MVCRX04IKQ0B
prvotní identifikátor

Smlouva

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

„Pokročilá orchestrace bezpečnosti a inteligentní řízení hrozeb“

VI20202022164

uzavřená mezi smluvními stranami

Česká republika – Ministerstvo vnitra

a

Masarykova univerzita

Č.j.MV-56617-5 /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.

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

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 **„Pokročilá orchestrace bezpečnosti a inteligentní řízení hrozeb“** a identifikačním kódem **„VI20202022164.“** 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 na výzkum a vývoj pokročilých nástrojů zajišťujících automatizaci a zefektivnění operativní činnosti bezpečnostních týmů v kontextu ochrany KII a VIS. Tyto nástroje poskytnou vysokou úroveň situačního povědomí o stavu chráněné infrastruktury a relevantních hrozbách. Vyvinuté nástroje dále umožní zefektivnit vybrané fáze řízení životního cyklu hrozeb díky podpoře orchestrace bezpečnosti ve spojení s kontextualizovaným uživatelským prostředím pro spolupráci.

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 RNDr. Daniel Tovarňák Ph.D.

Článek 5
Doba řešení Projektu

1) Příjemce zahájí řešení Projektu dne 01.01.2020.

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 **9 927 325,- Kč** (slovy: devětmilionůdevětsetdvacetsedmtisíctřistadvacetpětkorunčeských).
Tato částka zahrnuje podporu ve výši **9 927 325,- Kč** (slovy: devětmilionůdevětsetdvacetsedmtisíctřistadvacetpětkorunčeských), 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 odst. 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.

3) V případě, že součet objemu jednotlivých změn rozpočtu dle odst. 2 tohoto Článku v daném kalendářním roce dosáhne hranice stanovené v odst. 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 odst. 1 tohoto Článku nebo o změně dle odst. 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 lze tuto změnu realizovat pouze uzavřením dodatku k této Smlouvě.

6) Žádosti příjemce o předchozí souhlas poskytovatele podle odst. 1 a 3 tohoto Článku i oznámení změny rozpočtu podle odst. 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 o zadávání veřejných zakázek“).

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,
   - náklady na finanční pronájem a pronájem s následnou koupí (např. leasing, aj.),
   - manka a škody,

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

- 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 odst. 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 odst. 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 odst. 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 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 odst. 5 tohoto Článku, je povinen tyto prostředky poskytovateli vrátit do 15. února následujícího roku převedením

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

na bankovní účet poskytovatele číslo [redacted] 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 odst. 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.

12) Nebude-li příjemce postupovat dle povinností uvedených v odst. 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. 9 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 čl. 7 odst. 1 písm. d). 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 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 odst. 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 či služby, postupuje se podle zákona č. 137/2006 Sb. o veřejných zakázkách.

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., 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 odst. 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 29.6.2023.
3) Ukončení Smlouvy před datem uvedeným v odst. 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:

Pokročilá orchestrace bezpečnosti a inteligentní řízení hrozeb

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

Pokročilá orchestrace bezpečnosti a inteligentní řízení hrozeb

2.2 Název projektu anglicky

Název projektu anglicky

Advanced security orchestration and intelligent threat management

2.3 Anotace projektu

Anotace projektu

Cílem projektu je výzkum a vývoj pokročilých nástrojů zajišťujících automatizaci a zefektivnění operativní činnosti bezpečnostních týmů v kontextu ochrany KII a VIS. Tyto nástroje poskytnou vysokou úroveň situačního povědomí o stavu chráněné infrastruktury a relevantních hrozbách. Vyvinuté nástroje dále umožní zefektivnit vybrané fáze řízení životního cyklu hrozeb díky podpoře orchestrace bezpečnosti ve spojení s kontextualizovaným uživatelským prostředím pro spolupráci.

2.4 Anotace projektu anglicky

Anotace projektu anglicky

The project focuses on research and development of advanced tools for automation and streamlining of the operational activities of security teams protecting CII and IIS. These tools will provide a high level of situational awareness about the protected infrastructure and relevant threats. The tools will also allow for streamlining of the selected phases of threat lifecycle management by supporting security orchestration in conjunction with a contextualized user environment for collaboration.

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; řízení hrozeb; integrace dat; automatizace; kontextualizace; orchestrace; kolaborace; interaktivní UI

2.10 Klíčová slova anglicky

Klíčová slova anglicky

cyber security; threat management; data integration; automation; contextualization; orchestration; collaboration; interactive UI

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

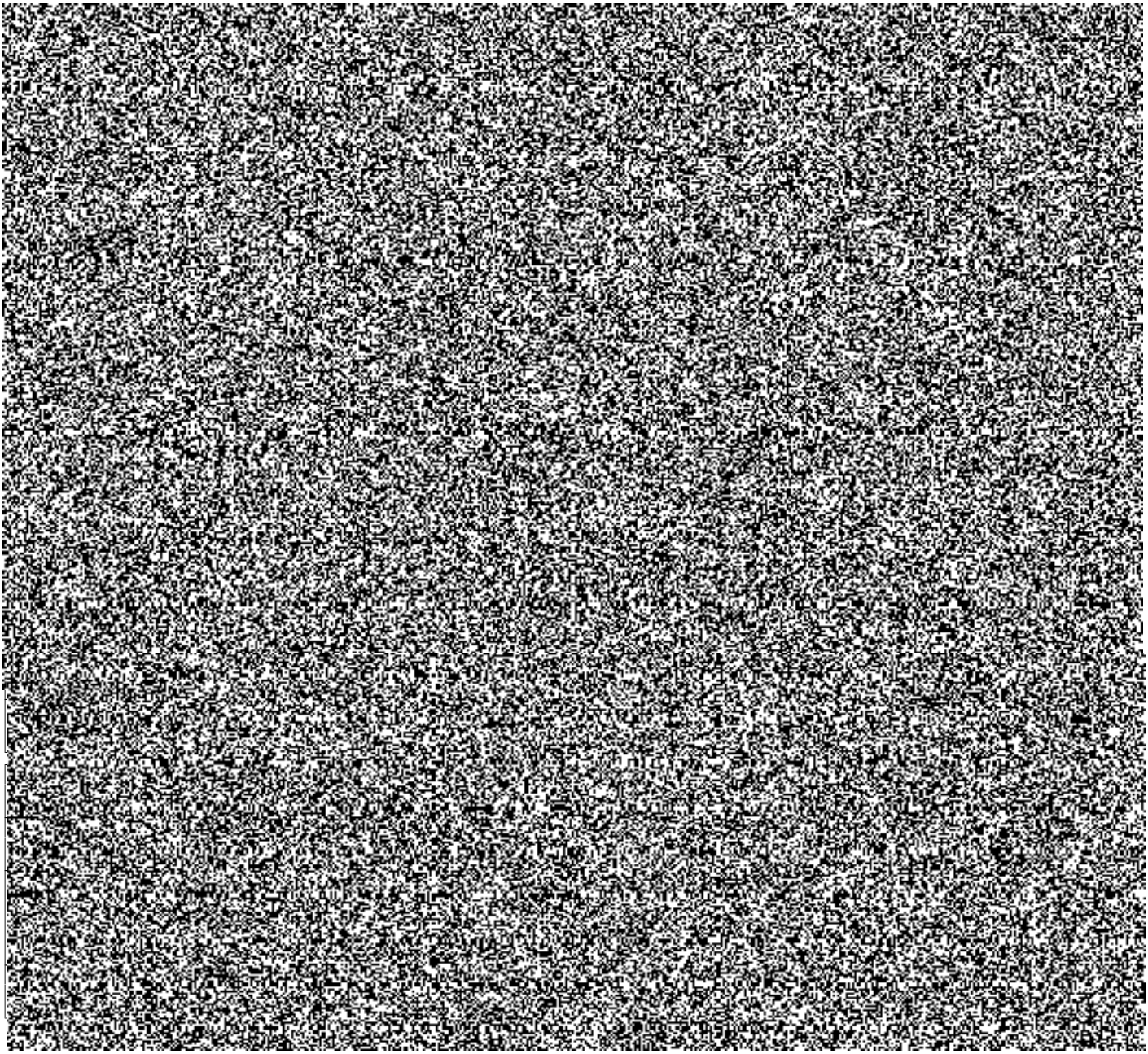
Výstupem projektu KYPO (VG20132015103) je software umožňující vytvářet a provádět technická cvičení kybernetické bezpečnosti. První cvičení pod názvem Cyber Czech bylo realizováno v roce 2015 ve spolupráci s Národním bezpečnostním úřadem (od roku 2017 NÚKIB). Jednalo se o první komplexní technické cvičení 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.

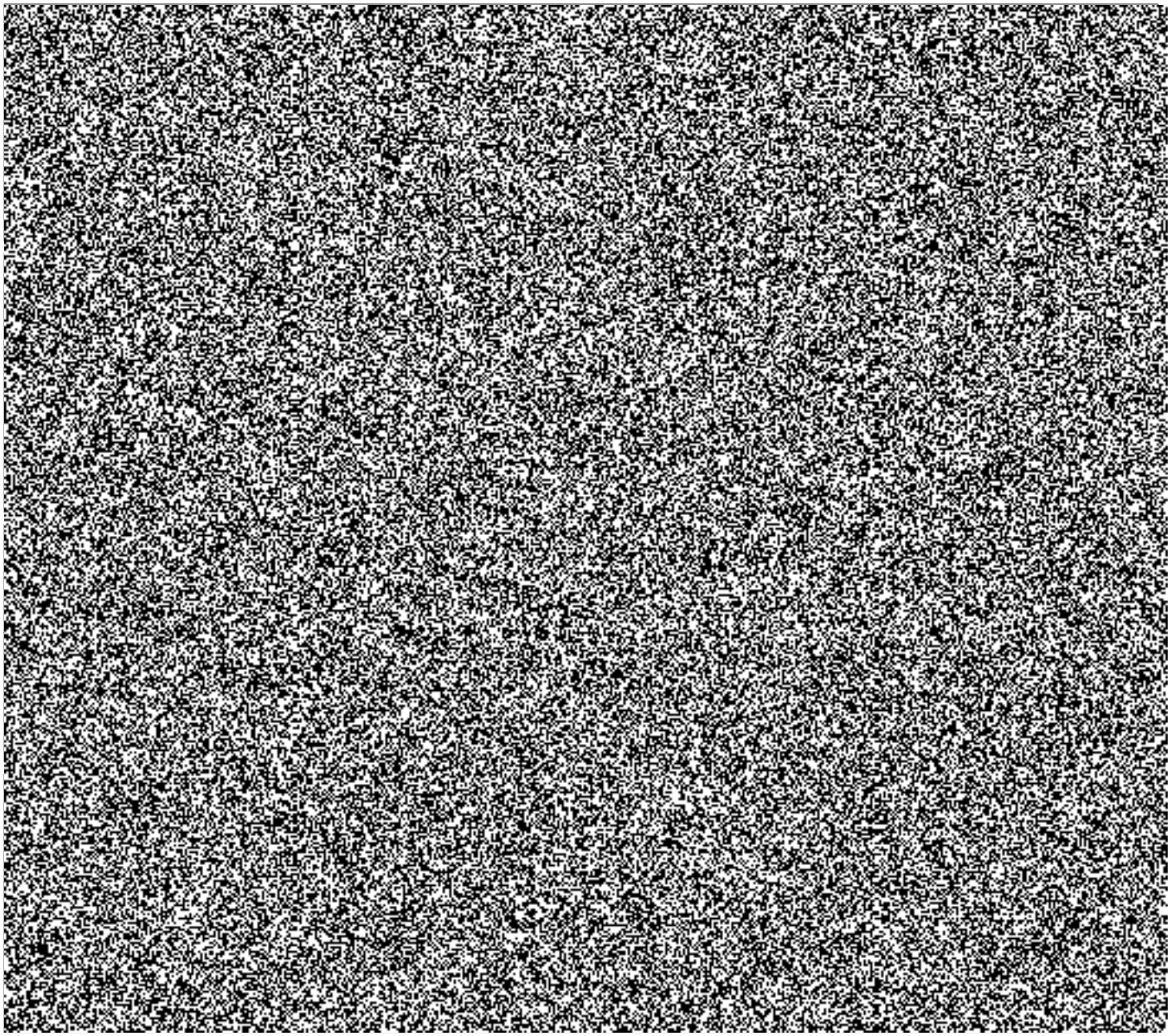
Identifikátor	Název
AXENTA	Vývoj simulačního prostředí pro analýzu kyberútoků

