvolených modelových případů Vyhodnocení zvoleného modelu a jazyka pro popis závislostí bezpečnostních zranitelností, analýza algoritmů pro dosažení cíle penetračního testování.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x	x	x
3.2 Integrace nástrojů ofenzivní bezpečnosti: Etapa III Výběr a integrace nástrojů ofenzivní bezpečnosti do Výsledku č. 1, tak aby bylo možné je jednotným způsobem ovládat.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x				
3.3 Vývoj a testování SW pro dynamickou analýzu bezp. opatření Implementace SW pro automatickou analýzu průniku do infrastruktury, testování na univerzitní infrastruktuře, v kyberbezpečnostních cvičeních a ve SCADA testbedu.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x				
3.4 Vývoj a testování SW pro st. verifikaci bezp. opatření: Etapa II Vývoj SW pro spouštění komplexních útočných scénářů pro statickou verifikaci bezpečnostních opatření, testování v prostředí univerzitní infrastruktury a na SCADA testbedu.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x				
3.5 Vývoj a integrační testování celého systému Integrace všech tří výsledků pro dosažení bezproblémového provozu v režimu statického testování, dynamické analýzy, i jejich kombinace.	Masarykova univerzita / Ústav výpočetní techniky						x	x	x	x	x	x	x

5.13 Popis rizik projektu a jejich řízení

Popis rizik projektu a jejich řízení

Kategorie: Rizika řízení projektu

Riziko nesprávného odhadu návaznosti aktivit a délky jejich trvání
Pravděpodobnost: nízká
Závažnost: vysoká

Popis rizik projektu a jejich řízení

Opatření: Harmonogram byl sestavován a konzultován s projektovými manažery organizace. Bylo provedeno několik expertních odhadů časové náročnosti jednotlivých aktivit a jejich návazností, na jejichž základě byl harmonogram finalizován. Klíčoví řešitelé, odpovědní za plánování a řízení projektu, jsou proškoleni v projektovém řízení a mají dostatečné zkušenosti s plánováním a realizací projektů.
Aktivity, u nichž hrozí zvýšená náročnost jsou umístěny v harmonogramu tak, aby prodloužení doby jejich řešení nezpůsobilo komplikace s realizací výstupů projektu. Harmonogram projektu bude průběžně kontrolován a aktualizován podle potřeby.

Riziko, že navržené postupy a technická řešení nepovedou k dosažení výsledků s očekávanými parametry
Pravděpodobnost: nízká
Závažnost: vysoká
Opatření: Všechny výsledky byly diskutovány s klíčovými osobami řešitelského týmu, které mají dlouhodobé zkušenosti v řešené oblasti. Harmonogram projektu obsahuje etapy vývoje zakončené testovacími a integračními etapami, na nichž bude ověřována dosažitelnost výsledků.

Kategorie: Personální rizika

Riziko krátkodobého výpadku, přetížení a fluktuace zaměstnanců
Pravděpodobnost: střední
Závažnost: nízká
Opatření: Řešitelský tým je sestaven tak, aby byla zajištěna krátkodobá zastupitelnost. Je kladen důraz na sdílení znalostí. Řešitelský tým má rovněž zkušenosti se získáváním a školením vysoce kvalifikovaných výzkumných a vývojových pracovníků z řad absolventů bakalářského, magisterského a doktorského studia.

Riziko odchodu klíčových zaměstnanců
Pravděpodobnost: střední
Závažnost: střední
Opatření: Pravidelně probíhají pohovory s projektovým týmem, které mají za úkol odhalit případné komplikace a hrozící odchod zaměstnance. Zaměstnanci průběžně zvyšují svou odbornost, takže mohou zastat i náročné úkoly.

Kategorie: Technologická rizika

Riziko nevhodně zvolené technologie
Pravděpodobnost: nízká
Závažnost: vysoká
Opatření: Řešitelé projektu mají dlouhodobé zkušenosti s vývojem a testováním software. Jsou tak schopni zvolit optimální technologii. Při řešení projektu se dále počítá s rešerší a tvorbou specifikací, které umožní vybrat vhodnou technologii dle zkušeností uživatelů a jimi používaných nástrojů.

Riziko nedostatečné spolupráce při testování výsledků
Pravděpodobnost: nízká
Závažnost: nízká
Opatření: Uchazeč disponuje vlastním bezpečnostním týmem, který provádí penetrační testování univerzitní infrastruktury, disponuje virtuálním testovacím prostředím i pro SCADA doménu a podílí se na organizaci kyberbezpečnostních cvičení. I v případě, že by potenciální uživatelé neposkytli součinnost při testování, má uchazeč odpovídající prostředky pro vlastní testování, které se bude blížit operativním podmínkám.

Kategorie: Rizika neuplatnění výsledku

Riziko nezájmu potenciálních uživatelů o výstupy projektu a věcné konzultace ke směřování projektu
Pravděpodobnost: nízká
Závažnost: vysoká
Opatření: Zájem potenciálních uživatelů byl prověřen v předcházejících aktivitách a projektech realizovaných uchazečem. Zájem je rovněž vyjádřen v přiloženém dopise vyjadřujícím podporu projektu. Riziko je dále minimalizováno dlouhodobě probíhající spoluprací s uživateli.

Riziko: Změna strategie poskytovatele
Pravděpodobnost: nízká
Závažnost: vysoká
Opatření: Probíhají pravidelné konzultace s poskytovatelem na několika úrovních. Výsledky projektu se plánují využít při provozu infrastruktury uchazeče.

5.14 Doplňující informace k projektu

Doplňující informace k projektu

V rámci předloženého projektu jsou využívány pojmy statického a dynamického penetračního testování, případně dynamické analýzy. Tyto pojmy nejsou ustálené a byly uchazečem zvoleny pro rozlišení dvou fundamentálně odlišných přístupů ke konkrétní instanci penetračního testování.