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

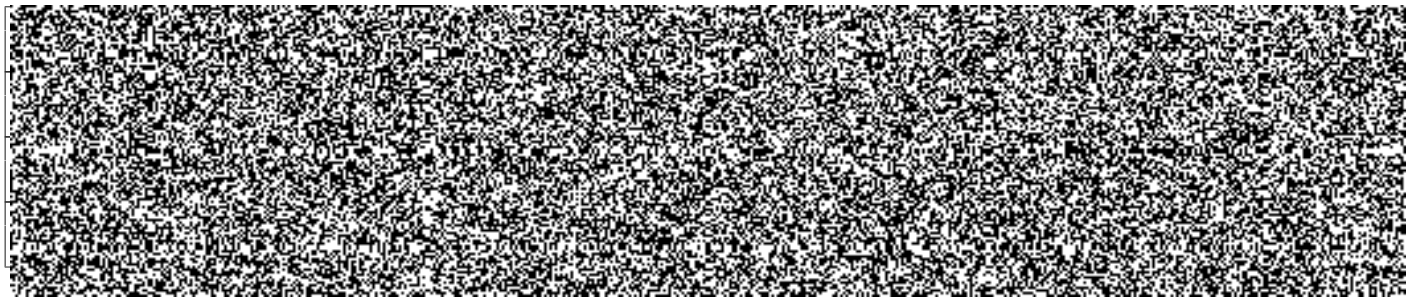
Výstupy projektu (CZ.01.1.02/0.0/0.0/16_045/0007358) byly v roce 2017 předány společnosti AXENTA a.s. (www.axenta.cz) v souladu s podmínkami projektové výzvy. Společnost výstupy projektu v současné době využívá pro demonstraci svých nástrojů a školení technického personálu v oblasti reakce bezpečnostního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

3.12 Řešitelský tým projektu

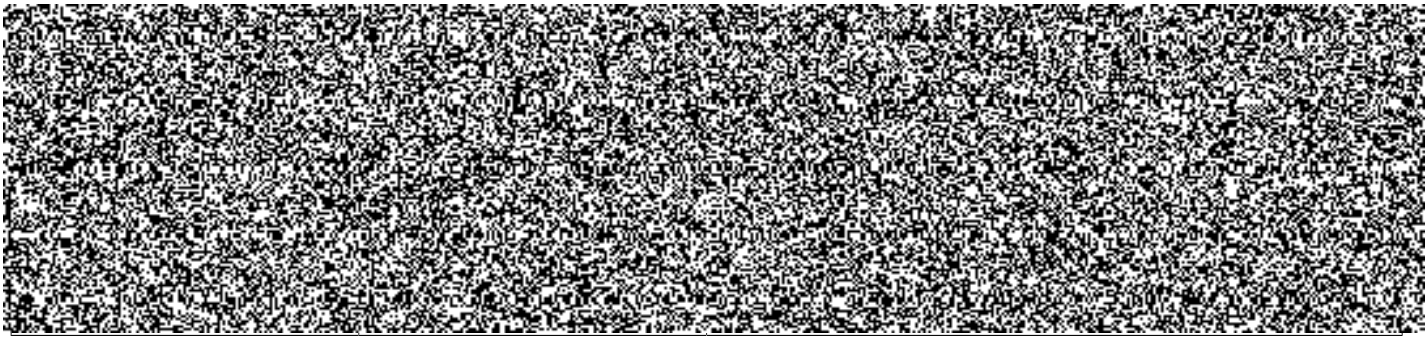




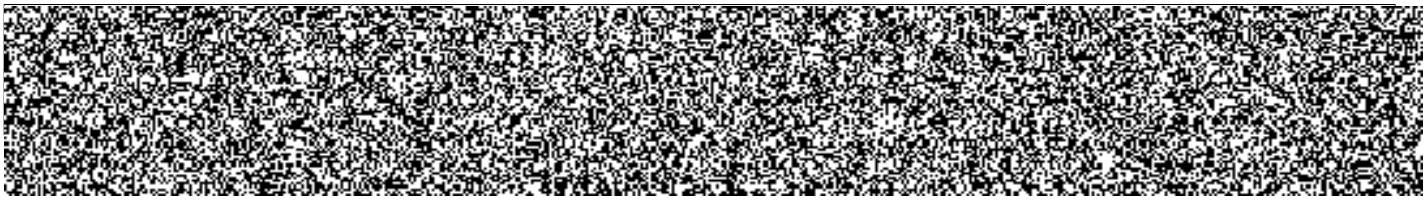
3.13 Manažer projektu



3.14 Další pracovníci projektového týmu



3.15 Kontaktní osoby



5. Popis projektu

5.1 Hlavní cíl projektu a jeho charakteristika

Hlavní cíl projektu a jeho charakteristika

Hlavním cílem projektu je zefektivnění operativní činnosti bezpečnostních týmů (CSIRT/CERT) za účelem zvýšení ochrany a odolnosti kritických informačních infrastruktur a významných informačních systémů.

Současná bezpečnostní praxe vykazuje z pohledu operativní činnosti bezpečnostních týmů řadu nedostatků. Množství a různorodost bezpečnostních a infrastrukturních dat se neustále zvyšuje, úroveň provázanosti v datech klesá, a s tím tak narůstá komplexita práce s nimi. S tím souvisí také vzrůstající počet vzájemně neprovázaných bezpečnostních nástrojů, jež musí členové bezpečnostních týmů používat při řešení incidentů. Celou problematiku pak podtrhuje nízký stupeň automatizace a nezanedbatelné množství manuálních kroků v celém procesu řízení životního cyklu hrozeb. Cílem předkládaného projektu je tyto nedostatky eliminovat.

K tomuto účelu je nutné vytvořit soubor nástrojů (Systém), který poskytne bezpečnostnímu týmu ucelený pohled na chráněnou infrastrukturu z hlediska všech relevantních dat a dovolí automatizovat rutinní činnosti v rámci procesu řízení životního cyklu hrozeb, včetně orchestrace typicky používaných bezpečnostních nástrojů. Důležitá je v tomto ohledu existence jednotného uživatelského prostředí, jež poskytne jednotlivým členům týmu vysoce kontextualizované pohledy na chráněnou infrastrukturu, dovolí jim reagovat na hrozby z centrálního bodu a umožní jim úzce spolupracovat při řešení bezpečnostních incidentů.

Naplnění hlavního cíle povede ke zvýšení úrovně ochrany a situačního povědomí o KII a VIS. Automatizace a orchestrace bezpečnosti v kolaborativním prostředí dovolí bezpečnostním týmům rychleji a jednodušeji reagovat na hrozby a zároveň tak dojde ke snížení požadavků na počet a vstupní expertízu členů bezpečnostních týmů. Toto je důležitý faktor vzhledem ke vnímanému nedostatku kvalifikovaných pracovníků v oboru kybernetické bezpečnosti a ICT. Celkově dojde ke zvýšení technické připravenosti ČR v oblasti kybernetické bezpečnosti.

5.2 Dílčí cíle projektu

Dílčí cíle projektu

K naplnění hlavního cíle projektu byly stanoveny následující dílčí cíle v podobě výzkumu metod a vývoje nástrojů pro podporu operativní činnosti bezpečnostních týmů při ochraně KII a VIS:

• Zvýšení úrovně situačního povědomí za pomoci integrovaného datového pohledu na chráněnou infrastrukturu. Dílčím cílem je výzkum metod a vývoj nástrojů, jež umožní integrovat různorodé typy bezpečnostních a infrastrukturních dat do jednotného úložiště, zvýšit jejich provázanost, a vytvořit tak podporu pro ucelený datový pohled na zájmové entity chráněné infrastruktury.

• Automatizace a orchestrace rutinních činností v procesu řízení životního cyklu hrozeb. Dílčím cílem je výzkum metod a vývoj nástrojů, které dovolí automatizovat vybrané operativní činnosti prováděné členy bezpečnostních týmů a umožní orchestraci typicky používaných bezpečnostních nástrojů, s nimiž se zpravidla pracuje samostatně. Nedílnou součástí cíle je identifikace, analýza a formalizace procesů probíhajících při řízení životního cyklu hrozeb, včetně určení relevantních externích systémů, lidských aktérů, a jejich odpovídajících rolí.

• Efektivní prezentace dat a podpora spolupráce členů bezpečnostního týmu v centrálním bodě. Dílčím cílem je výzkum metod a vývoj nástrojů, které budou tvořit jednotné uživatelské prostředí pro podporu operativní činnosti jednotlivých členů bezpečnostního týmu. Toto je motivováno snahou snížit kognitivní nároky na členy týmu při dohledu nad chráněnou infrastrukturou. S ohledem na předchozí dílčí cíle zajistí jednotné prostředí prezentaci vysoce kontextualizovaných a silně provázaných dat o zájmových entitách. Díky důrazu na vysokou interaktivitu a integraci nástrojů a prvků pro kolaborativní práci do jednoho centrálního bodu, bude možné řešit bezpečnostní incidenty efektivněji.

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	3

5.5 Popis současného stavu problematiky řešené oblasti

Popis současného stavu problematiky řešené oblasti

Hlavní řešenou oblastí projektu je efektivita operativní činnosti bezpečnostních týmů při ochraně KII a VIS v kontrastu s rostoucím počtem hrozeb a nedostatkem kvalifikovaných pracovníků v oboru kybernetické bezpečnosti a ICT. Předmětem zájmu je proces řízení životního cyklu hrozeb, jež se typicky skládá z následujících fází (viz sekce 5.14): sběr dat; detekce; třídění a kvalifikace; šetření; mitigace a zotavení; revize a post-analýza. Z pohledu řešené oblasti a zaměření projektu lze současný stav problematiky shrnout následovně.

• Nízká úroveň situačního povědomí o stavu chráněné infrastruktury. V současnosti neexistují podpůrné nástroje zajišťující dostatečnou úroveň situačního povědomí, což plyne především ze způsobu, jakým jsou zpracovávána infrastrukturní a bezpečnostní data. Ta jsou typicky produkována v různých podobách z mnoha separátních zdrojů a míra jejich propojení je velmi nízká. Přirozeně tak neexistuje uživatelské prostředí, které by efektivně prezentovalo relevantní pohledy na zájmové entity (viz sekce 5.14) dané infastruktury. Členové bezpečnostních týmů tak musí složitě kombinovat informace z různých zdrojů a obtížně si vytvářet celkový obraz o stavu chráněné infrastruktury. To klade vysoké kognitivní i odborné nároky na členy bezpečnostních týmů, jež musí být schopni udržovat kompletní přehled o dění v prostředí organizace, a navíc rychle reagovat na identifikované hrozby.

Popis současného stavu problematiky řešené oblasti

• Nezanedbatelné množství manuálně vykonávaných a rutinních činností v procesu řízení životního cyklu hrozeb. I přes postupný nárůst automatizace procesů a postupů při řízení životního cyklu hrozeb je stále velký počet činností vykonáván manuálně. Množství těchto činností je navíc nutné provádět v řadě vzájemně nepropojených systémů, což celý problém dále komplikuje. Procesy a postupy pro operativní činnost daného týmu jsou typicky zpracovány v textové podobě (ať už ve formě tištěných, či elektronických dokumentů) a jednotlivým členům slouží pouze jako vodítka při jejich činnosti. Kombinace výše uvedených faktorů vede ke zvýšené náchylnosti na vznik chyb a snížení účinnosti bezpečnostních opatření.

• Omezená podpora pro spolupráci členů bezpečnostních týmů při řešení bezpečnostních incidentů. Spolupráce členů bezpečnostního týmu je při řešení bezpečnostního incidentu klíčovou aktivitou v procesu řízení hrozeb. Tato aktivita zahrnuje sdílení dat a zjištěných informací, jež se vztahují k danému incidentu a plyne z ní také požadavek na strukturovanou formu komunikace v reálném čase při předávání nabytých informací. Členové týmu navíc využívají řadu různých bezpečnostních nástrojů, které typicky nejsou vůbec propojeny. Tato různorodost v kombinaci s nedostatečnými prostředky pro sdílení informací zvyšuje dobu pro vyřešení bezpečnostních incidentů a zvyšuje nároky na členy týmu. Myšlenka prostředí pro spolupráci zaměřeného na řešení bezpečnostních incidentů je v kontextu operativní činnosti bezpečnostních týmů poměrně ojedinělá. Současné projekty věnující se sdílení a spolupráci v kontextu kyberbezpečnosti jsou zpravidla zaměřeny na sdílení informací mezi organizacemi, ne však v rámci bezpečnostního týmu.

Níže je uveden seznam relevantních projektů v rámci výzkumných programů na kybernetickou bezpečnost a ochranu KII a VIS. Na základě rešerše veřejně dostupných informací lze konstatovat, že žádný z uvedených projektů není zaměřen na podporu operativní činnosti bezpečnostních týmů v rozsahu navrhovaném předkládaným projektem.

Systémy pro sdílení informací o bezpečnostních událostech:

• [SABU, VI20162019029] Sdílení a analýza bezpečnostních událostí v ČR (řešeno uchazečem)
• [VH20172021022] Vybudování a ověřovací provoz systému Cyber Threat Intelligence
• [VI20152020026] Predikce a ochrana před kybernetickými incidenty
• [C3ISP, 700294, EU/H2020] Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Analýza a detekce incidentů:

• [KYPO II, VI20162019014] Simulace, detekce a potlačení kybernetických hrozeb ohrožujících kritickou infrastrukturu (řešeno uchazečem)
• [ITOA, TH02010185] Výzkum a vývoj pokročilých analytických nástrojů pro analýzu bezpečnostních a výkonnostních problémů síťové infrastruktury, aplikací a služeb (řešeno uchazečem)
• [Security Cloud, TA04010062/2014] Technologie pro zpracování a analýzu síťových dat velkého rozsahu (řešeno uchazečem)
• [VG20122014079] Behaviorální detekce pokročilých útočníků v počítačových sítích
• [VI20172019054] Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti
• [VI20172019057] Monitoring a analýza komunikace pro bezpečnostní dohled kritických energetických infrastruktur
• [VI20172020078] Systém pro centralizovaný dohled nad komplexními a rozlehlými objekty kritické infrastruktury státu

Situační povědomí:

• [CRUSOE, VI20172020070] Výzkum nástrojů pro hodnocení kybernetické situace a podporu rozhodování CSIRT týmů při ochraně kritické infrastruktury (řešeno uchazečem)
• [DiSIEM, 700692, EU/H2020] Diversity Enhancements for Security Information and Event Management
• [PROTECTIVE, 700071, EU/H2020] Proactive Risk Management through Improved Cyber Situational Awareness
• [SHIELD, 700199, EU/H2020] Securing Against Intruders and Other Threats Through a NFV-Enabled Environment

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 a naplnění projektu budou mít bezprostřední vliv na zvýšení technické vybavenosti ČR a optimalizaci operativních činností v každodenní praxi bezpečnostních týmů chránících KII a VIS. Výstupy projektu přispějí k naplnění Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 v prioritních oblastech Ochrana národní kritické informační infrastruktury (KII) a významných informačních systémů (VIS), potažmo cílů definovaných v souvisejícím Akčním plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 (dále jen Akční plán). V neposlední řadě, výstupy projektu přispějí také k plnění cílů tematické oblasti 2) Bezpečnost kritických infrastruktur, podoblastí a), b) a d) Programu.

Konkrétní přínosy a dopady výsledků projektu zahrnují:

• Získání uceleného pohledu na chráněnou infrastrukturu spočívající v integraci různorodých infrastrukturních a bezpečnostních dat z existujících bezpečnostních nástrojů. Jednotný pohled na všechna relevantní data povede ke zvýšení přesnosti a účinnosti opatření v oblasti aktivní obrany a ochrany proti kybernetickým útokům. Tyto přínosy budou realizovány zejména Výsledkem č. 1, který tak adresuje cíle C.4.01-03 Akčního plánu. Realizace výsledku adresuje problém nedostatečné úrovně situačního povědomí o chráněné KII a VIS, která je dnes dána zejména způsobem zpracování relevantních dat. Ta jsou typicky produkována v různých podobách z mnoha separátních zdrojů a míra jejich propojení je velmi nízká.

• Optimalizace procesu řízení životního cyklu hrozeb spočívá v identifikaci, analýze, formalizaci a automatizaci používaných předpisů a postupů (viz výstupy cíle A.2.04 Akčního plánu). Formalizace těchto předpisů umožní jejich strojové zpracování a tam, kde to bude možné, také automatizaci prováděných činností. Výstupy pak budou realizovány primárně Výsledkem č. 2, který tak přispěje k naplnění cílů C.6.03, C.6.05 a G.2.01-02 Akčního plánu. Důsledkem bude netriviální redukce počtu manuálních úkonů, jež povede ke zkrácení doby řešení bezpečnostních incidentů a k celkovému zefektivnění tohoto procesu.

Přínosy a dopady projektu v oblasti bezpečnosti a cílů stanovených Programem

• Pokročilé prostředí pro spolupráci při řízení životního cyklu hrozeb je zásadní komponentou. Bude poskytovat sadu nástrojů pro bezpečné sdílení informací mezi členy bezpečnostního týmu, které vznikají při řešení incidentů. Komponenta umožní efektivní prezentaci dat a sjednotí ovládání nástrojů vzniklých v rámci projektu a také existujících bezpečnostních nástrojů prostřednictvím jednotného uživatelského rozhraní. Zároveň bude poskytovat funkcionalitu umožňující interaktivní manipulaci s daty o chráněné infrastruktuře. Data budou plněna automatizovanými postupy a procesy, které vzniknou v rámci Výsledků č. 1 a 2. Prostředí pro spolupráci bude součástí Výsledku č. 3 a bude dále rozvíjet cíle C.4.03, C.6.03 a D.5.01 Akčního plánu. Realizace výsledku povede k zásadnímu zvýšení uživatelského komfortu členů bezpečnostního týmu při řešení bezpečnostních incidentů a při řízení hrozeb, a také ke zlepšení situačního pohledu na chráněnou infrastrukturu.

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

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

Projekt bude řešen iterativně a inkrementálně dle harmonogramu uvedeném v bodě 5.12. Vzhledem k povaze plánovaných výsledků bude možné na nich pracovat paralelně a průběžně je integrovat do ucelené podoby tak, aby naplnily hlavní cíl projektu. Uchazeč získal řadu cenných zkušeností při řešení předchozích projektů bezpečnostního výzkumu. Řešitelský tým je díky tomu dobře obeznámen se současným stavem problematiky kybernetické bezpečnosti a ochrany KII a VIS v ČR i zahraničí. Dále také prokázal schopnost realizovat složité systémy z oblasti kyberbezpečnosti. Při řešení projektu budou průběžně probíhat věcné konzultace řešitele, gestora a uživatelů výsledků projektu tak, aby plánované výstupy naplnily uživatelské potřeby a byly aktuální při ukončení projektu.

Po nezbytné analytické fázi bude navržena architektura Systému jakožto celku, a to především z pohledu detailního rozpracování jeho jednotlivých komponent, jež ve vysoké míře odpovídají plánovaným výsledkům projektu. Komponenty odpovídající výsledkům č. 1 a č. 2 budou využitelné samostatně a budou mít definovány vhodná komunikační rozhraní a formáty výměny dat. Cílem je zajištění interoperability a dekompozice funkcionality tak, aby bylo možné obě komponenty používat i ve spojení s dalšími nástroji. Komponenta odpovídající výsledku č. 3 má zásadní roli – vytváří uživatelskou nástavbu pro podporu spolupráce a pro celý Systém poskytuje jednotné uživatelské rozhraní.

Při realizaci jednotlivých komponent bude postupováno takto:

• Software pro integrovaný datový pohled na chráněnou infrastrukturu bude využívat existující návrhové vzory z oblasti datové integrace – především se jedná o návrhový vzor pro normalizaci, kdy jsou data převáděna do tzv. kanonického datového modelu. Normalizace umožňuje zpracování a výměnu dat, která jsou sémanticky ekvivalentní, ale používají různé datové formáty. Normalizace je používána v případech, kdy je nutné integrovat data z různorodých systémů tak, aby s nimi bylo možné pracovat jednotně. Plánovaná integrace zahrnuje například následující kategorie dat – informace o složení a konfiguraci chráněné infrastruktury, provozní bezpečnostní data, informace o hrozbách a zranitelnostech, hlášení o bezpečnostních událostech a incidentech či dodatečné informace o zájmových entitách. Normalizovaná data budou uložena v jednotném úložišti tak, aby je bylo možné jednoduše korelovat a agregovat za účelem zvýšení jejich provázanosti a docílení možnosti tvorby vysoce kontextualizovaných dotazů.

• Software pro podporu orchestrace bezpečnosti a řízení životního cyklu hrozeb bude čerpat z obecných poznatků v oblasti procesního řízení a automatizace procesů. Z pohledu výzkumných aktivit je důležité určit, do jaké míry lze tyto poznatky a existující technologie aplikovat na problematiku operativní činnosti bezpečnostních týmů. V současnosti musí členové bezpečnostních týmů, v rámci procesu řízení hrozeb, často provádět opakované manuální aktivity v řadě vzájemně nepropojených systémů. Při realizaci výsledku výzkumný tým identifikuje vybrané aktivity a zajistí jejich převedení do formy automatizovaných bezpečnostních předpisů, tzv. playbooků, včetně vazeb na externí systémy. V tomto kontextu je důležité zdůraznit potřebu identifikace, analýzy a formalizace procesů probíhajících při řízení životního cyklu hrozeb, včetně určení relevantních externích systémů, automatizovatelných aktivit, lidských aktérů, a jejich odpovídajících rolí.