Statické penetrační testování zahrnuje pevně danou sadu akcí, která je vykonána podle předem daného plánu. Typickým příkladem je penetrační testování, které zahrnuje pouze spuštění nástroje na detekci zranitelností a případné provedení jednoduchých útoků na objevené zranitelnosti.

Dynamické penetrační testování má definovanou sadu cílů a sestává z posloupnosti akcí, které vedou k danému cíli a zároveň jsou voleny na základě odezvy systému, na který se útočí. Tento typ testování tak zahrnuje laterální postupy infrastrukturou a post-exploitační aktivity. Typicky je tento typ testování realizován experty na penetrační testování na základě jejich zkušeností.

6. Financování a náklady projektu

6.1 Výše státní podpory projektu podle jednotlivých uchazečů

Uchazeč	Rok	Způsobilé náklady projektu (tis. Kč)	Z toho vlastní zdroje (tis. Kč)	Požadovaná státní podpora (tis. Kč)	Intenzita podpory (%)
Masarykova univerzita / Ústav výpočetní techniky	**Celkem**	**9 679.618**	**0**	**9 679.618**	**100**
	2020	3 141.267	0	3 141.267	100
	2021	3 238.721	0	3 238.721	100
	2022	3 299.63	0	3 299.63	100
PROJEKT	**Celkem**	**9 679.618**	**0**	**9 679.618**	**100**

6.2 Rozpočet projektu

6.2.1 Výpočet maximální míry podpory uchazeče Masarykova univerzita / Ústav výpočetní techniky

Kategorie uchazeče	výzkumná organizace
Kategorie výzkumu	experimentální vývoj
Způsobilé náklady uchazeče (tis. Kč)	**9 679.618**

Účastní se projektu alespoň dva nezávislé podniky?	NE
Hradí každý podnik maximálně 70% nákladů projektu?	NE
Účastní se projektu malý nebo střední nebo zahraniční podnik?	NE
Účastní se projektu výzkumná organizace?	ANO
Je podíl výzkumné organizace na celkovém rozpočtu projektu vyšší než 10 %?	ANO
Může výzkumná organizace zveřejnit své výsledky?	ANO
Budou výsledky projektu obecně šířeny?	ANO

Základní intenzita podpory (%)	25.00
Bonus (%)	75.00
Maximální intenzita podpory (%)	**100.00**
Maximální výše podpory (tis. Kč)	**9 679.618**

6.2.2 Náklady na mzdy/platy uchazeče Masarykova univerzita / Ústav výpočetní techniky

Jméno	Pozice v projektu	Druh pracovní smlouvy	Hodinová mzdová sazba (Kč)	Průměrný počet odprac. hodin měsíčně	Náklady na mzdy/platy v jednotlivých letech trvání projektu (tis. Kč)			Náklady celkem (tis. Kč)
					2020	2021	2022	
Řešitelé								
[redacted]								

6.2.3 Náklady uchazeče Masarykova univerzita / Ústav výpočetní techniky na pořízení majetku

6.2.4 Rozpočet nákladů uchazeče Masarykova univerzita / Ústav výpočetní techniky

Náklady/výdaje uchazeče (tis. Kč)	2020	2021	2022	Celkem
Osobní náklady/výdaje - mezisoučet	**2 538.666**	**2 588.666**	**2 588.666**	**7 715.998**
a) mzdy/platy na základě pracovního poměru	1 480.28	1 480.28	1 480.28	4 440.84
b) osobní náklady/výdaje na základě dohody o pracovní činnosti	403.2	403.2	403.2	1 209.6
c) osobní náklady/výdaje na základě dohody o provedení práce	0	0	0	0
d) povinné pojistné na sociální zabezpečení	470.87	470.87	470.87	1 412.61
e) povinné pojistné na zdravotní pojištění	169.513	169.513	169.513	508.539
f) odvody do FKSP nebo sociálního fondu	14.803	14.803	14.803	44.409
g) cestovné	0	50	50	100
Náklady/výdaje na pořízení hmotného a nehmotného majetku - mezisoučet	**0**	**0**	**0**	**0**
a) dlouhodobý hmotný majetek	0	0	0	0
b) dlouhodobý nehmotný majetek	0	0	0	0
c) drobný hmotný majetek	0	0	0	0
d) drobný nehmotný majetek	0	0	0	0
Další provozní náklady/výdaje - mezisoučet	**0**	**0**	**0**	**0**
Náklady/výdaje na služby - mezisoučet	**40**	**70**	**120**	**230**
a) subdodávky	0	0	0	0
b) ostatní služby	40	70	120	230
audit	0	0	50	50
výjezdní zasedání	40	40	40	120
konferenční poplatky	0	30	30	60
Doplňkové náklady/výdaje - mezisoučet	**562.601**	**580.055**	**590.964**	**1 733.62**
režie	562.601	580.055	590.964	1 733.62
Celkové způsobilé náklady - mezisoučet	**3 141.267**	**3 238.721**	**3 299.63**	**9 679.618**
Celková státní podpora - mezisoučet	**3 141.267**	**3 238.721**	**3 299.63**	**9 679.618**

6.2.5 Rozpočet nákladů za celý projekt

Náklady/výdaje za celý projekt (tis. Kč)	2020	2021	2022	Celkem
Osobní náklady/výdaje	**2 538.666**	**2 588.666**	**2 588.666**	**7 715.998**
Náklady/výdaje na pořízení hmotného a nehmotného majetku	**0**	**0**	**0**	**0**
Další provozní náklady/výdaje	**0**	**0**	**0**	**0**
Náklady/výdaje na služby	**40**	**70**	**120**	**230**
Doplňkové náklady/výdaje	**562.601**	**580.055**	**590.964**	**1 733.62**
Celkové způsobilé náklady	**3 141.267**	**3 238.721**	**3 299.63**	**9 679.618**
Celková státní podpora	**3 141.267**	**3 238.721**	**3 299.63**	**9 679.618**

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS | PID: VI3VS/712 | Hlavní obor: IN | Stupeň důvěrnosti: S

Souhlas statutárního zástupce uchazeče Masarykova univerzita / Ústav výpočetní techniky s návrhem projektu, se zveřejněním údajů v rozsahu požadovaném CEP a potvrzení správnosti údajů předkládaných k žádosti a souhlas s postupem stanoveným v zadávací dokumentaci.