• Kolaborativní prostředí pro členy bezpečnostních týmů bude mít podobu webové aplikace, jež poskytne přehled o stavu chráněné infrastruktury a pro uživatele bude představovat centrální bod pro interakci se Systémem. Uživatelské prostředí bude založeno na modulárním webovém frameworku, který umožní tvorbu specializovaných pohledů na chráněnou infrastrukturu reflektujících například: typ bezpečnostního incidentu, druh zájmové entity, fázi životního cyklu hrozeb, či aktuální uživatelskou roli. Součástí prostředí bude nejen samotné uživatelské rozhraní, ale také soubor odpovídajících datových služeb, funkcionalita pro podporu komunikace v reálném čase, a zejména také nástroj pro bezpečné sdílení kontextově obohacených dat o řešených incidentech a hrozbách. Sdílení informací bude založeno na principu zabezpečených izolovaných pracovních složek, obsahujících relevantní data týkající se dané bezpečnostní hrozby či incidentu.

Z hlediska použitých technologií bude kladen důraz na využití open-source nástrojů a knihoven. Technologie, programovací jazyky a frameworky budou zvoleny tak, aby bylo možné zkoumané metody a nástroje rapidně prototypovat, avšak bez rizika omezení produkčního potenciálu. V počátcích realizace zaměří řešitelský tým svoji pozornost především na následující potenciálně využitelné technologie: platforma pro proudové zpracování dat (Apache Kafka, Apache Flink, Apache Spark), úložiště pro data velkého rozsahu (Elasticsearch, Druid, Hadoop), platforma pro orchestraci procesů (Activiti, Camunda), framework pro tvorbu datových služeb a REST rozhraní (Spring Boot, Django) a MVVM framework pro tvorbu uživatelských rozhraní (Angular, Vue).

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 – jediného bezpečnostního týmu v ČR certifikovaného úřadem Trusted Introducer.

Realizace jednotlivých výsledků bude řešena specializovanými skupinami, jež budou tvořeny řešiteli projektu, disponujícími potřebnými zkušenostmi. Jednotliví řešitelé se těmto tématům přímo věnují v rámci svého výzkumu či odborné praxe. Řešená témata jsou zároveň předmětem jejich disertačních či habilitačních prací. Jelikož výsledky budou vyžadovat také netriviální podíl vývojových prací spojených s vytvořením softwarových nástrojů, budou do projektu, na pozice programátorů, zapojeni studenti Fakulty informatiky MU.

Masarykova univerzita disponuje potřebným technologickým zázemím pro řešení projektu. V rámci Centra excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur (C4e, reg. č. CZ.02.1.01/0.0/0.0/16_019/0000822) bude poskytnuta výpočetní a

Způsob a podíl zapojení jednotlivých účastníků do realizace projektu

síťová infrastruktura pro vývoj a testování vytvářeného software. V případě potřeby bude další infrastruktura zajištěna v rámci univerzitního centra CERIT Scientific Cloud (CERIT-SC – OP VaVpI reg. č. CZ. 1.05/3.2.00/08.0144).

Pilotní nasazení výsledků projektu bude provedeno řešitelským týmem v rámci infrastruktury Masarykovy univerzity. Výsledky projektu budou napojeny na technické a programové vybavení, které využívá bezpečnostní tým CSIRT-MU při ochraně sítě MU. Dále předpokládáme uplatnění výsledku i u dalších subjektů státní správy (NAKIT, GovCERT.cz a jimi koordinovanými týmy dohlížejícími na kybernetickou bezpečnost KII a VIS), či u třetích stran (firem a organizací) zajišťujících budování nebo provoz bezpečnostních operačních středisek v kontextu ochrany KII a VIS.

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 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), Ministerstvo vnitra a bezpečnostní týmy (Vládní CERT ČR, národní CSIRT ČR, CESNET-CERTS, CSIRT-MU a další). Výsledky projektu najdou uplatnění při plnění požadavků vyplývajících ze Zákona o kybernetické bezpečnosti, dlouhodobé strategie Evropské unie a strategických cílů a závazků České republiky v rámci NATO.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost. Mezi jeho hlavní úlohy patří koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům a přijímání opatření proti probíhajícím útokům při řešení incidentů. NÚKIB také provozuje Vládní CERT (GovCERT.CZ), který hraje klíčovou roli při ochraně KII a VIS. Plánované výsledky projektu budou poskytnuty Vládnímu CERT a jemu podřízeným a s ním spolupracujícím organizacím, zajišťujících bezpečnost IT infrastruktur jednotlivých resortů.

Ministerstvo vnitra plní úkoly v oblasti vnitřní bezpečnosti a veřejného pořádku. Z hlediska kybernetické bezpečnosti má klíčovou roli především jako hlavní gestor elektronizace výkonu veřejné správy (eGovernmentu) a je zodpovědné za provoz celé řady VIS důležitých pro fungování státní správy (základní registry, datové schránky, systém Czech POINT atd.). Výstupy projektu naleznou uplatnění především u Národní agentury pro komunikační a informační technologie (NAKIT), jež mimo jiných úkolů, zajišťuje rovněž provoz a bezpečnostní dohled nad komunikačními sítěmi pro potřeby složek integrovaného záchranného systému (IZS) a VIS státní správy.

Výsledky projektu budou využitelné i dalšími organizacemi řešícími problematiku kybernetické bezpečnosti a bezpečnostního výzkumu i mimo oblast státní správy. Jedná se o třetí strany (firmy a organizace) zajišťující budování či provoz bezpečnostních operačních center v kontextu ochrany KII a VIS.

Zájem a podpora projektu ze strany subjektů státní správy i třetích stran je vyjádřena formou dopisů uvedených v příloze 4.3.4.

V neposlední řadě budou výsledky projektu využity bezpečnostním týmem uchazeče (CSIRT-MU), který je použije pro ochranu informačních a komunikačních systémů Masarykovy univerzity. Výsledky projektu budou rozvíjeny v jeho dalších vědecko-výzkumných aktivitách. Cílem uchazeče je vytvořit a dále rozvíjet plánované výsledky takovým způsobem, 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.

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 Kolaborativní prostředí – Etapa I Sběr uživatelských požadavků a tvorba modulárního frameworku pro tvorbu kontextualizovaných pohledů. Tvorba základních pohledů na chráněnou infrastrukturu.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x		
1.2 Nástroj pro integrovaný datový pohled – Etapa I Identifikace a analýza relevantních datových zdrojů pro základní kategorie bezpečnostních a infrastrukturních dat. Návrh kanonického modelu dat. Tvorba vstupních datových konektorů.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x		
1.3 Nástroj pro orchestraci a řízení hrozeb – Etapa I Identifikace , analýza a formalizace procesů probíhajících při řízení životního cyklu hrozeb, včetně určení relevantních externích systémů, lidských aktérů, a jejich odpovídajících rolí.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x		
1.4 Prvotní integrace nástrojů a ověření jejich vlastností Ověření navrhnutých komunikačních rozhraní a formátů výměny dat. Prvotní integrace vytvořených SW artefaktů a ověření jejich vlastností.	Masarykova univerzita / Ústav výpočetní techniky									x	x	x	x
Rok 2021													

Název činnosti	Uchazeč	0bdobí, kdy je činnost uskutečňována											
		1	2	3	4	5	6	7	8	9	10	11	12
2.1 Kolaborativní prostředí – Etapa II Tvorba pokročilých pohledů na chráněnou infrastrukturu. Návrh a implementace základní verze uživatelského prostředí pro podporu spolupráce a pro bezpečné sdílení kontextově obohacených dat o řešených incidentech a hrozbách.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x		
2.2 Nástroj pro integrovaný datový pohled – Etapa II Návrh a implementace normalizační logiky pro převod dat do kanonického datového modelu. Zapojení do platformy pro proudové zpracování dat. Tvorba výstupních konektorů do datových úložišť.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x		
2.3 Nástroj pro orchestraci a řízení hrozeb – Etapa II Identifikace a automatizace základních aktivit v procesu řízení hrozeb. Návrh a implementace vybraných orchestračních scénářů - bezpečnostních playbooků.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x	x	x	x	x		
2.4 Pokročilé ověření schopností vytvořených nástrojů Ověření schopností vytvořených nástrojů ve formě uceleného prototypu se základní funkcionalitou. Revize a vylepšení navrhnutých komunikačních rozhraní a formátů výměny dat.	Masarykova univerzita / Ústav výpočetní techniky									x	x	x	x
Rok 2022													
3.1 Kolaborativní prostředí – Etapa III Finalizace implementace uživatelského prostředí pro podporu spolupráce a pro bezpečné sdílení kontextově obohacených dat o řešených incidentech a hrozbách.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x						
3.2 Nástroj pro integrovaný datový pohled – Etapa III Tvorba agregačních a korelačních operátorů pro proudové zpracování. Návrh a implementace dotazovací vrstvy pro integrovaný datový pohled.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x						
3.3 Nástroj pro orchestraci a řízení hrozeb – Etapa III Identifikace a automatizace pokročilých aktivit v procesu řízení hrozeb. Návrh a implementace složitějších orchestračních scénářů.	Masarykova univerzita / Ústav výpočetní techniky	x	x	x	x	x	x						
3.4 Provázání vytvořených nástrojů do ucelené podoby Integrace vytvořených nástrojů do jednotného celku - materializace Systému jako centrálního bodu pro řízení hrozeb a orchestraci bezpečnosti.	Masarykova univerzita / Ústav výpočetní techniky				x	x	x	x	x	x			
3.5 Ověření vytvořených nástrojů a jejich použitelnosti v praxi Uživatelské a zátěžové testování. Ověření praktické použitelnosti Systém při testovacím provozu nad reálnou infrastrukturou.	Masarykova univerzita / Ústav výpočetní techniky							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
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 týmů, 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

Popis rizik projektu a jejich řízení

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 ukončení vývoje klíčové technologie
Pravděpodobnost: střední
Závažnost: střední
Opatření: Tým průběžně sleduje technologické trendy a je schopen pružně reagovat v případě potřeby změny technologií. Budou využity open-source technologie, jejichž vývoj je řízen a financován renomovanými společnostmi. Návrh software bude umožňovat případnou výměnu použité technologie.

Riziko nedostupnosti dat pro vývoj a testování výsledků
Pravděpodobnost: nízká
Závažnost: vysoká
Opatření: Uchazeč disponuje vlastním bezpečnostním týmem, který v rámci své agendy sbírá data o bezpečnostních událostech a incidentech. Další vzorky dat je možné získat ze systémů pro sdílení informací o bezpečnostních událostech, na jejichž vývoji se uchazeč podílí.

- 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

Řízení životního cyklu hrozeb je stěžejní proces v rámci operativní činnosti bezpečnostních týmů při ochraně KII a VIS. Jedná se o opakující se posloupnost bezpečnostních postupů a činností běžně organizovaných do šesti fází. Je nutné podotknout, že aktivity a činnosti v rámci jednotlivých fází typicky probíhají v rámci několika separovaných systémů.

- Fáze 1 (Sběr dat) zahrnuje zajištění viditelnosti do dějů probíhajících v chráněné infrastruktuře. Je založena na principu akvizice relevantních dat pro zajištění ochrany dané infrastruktury, např. bezpečnostních událostí, provozních bezpečnostních dat, infrastrukturních dat a informací o síťovém provozu.