Datum podpisu	Místo podpisu	Otisk razítka uchazeče projektu

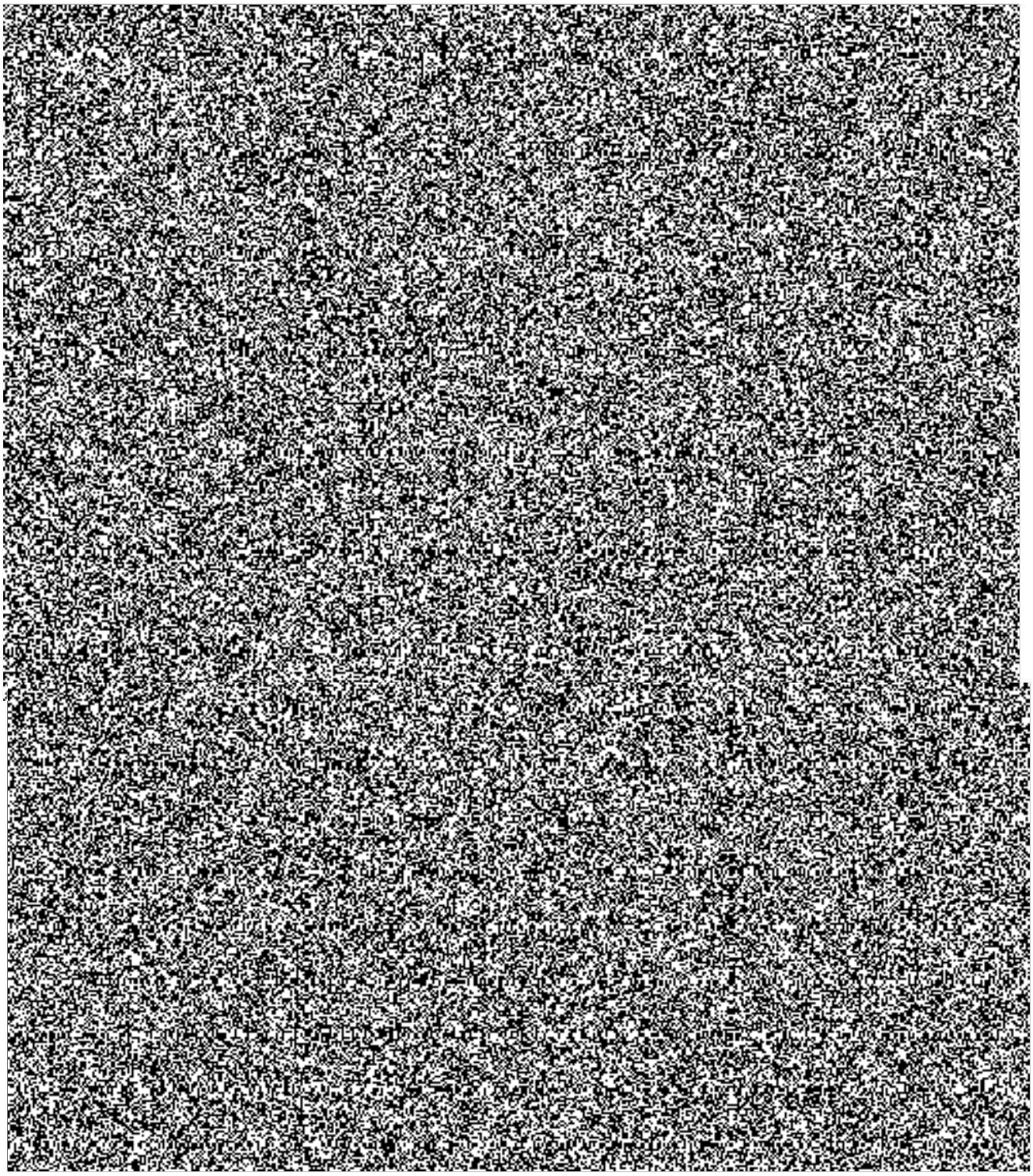
Titul před jménem	Jméno	Příjmení	Titul za jménem	Podpis
doc. PhDr.	Mikuláš	Bek	Ph.D.	

Elektronický podpis - 18.6.2019
Certifikát autora podpisu :
Jméno : JUDr. Petr Novák, Ph.D.
Vydal : PostSignum Qualified C...
Platnost do : 30.4.2020 10:17:21-000 +02:00

Příloha č. 4.2.2

Počet listů[1]: 9

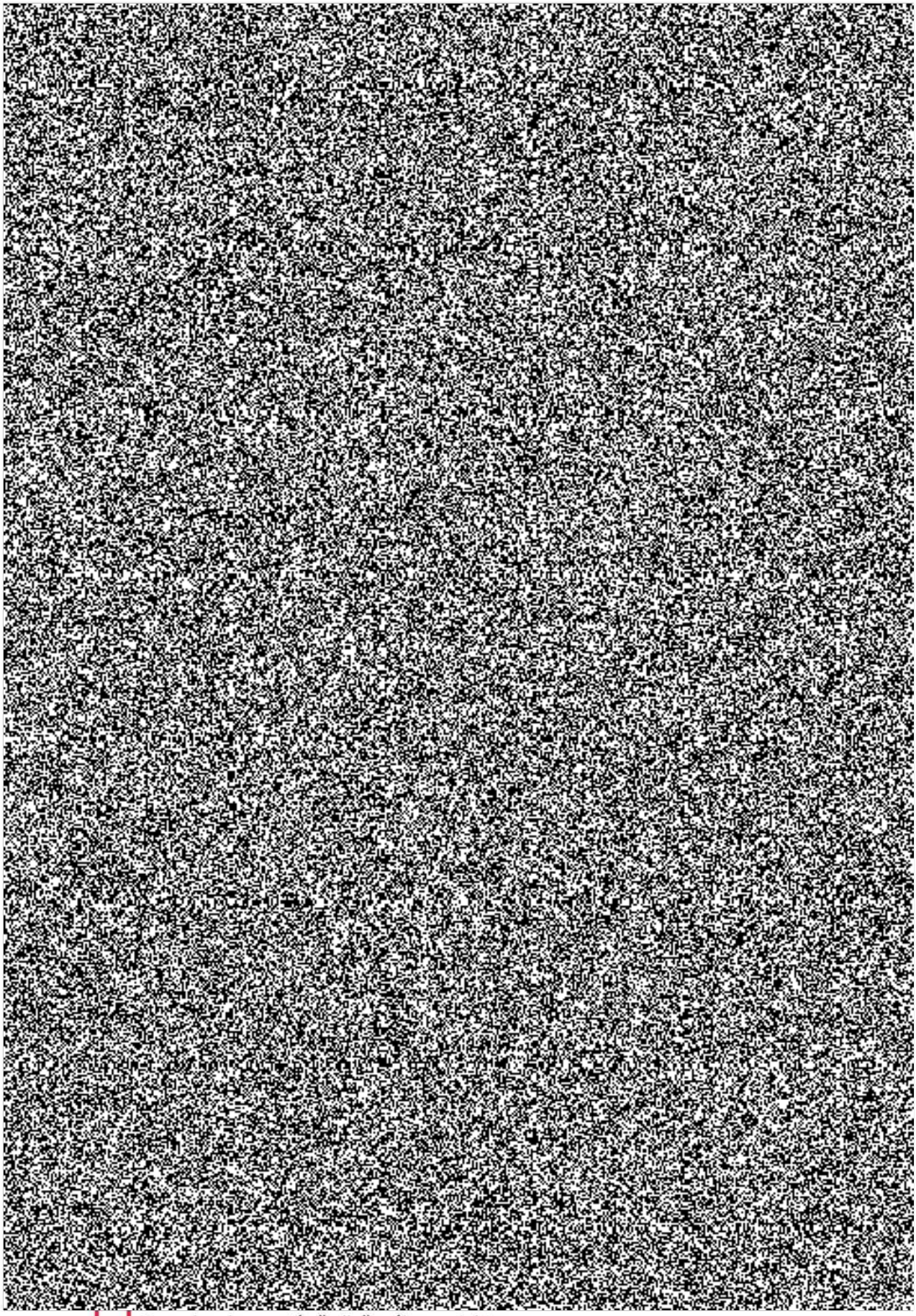
Plán využití výsledků projektu a jejich popis[2]



*) Uchazeč záhlaví vyplní, nehodící se škrtněte

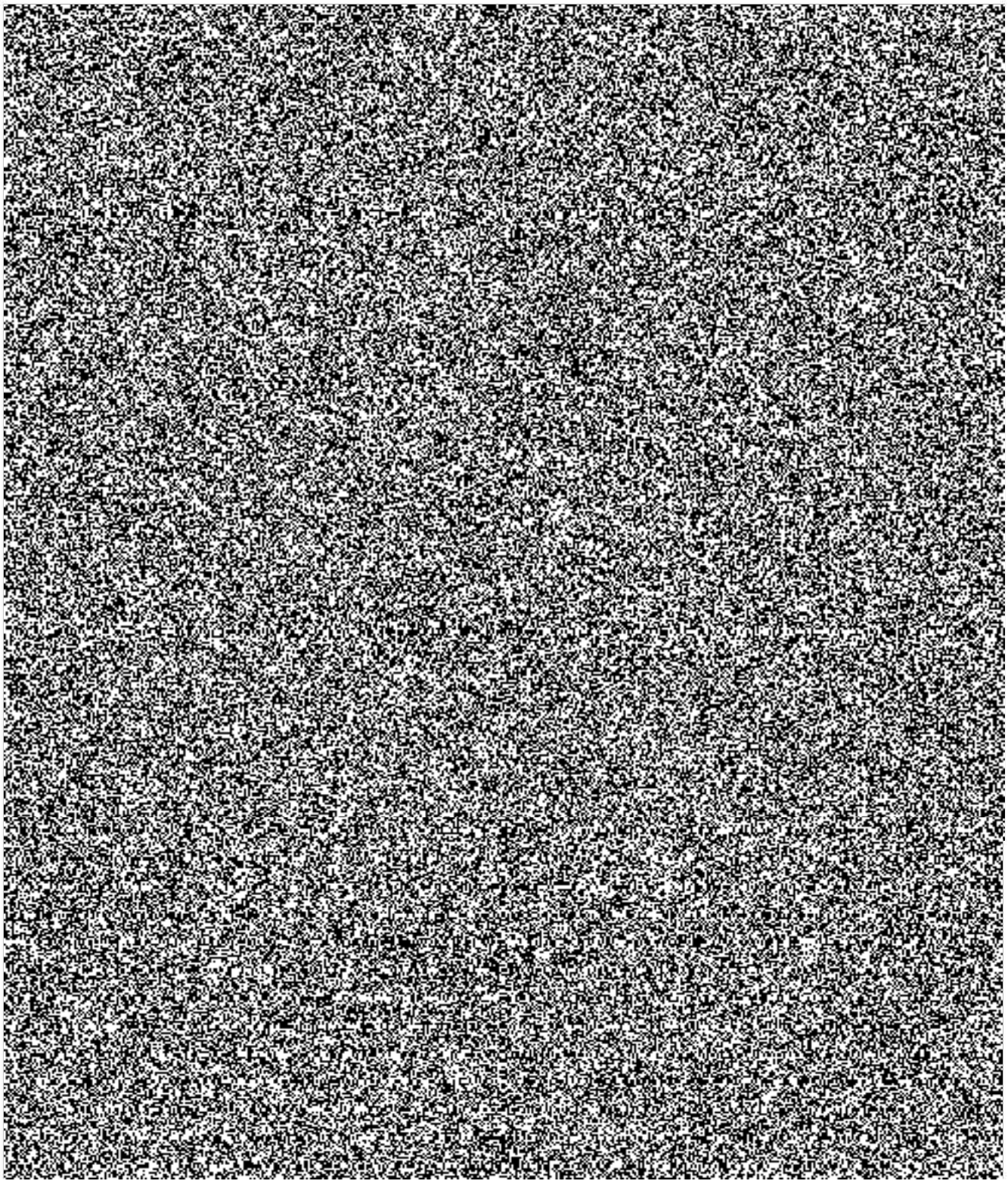
[1] Uchazeč list vyplní, aktualizuje Počet listů