- Fáze 2 (Detekce) se zaměřuje na detekci hrozeb a reakci na ně. Vzhledem k množství a rychlosti vzniku dat v moderních infrastrukturách je při detekci kladen důraz na co nejvyšší stupeň automatizace. Detekční nástroj upozorňují na podezřelé a anomální děje, případně detekují známé signatury a indikátory kompromitace.

- Fáze 3 (Třídění a kvalifikace) se zabývá vyhodnocením hrozby za účelem stanovení míry dopadu na chráněnou infrastrukturu. Tato fáze vyžaduje rozhodnutí zkušeného bezpečnostního odborníka a je relativně časově náročná vzhledem k počtu manuálních kroků.

- Fáze 4 (Šetření) je zaměřena na podrobnější analýzu hrozby či incidentu s cílem určit jejich podstatu a případně míru zasažení dané infrastruktury. Míra automatizace rutinních analytických úkonů a nástrojů usnadňujících spolupráci mezi členy týmu i mezi organizacemi typicky určuje průměrnou dobu obnovení chráněné infrastruktury do bezpečného stavu.

- Fáze 5 (Mitigace a zotavení) se zaměřuje na aplikaci protiopatření za účelem zabránění šíření a následné eliminace hrozby. Stěžejní roli zde hraje dostupnost nástrojů a aktuálnost předpisů a procesů pro reakci na incidenty. Míra automatizace a orchestrace analogicky určuje průměrnou dobu obnovení chráněné infrastruktury do bezpečného stavu.

- Fáze 6 (Revize a post-analýza) přichází na řadu po úspěšné mitigaci incidentu. Tato fáze není časově kritická, je však časově náročná, a její dopady mají bezprostřední vliv na budoucí bezpečnost chráněné infrastruktury. Hlavní činnosti spočívají v důkladné forenzní analýze hrozby a souvisejících rizik, jejich reportingu a stanovení udržitelných bezpečnostních opatření, které jsou následně implementovány v rámci chráněné infrastruktury.

V kontextu ochrany informační infrastruktury je nutné mít přehled nejen o jednotlivých prvcích infrastruktury z pohledu fyzického světa, ale především z pohledu tzv. zájmových entit relevantních pro zajištění bezpečnosti. Zájmové entity jsou typicky předmětem procesu řízení životního cyklu hrozeb – mohou být buď cílem, nebo zdrojem hrozeb. Mezi vybrané zájmové entity patří například:

- uživatelé a jejich chování,
- stroje – HW servery, síťové prvky, prvky aktivní ochrany,
- instalovaný software,
- doménová jména strojů,
- běžící služby,
- běžící procesy,
- chráněné IP adresy,

Doplňující informace k projektu

- útočící IP adresy,
- blokované IP adresy,
- zranitelnosti strojů a instalovaného software,
- indikátory útoku a kompromitace,
- detekované útoky na chráněnou infrastrukturu.

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**	**9 927.325**	**0**	**9 927.325**	**100**
	2020	3 191.355	0	3 191.355	100
	2021	3 288.809	0	3 288.809	100
	2022	3 447.161	0	3 447.161	100
PROJEKT	**Celkem**	**9 927.325**	**0**	**9 927.325**	**100**

6.2 Rozpočet projektu

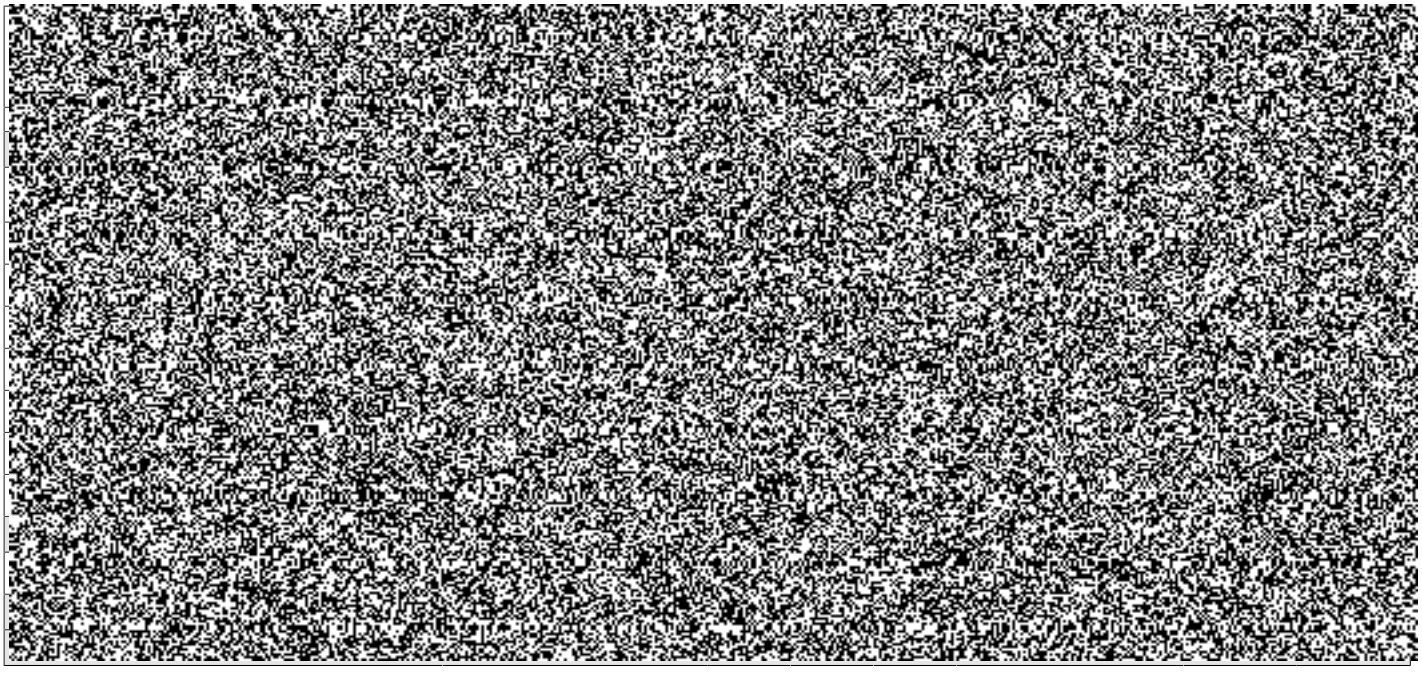
6.2.1 Výpočet maximální míry podpory uchazeče Masarykova univerzita / Ústav výpočetní techniky

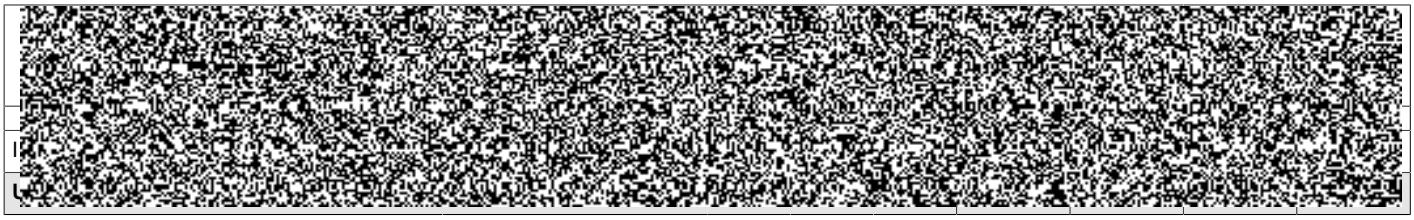
Kategorie uchazeče	výzkumná organizace
Kategorie výzkumu	experimentální vývoj
Způsobilé náklady uchazeče (tis. Kč)	**9 927.325**

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)	**9 927.325**

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





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	**2 579.783**	**2 629.783**	**2 679.783**	**7 889.349**
a) mzdy/platy na základě pracovního poměru	1 310.63	1 310.63	1 310.63	3 931.89
b) osobní náklady/výdaje na základě dohody o pracovní činnosti	604.8	604.8	604.8	1 814.4
c) osobní náklady/výdaje na základě dohody o provedení práce	0	0	0	0
d) povinné pojistné na sociální zabezpečení	478.858	478.858	478.858	1 436.574
e) povinné pojistné na zdravotní pojištění	172.389	172.389	172.389	517.167
f) odvody do FKSP nebo sociálního fondu	13.106	13.106	13.106	39.318
g) cestovné	0	50	100	150
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**	**150**	**260**
a) subdodávky	0	0	0	0
b) ostatní služby	40	70	150	260
audit	0	0	50	50
výjezdní zasedání	40	40	40	120
konferenční poplatky	0	30	60	90
Doplňkové náklady/výdaje - mezisoučet	**571.572**	**589.026**	**617.378**	**1 777.976**
režie	571.572	589.026	617.378	1 777.976
Celkové způsobilé náklady - mezisoučet	**3 191.355**	**3 288.809**	**3 447.161**	**9 927.325**
Celková státní podpora - mezisoučet	**3 191.355**	**3 288.809**	**3 447.161**	**9 927.325**

6.2.5 Rozpočet nákladů za celý projekt

Náklady/výdaje za celý projekt (tis. Kč)	2020	2021	2022	Celkem
Osobní náklady/výdaje	**2 579.783**	**2 629.783**	**2 679.783**	**7 889.349**
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**	**150**	**260**
Doplňkové náklady/výdaje	**571.572**	**589.026**	**617.378**	**1 777.976**
Celkové způsobilé náklady	**3 191.355**	**3 288.809**	**3 447.161**	**9 927.325**
Celková státní podpora	**3 191.355**	**3 288.809**	**3 447.161**	**9 927.325**

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS | PID: VI3VS/715 | 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

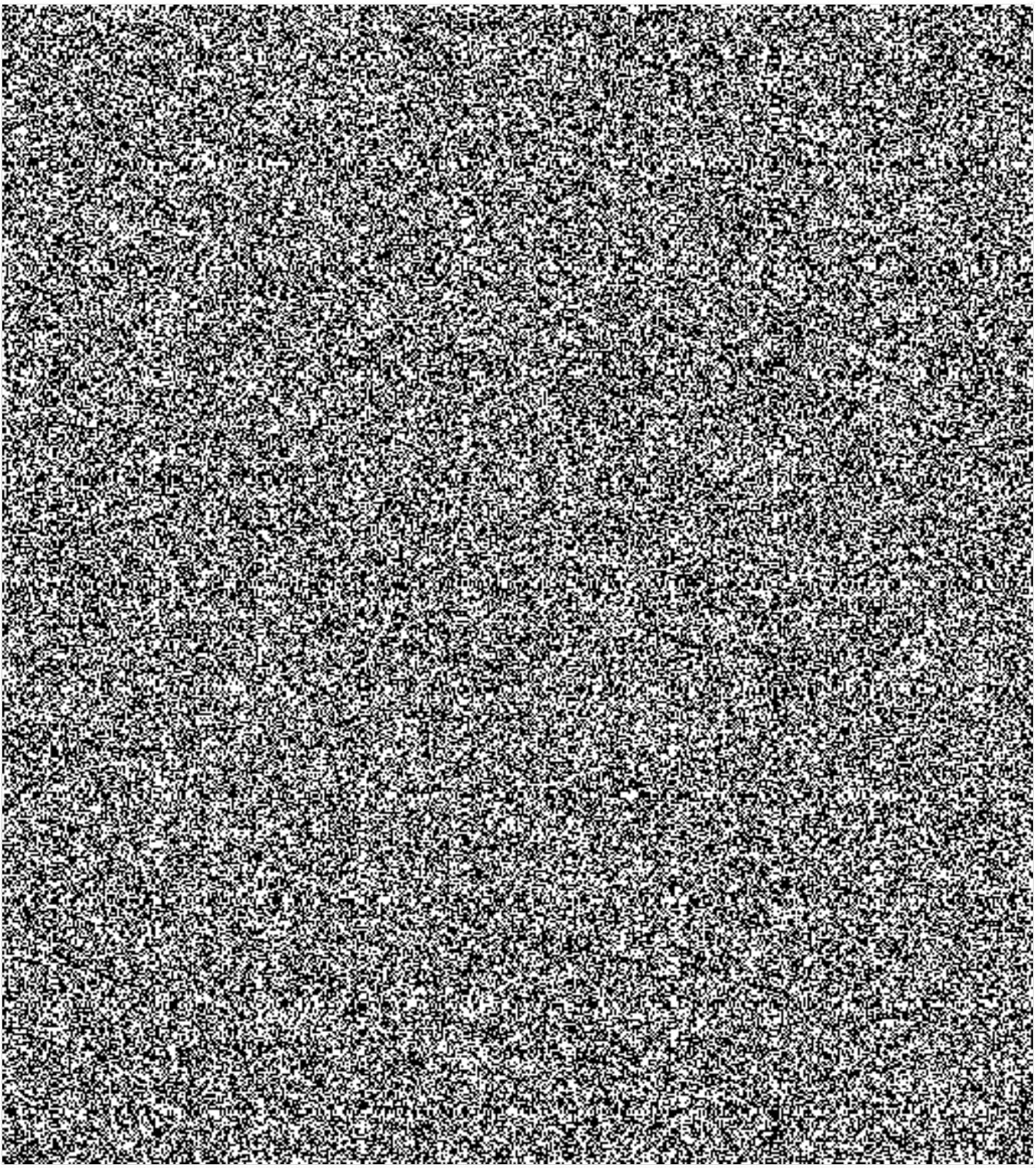
Titul před jménem	Jméno	Příjmení	Titul za jménem	Podpis
doc. PhDr.	Mikuláš	Bek	Ph.D.	

Elektronický podpis - 19.6.2019
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]: 10

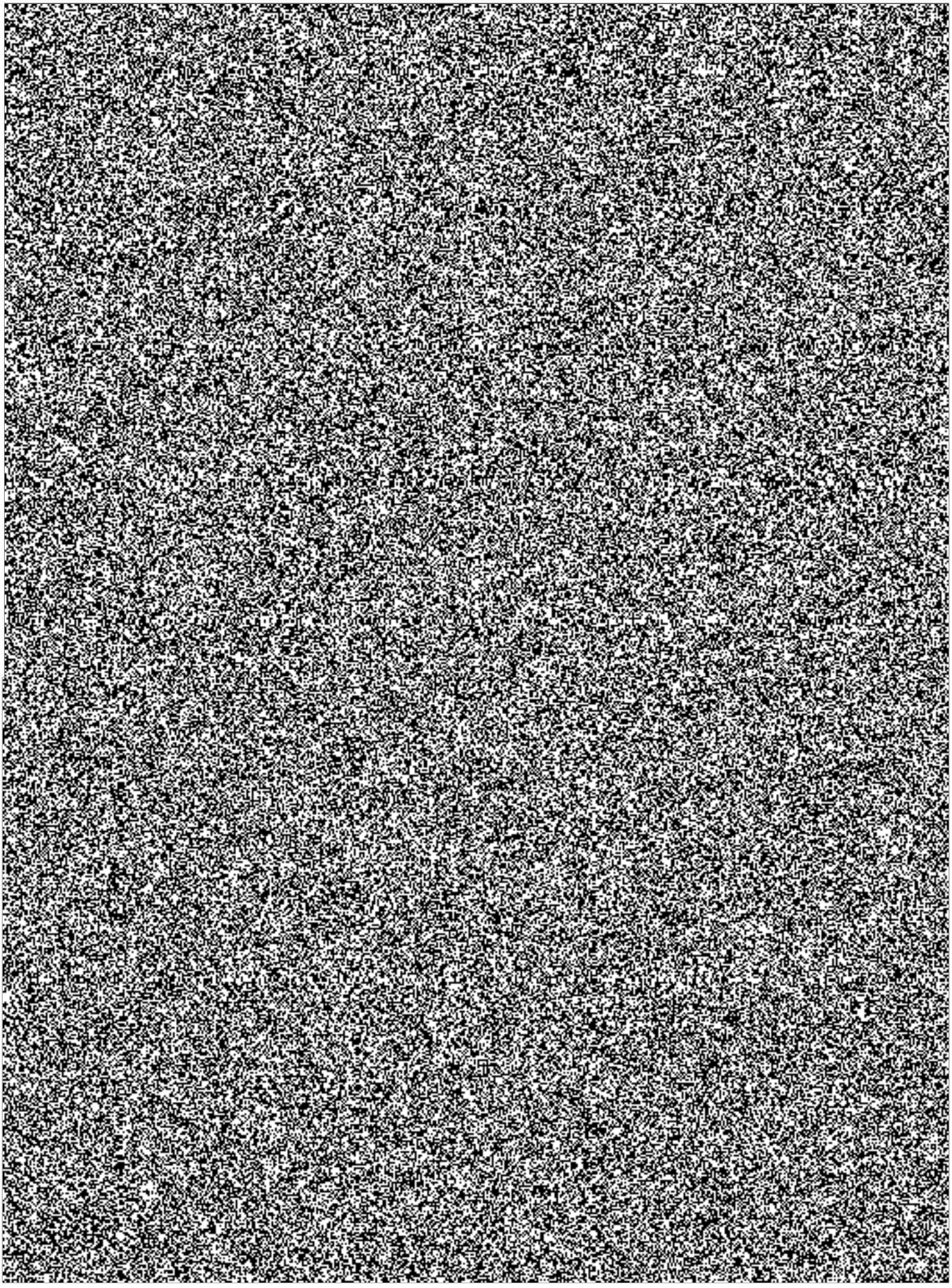
Plán využití výsledků projektu a jejich popis[2]