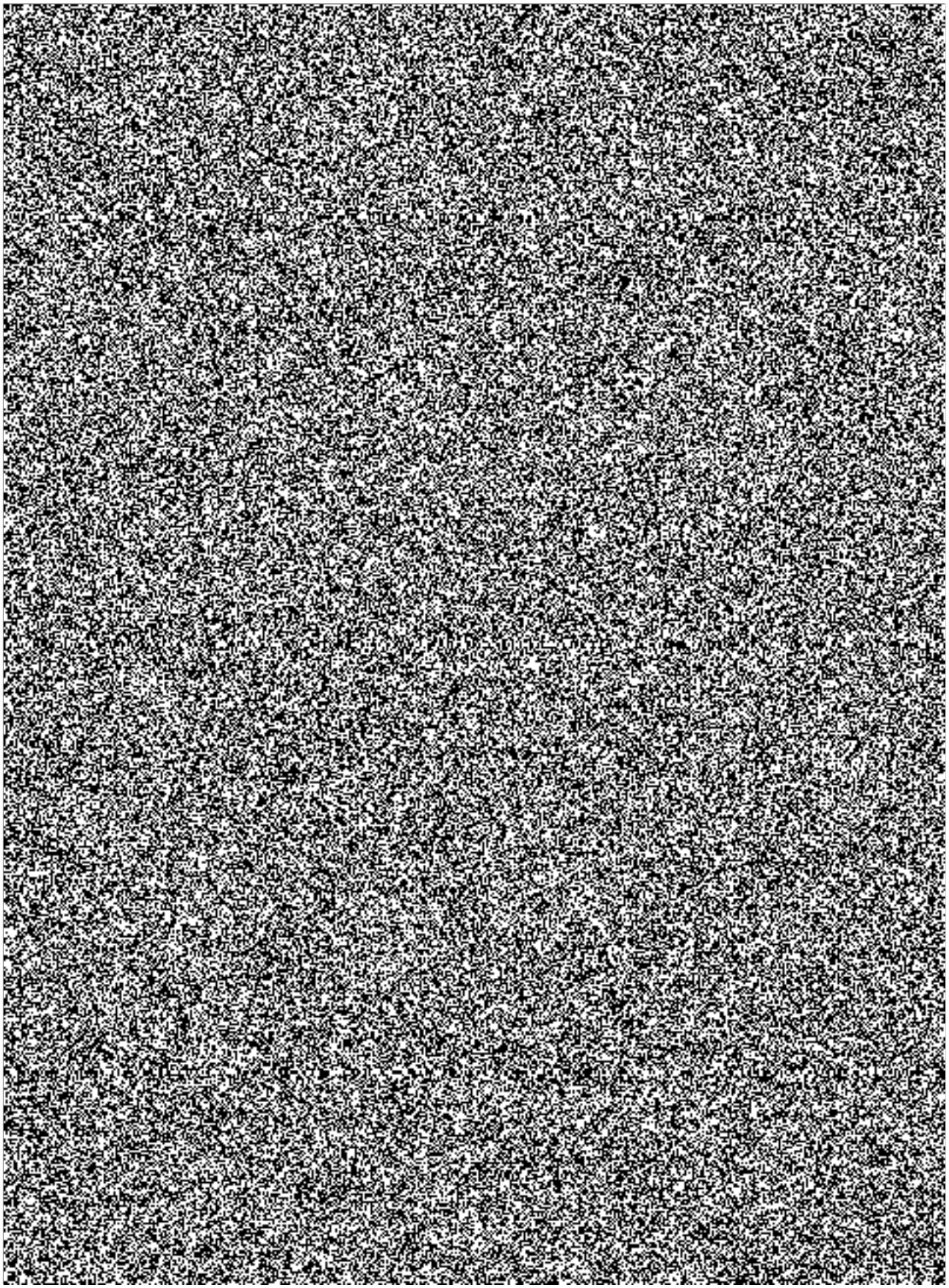
[2] Povinná příloha pro všechny uchazeče, v případě, že projekt podává více uchazečů, předkládá koordinátor

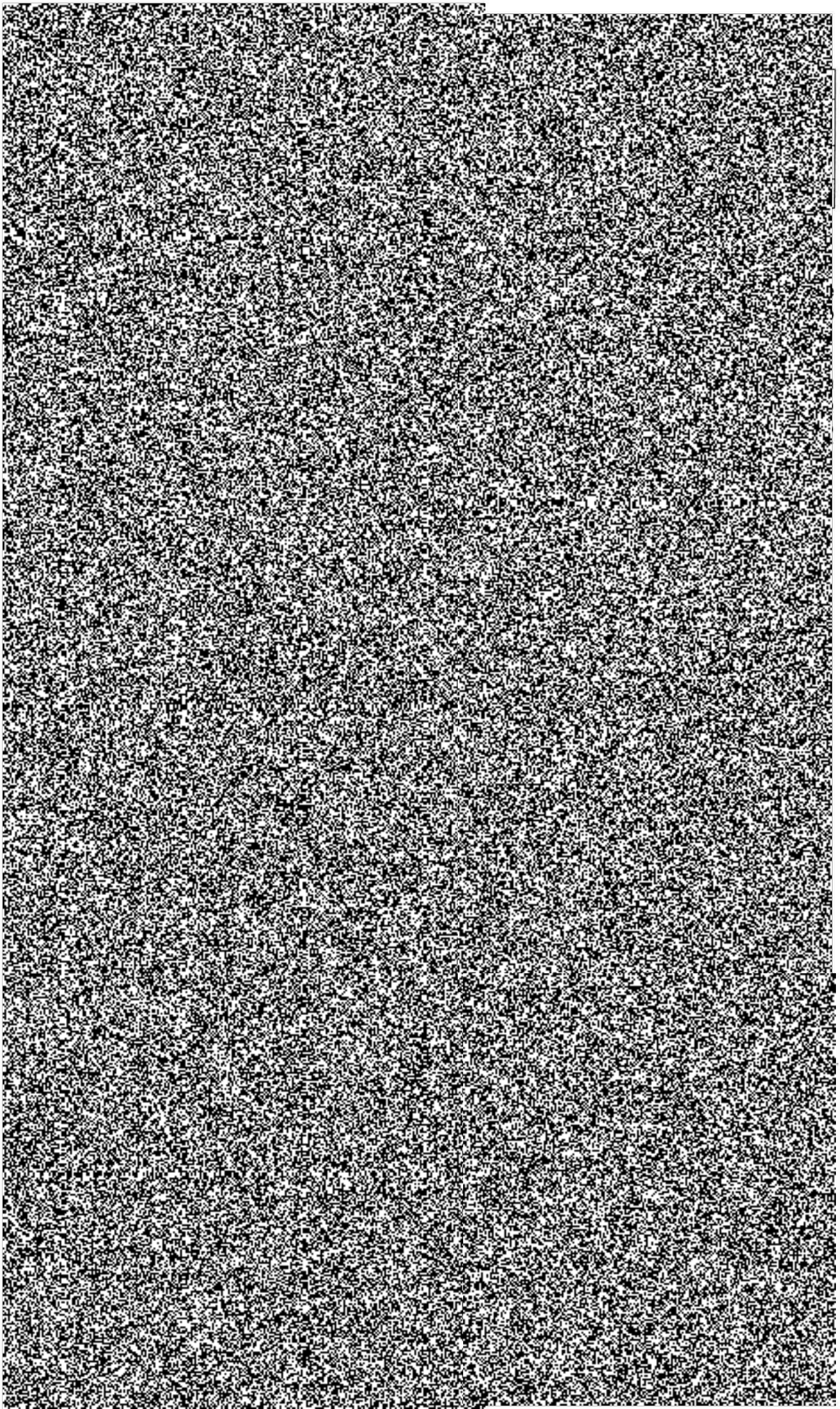


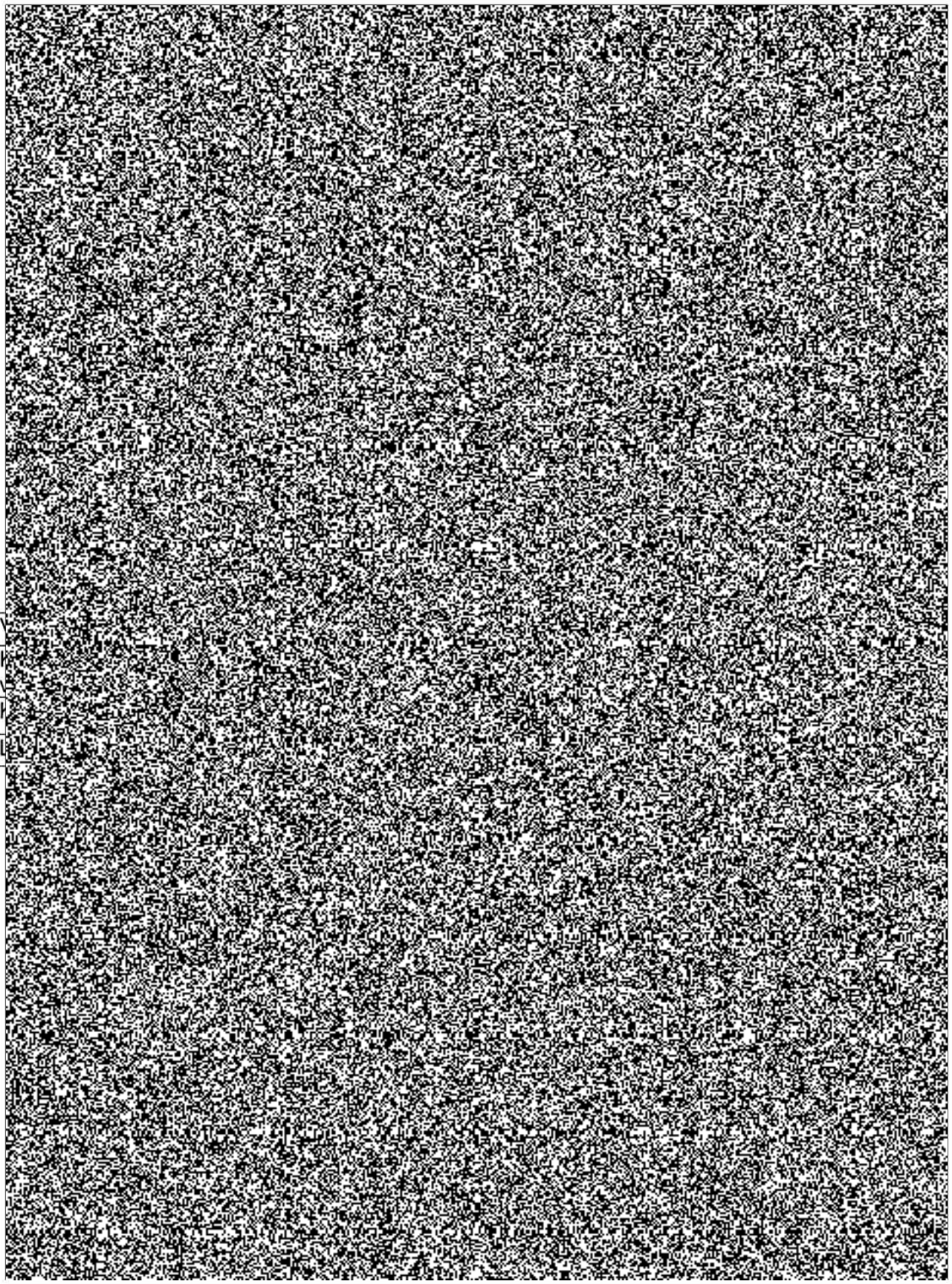
Rozsah schopností předloženého projektu

Obrázek 1- Kontext předkládaného projektu

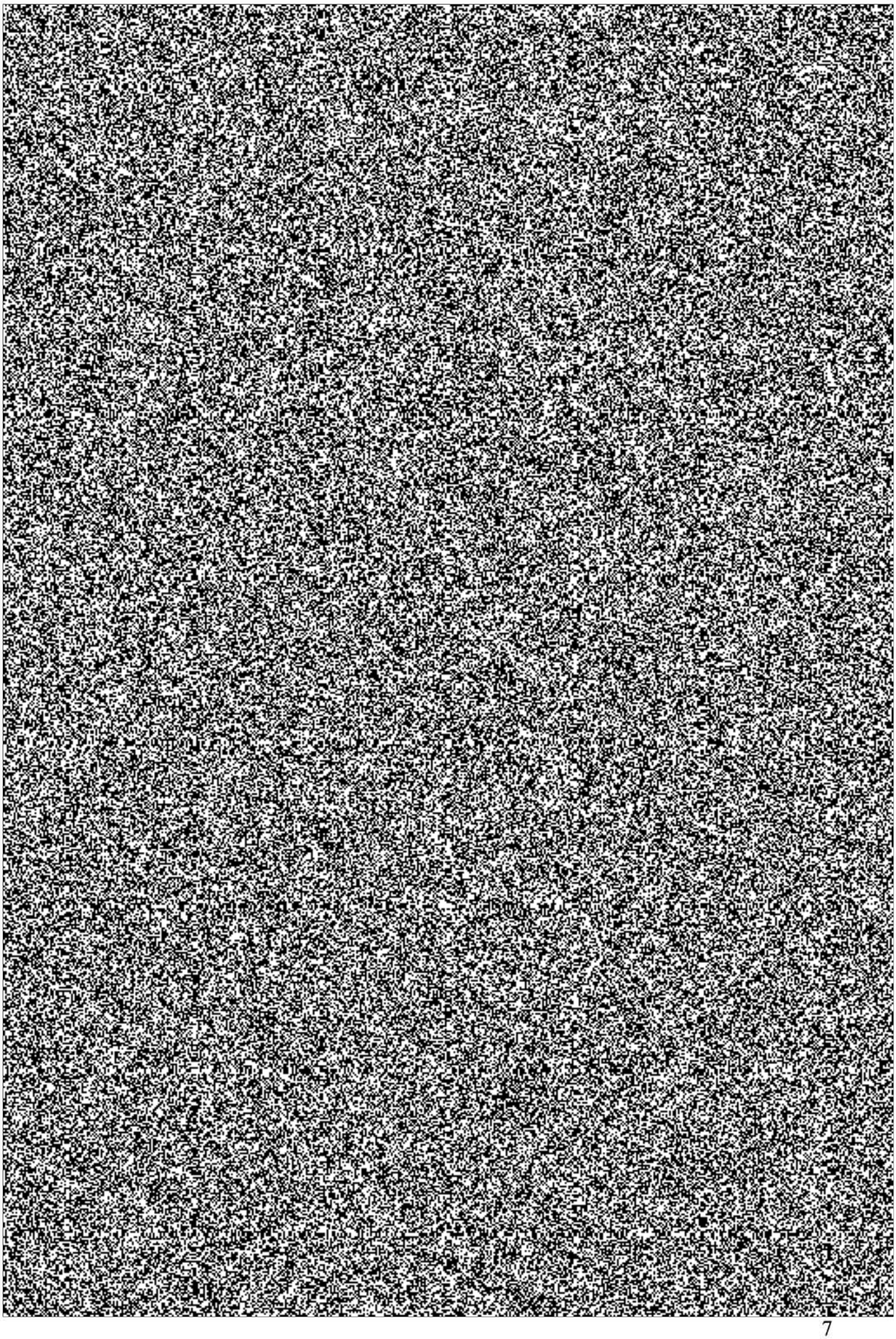


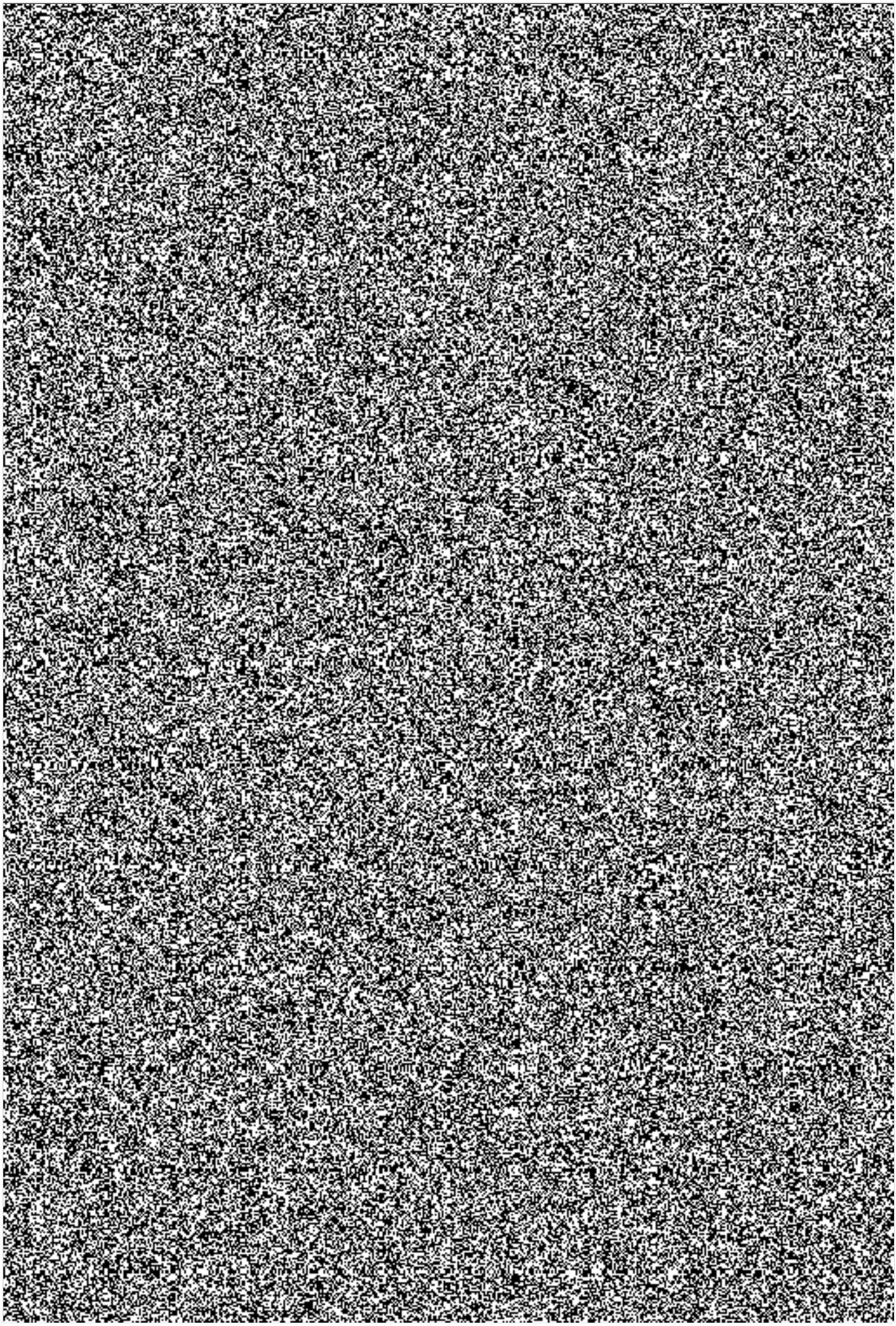






[4] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)





Datum podpisu	03-10-2018
Místo podpisu	Brno
Otisk razítka uchazeče	
Jméno, příjmení a podpis uchazeče, resp. statutárního zástupce uchazeče	

Metodika 2013 (zadávací dokumentace + elektronická přihláška)		**Metodika 2017+**	
název výsledku	kód výsledku	název výsledku	kód výsledku