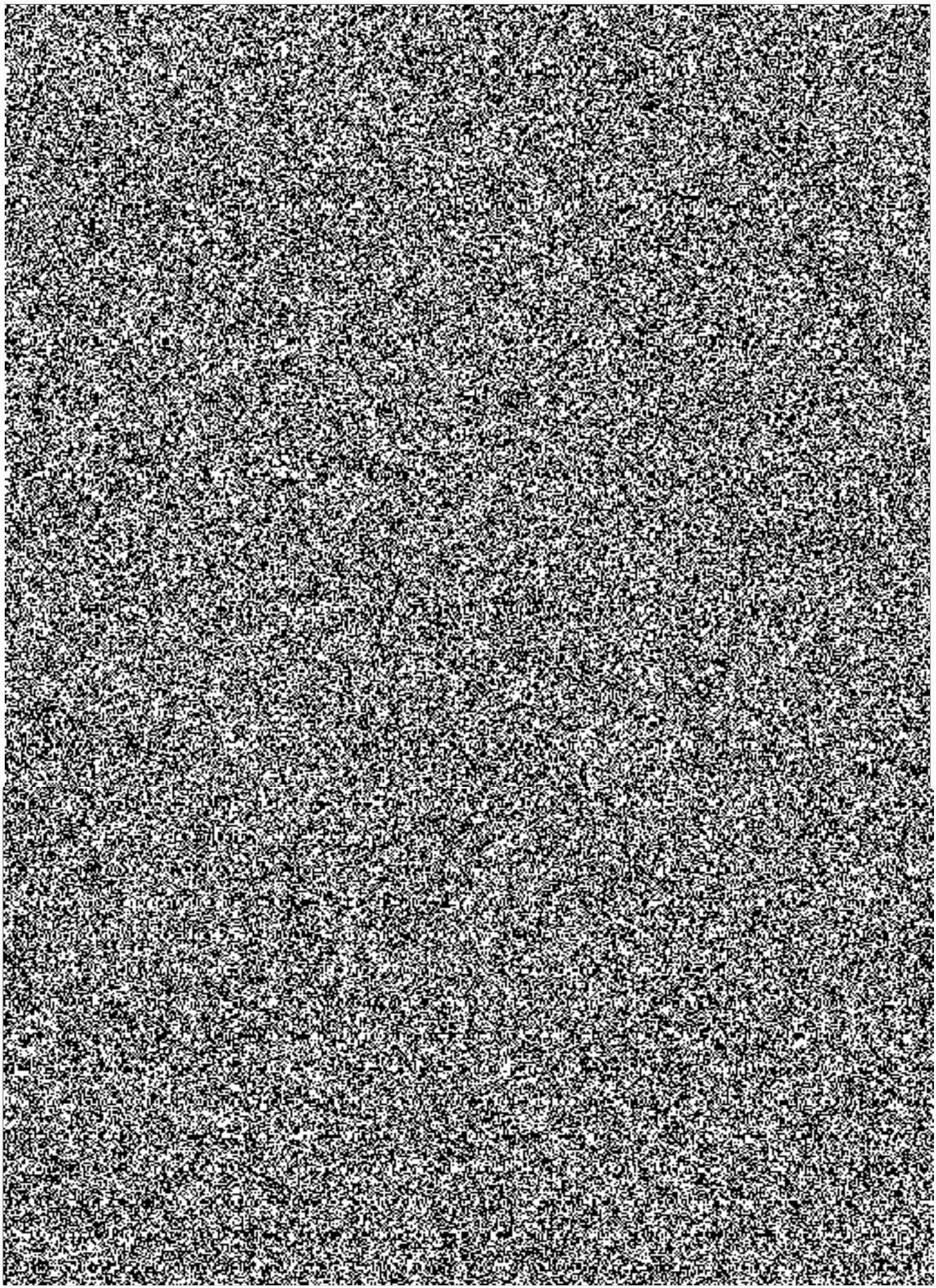


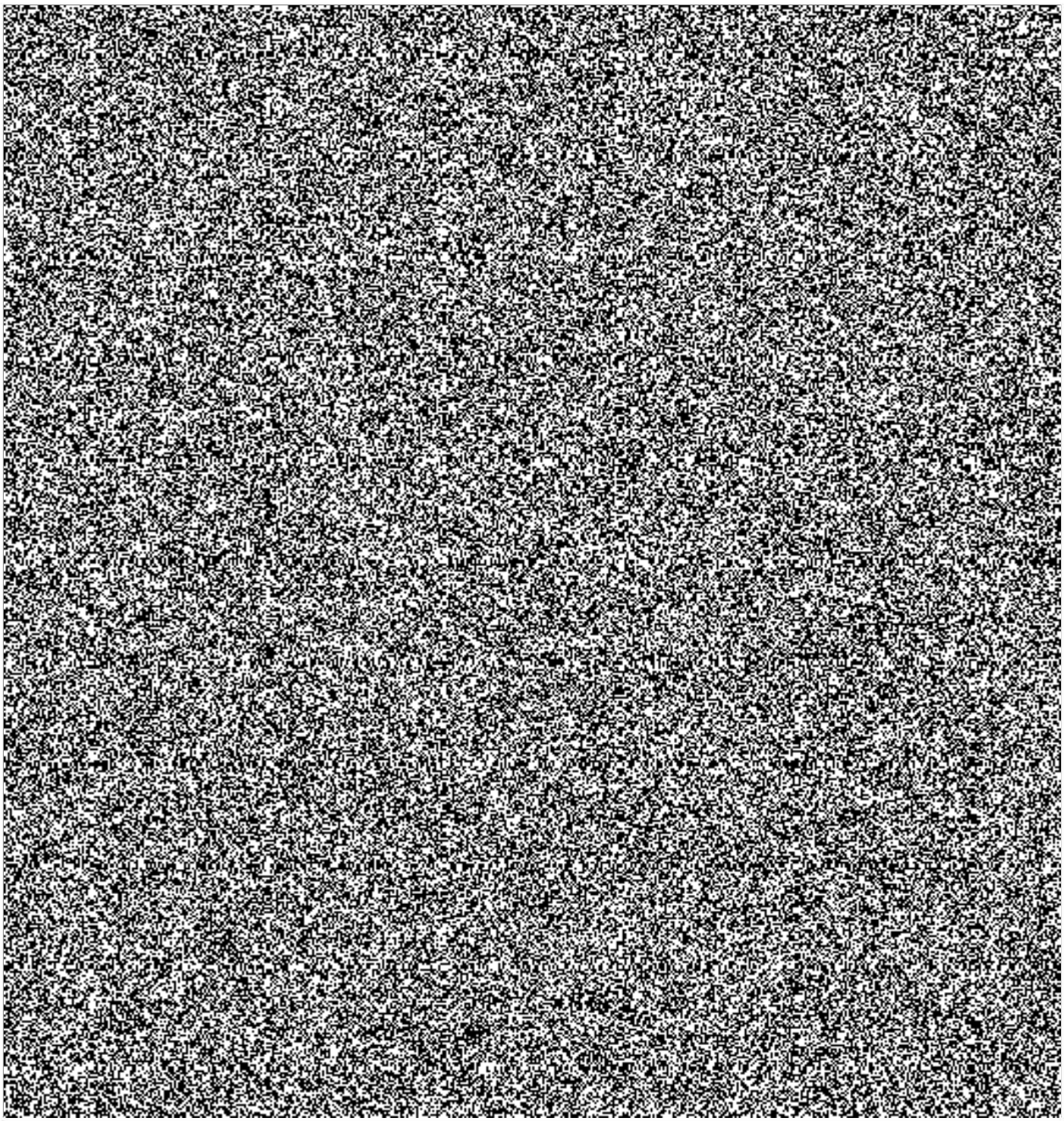
*) Uchazeč záhlaví vyplní, nehodící se škrtněte

[1] Uchazeč list vyplní, aktualizuje Počet listů

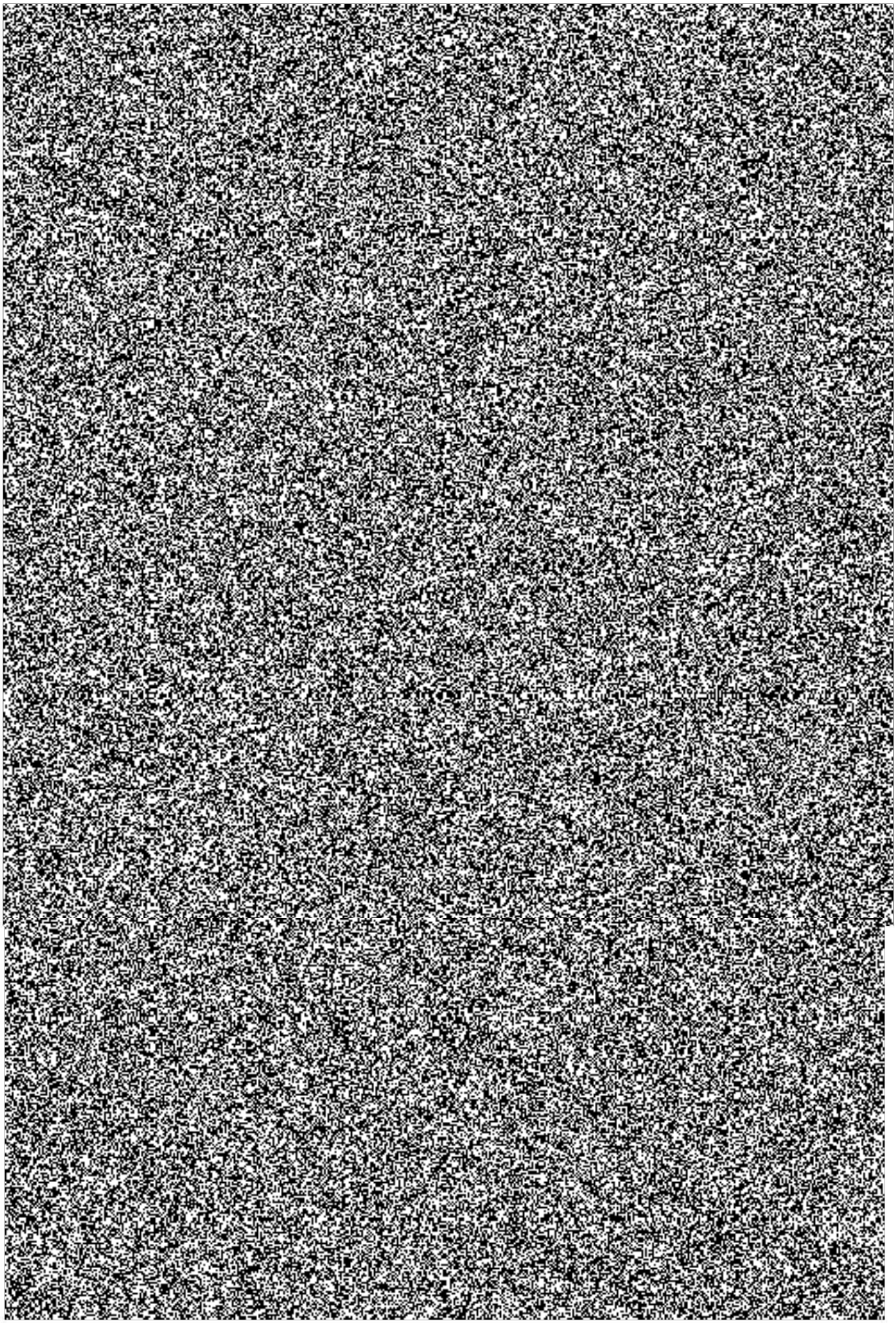
[2] Povinná příloha pro všechny uchazeče, v případě, že projekt podává více uchazečů, předkládá koordinátor