patent	P	patent	P
software	R	software	R
		specializovaná veřejná databáze	S
výsledky s právní ochranou - užitný vzor, průmyslový vzor	F	užitný vzor	F_{uzit}
		průmyslový vzor	F_{prum}
poloprovoz, ověřená technologie	Z	poloprovoz	Z_{polop}
		ověřená technologie	Z_{tech}
technicky realizované výsledky - prototyp, funkční vzorek	G	prototyp	G_{prot}
		funkční vzorek	G_{funk}
metodika	N	metodiky schválené příslušným orgánem státní správy, do jehož kompetence daná problematika spadá	N_{metS}
		metodiky certifikované oprávněným orgánem	N_{metC}
		metodiky a postupy akreditované oprávněným orgánem	N_{metA}
		specializovaná mapa s odborným obsahem	N_{map}
poskytovatelem realizované výsledky - výsledky promítnuté do právních předpisů, norem, směrnic a výsledky promítnuté do předpisů nelegislativní povahy	H	výsledky promítnuté do právních předpisů a norem	H_{leg}
		výsledky promítnuté do směrnic a předpisů nelegislativní povahy závazných v rámci kompetence příslušného poskytovatele	H_{neleg}
		výsledky promítnuté do schválených strategických a koncepčních dokumentů orgánů státní nebo veřejné správy	H_{konc}
výzkumná zpráva obsahující utajované informace	V	výzkumná zpráva	V