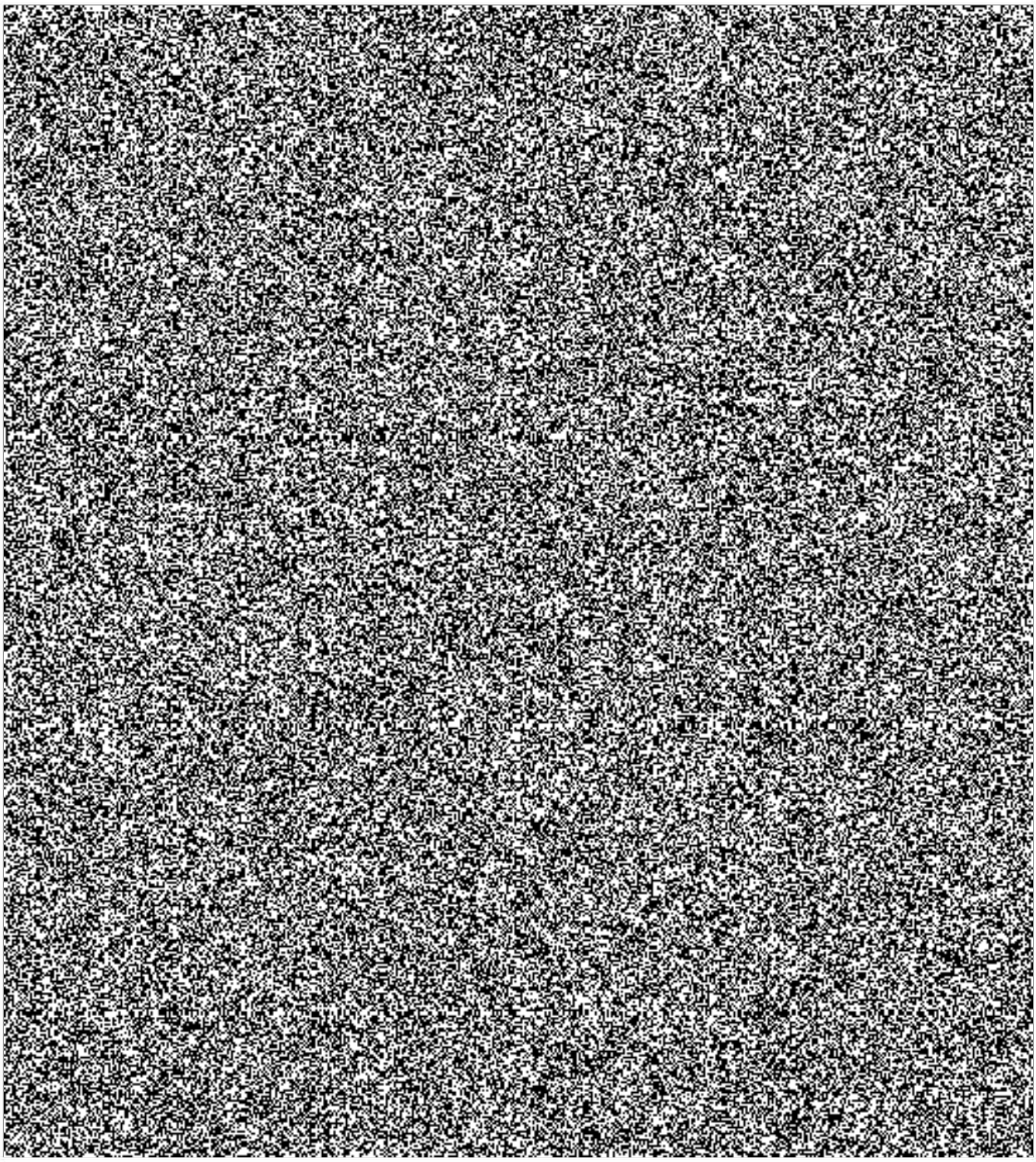




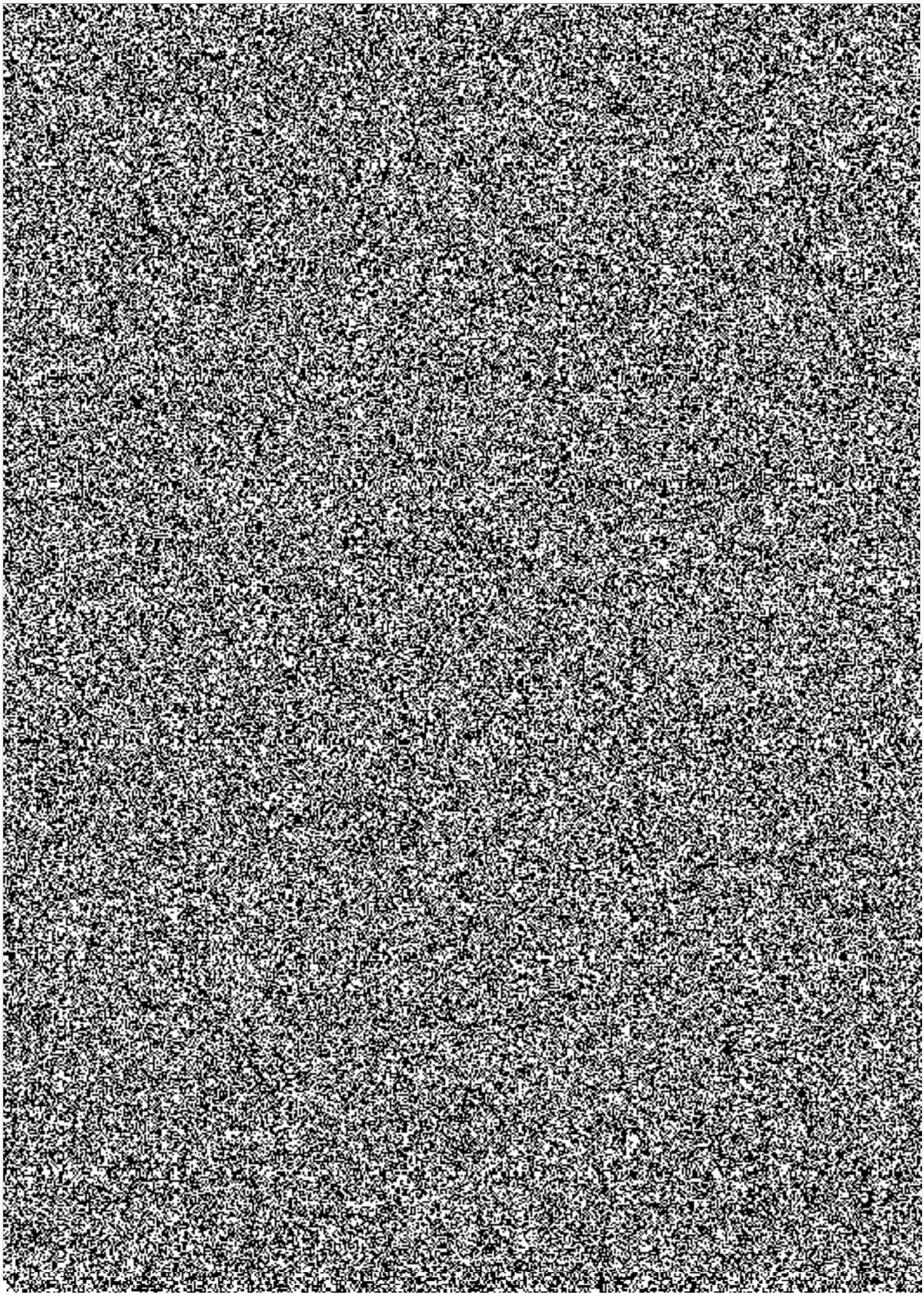


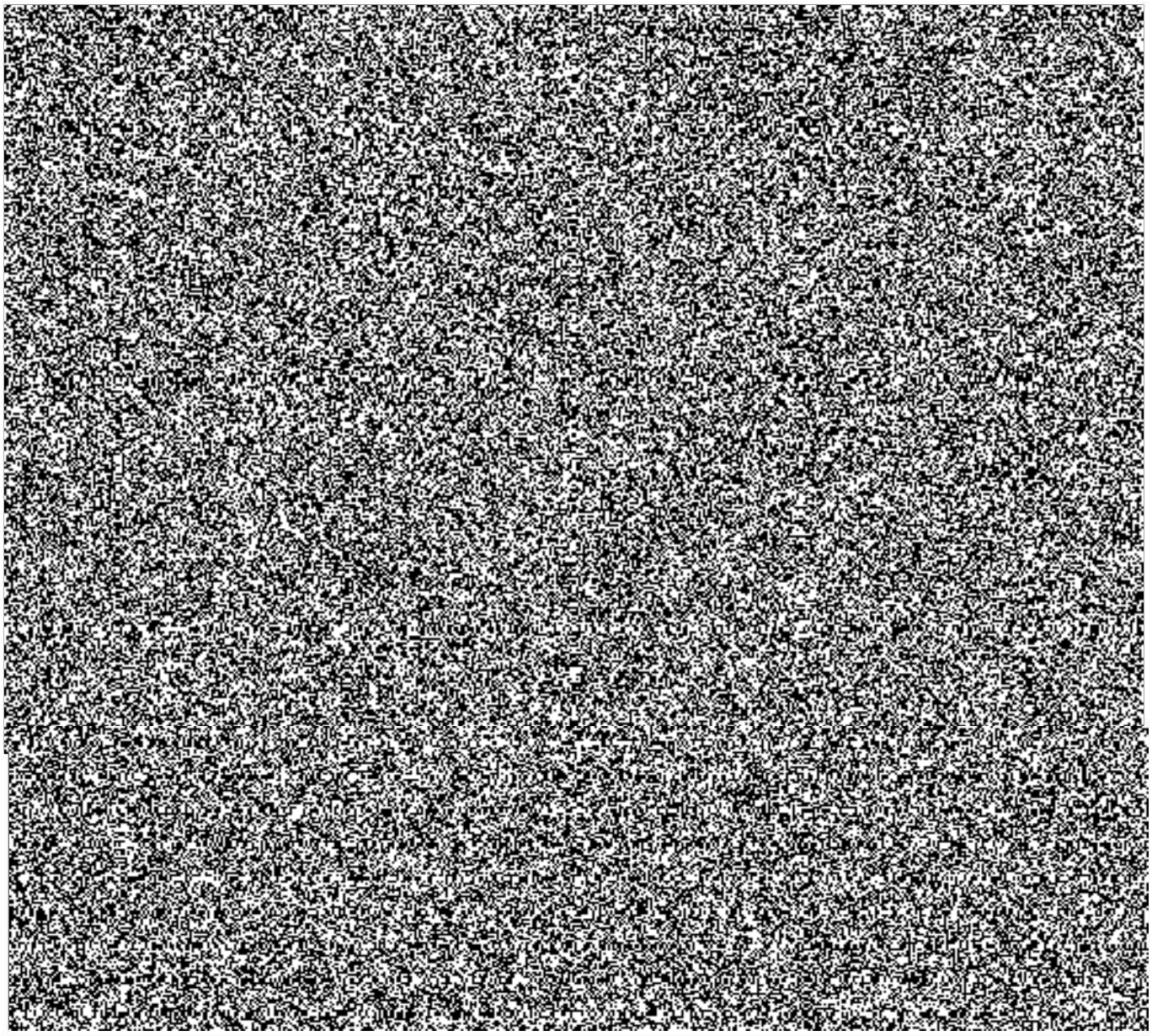
[3] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)



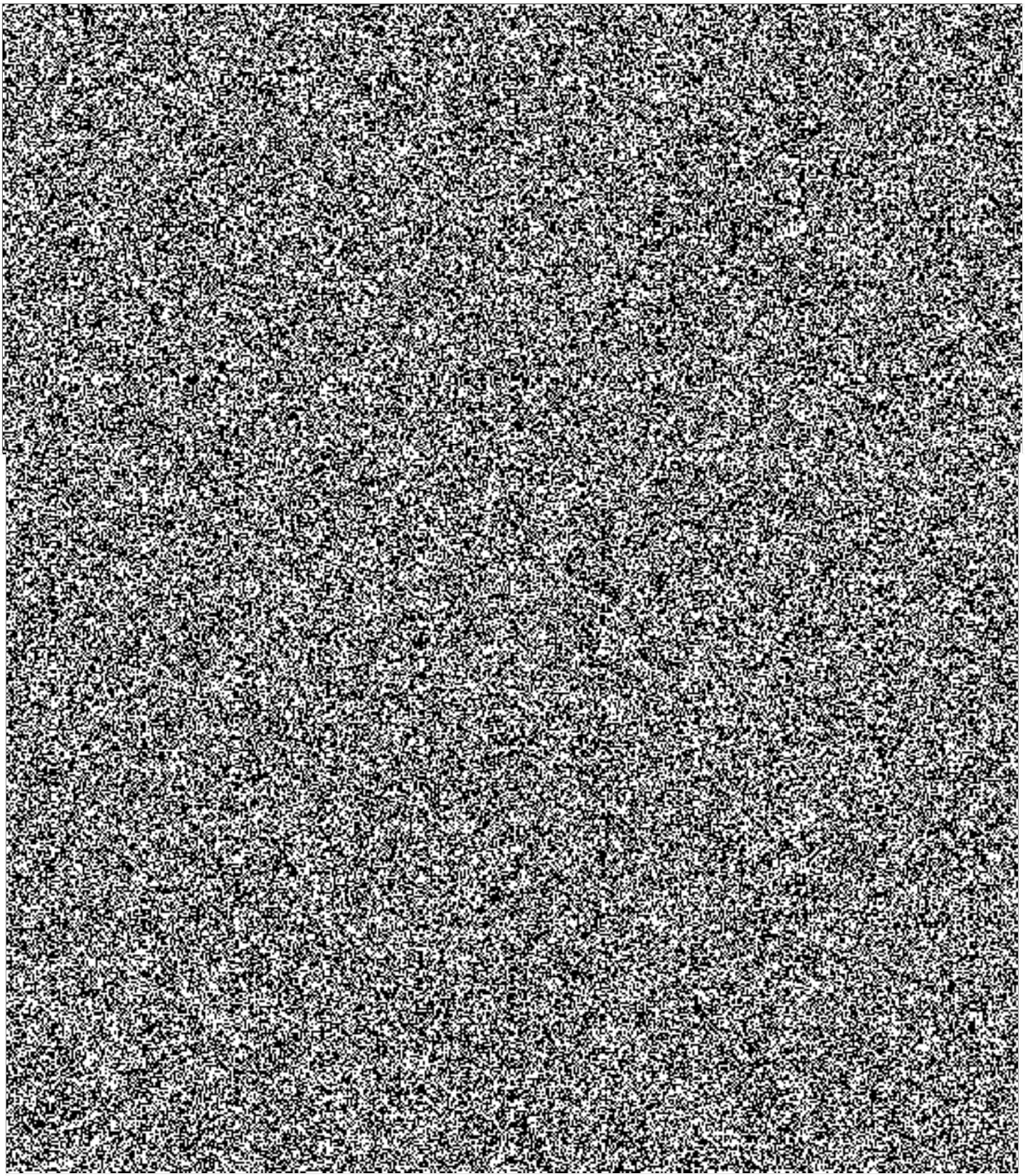


[4] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

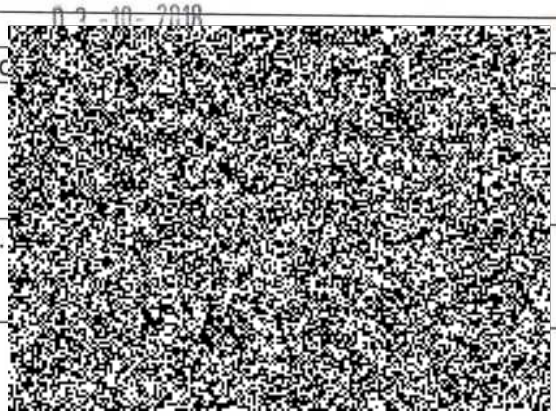




[5] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)



Datum podpisu	0 2 -10- 2019
Místo podpisu	Brno
Otisk razítka uchazeče	
Jméno, příjmení a podpis uchazeče, resp. statutárního zástupce uchazeče	doc.



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