MVCRX04HL9NJ
prvotní identifikátor

Smlouva

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

„Adaptivní ochrana před DDoS útoky“

VI20192022137

uzavřená mezi smluvními stranami

Česká republika – Ministerstvo vnitra

a

CESNET, zájmové sdružení právnických osob

Č.j.MV-56070-5/OBVV-2019
Počet stran: 15
Přílohy: 3

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.
[redacted]
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

CESNET, zájmové sdružení právnických osob

se sídlem: Zikova 1903/4, 160 00 Praha 6
IČ: 63839172
DIČ: CZ63839172
statutární zástupce: Ing. Jan Gruntorád, CSc., ředitel sdružení
zájmové sdružení právnických osob, zapsáno ve spolkovém rejstříku vedeném u Městského soudu v Praze oddíl L, vložka 58848
[redacted]
adresa pro doručování: sídlo příjemce

kontaktní osoba: manažer projektu
[redacted]

(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 **„Adaptivní ochrana před DDoS útoky“** a identifikačním kódem **„VI20192022137**“ 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 průmyslový výzkum zaměřený na výzkum a vývoj v oblasti pokročilé obrany před útoky na dostupnost služeb, tzv. DDoS útoky. Rychlá adaptace na měnící se vektor útoku, automatizace postupů uživatele, využívání externích informačních zdrojů jsou velmi důležité schopnosti, které nabízí možnosti zlepšení současného stavu a budou v rámci projektu rozvíjeny, aby byla docílena efektivní reakce na útok nejen z pohledu přesnosti, ale i z pohledu snížení personální a finanční náročnosti.

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

Článek 2
Administrátor Projektu

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

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

Článek 3
Manažer Projektu

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

Článek 4
Hlavní řešitel Projektu

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

Článek 5
Doba řešení Projektu

1) Příjemce je povinen zahájit řešení Projektu dne 1. 9. 2019.

2) Příjemce je povinen ukončit řešení Projektu nejpozději ke dni 31. 8. 2022.

Článek 6
Uznané náklady, výše podpory a platební podmínky

1) Uznané náklady[1] na řešení Projektu se stanovují ve výši **19 845 815,- Kč** (slovy:devatenáctmilionůosmsetčtyřicetpěttisícosmsetpatnáctkorunčeských).
Tato částka zahrnuje podporu ve výši **19 845 815,- Kč** (slovy:devatenáctmilionůosmsetčtyřicetpěttisícosmsetpatnáctkorunčeských), která je poskytovaná formou dotace z rozpočtové kapitoly Ministerstva vnitra.

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

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

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

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

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

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

Článek 7
Změny Rozpočtu

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

   a) zdůvodněná změna celkové výše rozpočtu příjemce,

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

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

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

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

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

tohoto článku, podléhá každá další změna rozpočtu předchozímu souhlasu poskytovatele.

4) Pokud příjemce neobdrží stanovisko poskytovatele do 15 pracovních dnů ode dne odeslání informace o podstatné změně rozpočtu dle odstavce 1 tohoto článku nebo o změně dle odstavce 3 tohoto článku, považuje se změna rozpočtu za schválenou poskytovatelem, pokud není stanoveno jinak. Poskytovatel může lhůtu prodloužit o 15 pracovních dnů; je však povinen o prodloužení lhůty příjemce písemně informovat.
5) V případě změny celkové výše rozpočtu, při které dochází k navýšení podpory podle Článku 7 odst. 1 Smlouvy lze tuto změnu realizovat pouze uzavřením dodatku k této Smlouvě.
6) Žádosti příjemce o předchozí souhlas poskytovatele podle odstavce 1 a 3 tohoto článku i oznámení změny rozpočtu podle odstavce 2 tohoto článku předává příjemce prostřednictvím formuláře zveřejněného na webových stránkách Ministerstva vnitra včetně nové verze rozpočtu a komentáře popisujícího jeho změny.

Článek 8
Intenzita podpory

1) Intenzitou podpory se rozumí v procentech vyjádřený podíl výše podpory k uznaným nákladům příjemce v daném roce řešení Projektu.
2) Maximální povolená výše intenzity podpory činí 100 %.

Článek 9
Subdodávky

1) V rámci řešení Projektu nebudou realizovány subdodávky.
2) Pokud se v průběhu řešení Projektu vyskytne potřeba realizace subdodávky, postupuje příjemce podle zákona č. 134/2016 Sb. o zadávání veřejných zakázek (dále jen „zákon č. 134/2016 Sb.“).
3) Subdodávky je příjemce povinen pořizovat za tržní ceny (tj. cena v místě a čase obvyklá). Toto je příjemce povinen poskytovateli doložit.
4) Subdodávky na výzkum nebo experimentální vývoj mohou být realizovány maximálně do výše 20 % celkových uznaných nákladů Projektu.
5) Nové subdodávky musí být předem odsouhlaseny poskytovatelem a upraveny písemným dodatkem ke Smlouvě.
6) Je-li subdodavatelem veřejně financovaná výzkumná organizace, mohou být předmětem subdodávek pouze výzkum nebo experimentální vývoj za těchto podmínek:
   a) výzkumná organizace poskytuje danou výzkumnou službu nebo provádí smluvní výzkum za tržní cenu nebo
   b) nelze-li určit tržní cenu, výzkumná organizace poskytne danou výzkumnou službu nebo provede smluvní výzkum za cenu, která zahrnuje plné náklady a přiměřený zisk.
7) Je-li příjemce výzkumnou organizací, může pořizovat subdodávky pouze od jiné výzkumné organizace.
8) Při pořízení subdodávek v rozporu s tímto článkem bude postupováno dle Článku 20 Smlouvy.

Článek 10
Vedení účetnictví o uznaných nákladech Projektu

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

2) Nezpůsobilými náklady projektu jsou zejména:
   - zisk,
   - daň z přidané hodnoty (u příjemců, kteří jsou plátci této daně a kteří uplatňují její odpočet nebo odpočet její poměrné části)[2],
   - jiné daně (silniční daň, daň z nemovitosti, daň darovací, dědická, apod.),
   - náklady na marketing, prodej a distribuci výrobků,
   - úroky z dluhů,
   - náklady na finanční pronájem a pronájem s následnou koupí (např. leasing, aj.),
   - manka a škody,
   - náklady na pohoštění, dary a reprezentaci,
   - náklady na vydání periodických publikací, učebnic a skript,
   - náklady/výdaje na pořízení budov a pozemků,
   - opravy nebo údržba místností, stavby, rekonstrukce budov nebo místností, nábytek či zařízení, která nejsou pevnou součástí místností, a další náklady, které bezprostředně nesouvisejí s předmětem řešení projektu,
   - správní poplatky,
   - výdaje související s likvidací příjemce, nedobytné pohledávky,
   - platby příspěvků do soukromých penzijních fondů,
   - peněžitá pomoc v mateřství,
   - ostatní sociální výdaje na zaměstnance, které nejsou zaměstnavatelé povinni odvádět dle zvláštních předpisů (např. dary k životním jubileím, příspěvky na rekreaci, příspěvky na penzijní připojištění, životní pojištění apod.),
   - odstupné,
   - nájemné, kdy příjemce je vlastníkem nemovitosti nebo ji užívá zdarma,
   - výdaje na školení a vzdělávání personálu (pokud se nejedná o odborné akce přímo související s řešením projektu).

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

4) Příjemce účtuje doplňkové náklady související s Projektem **metodou vykazování doplňkových nákladů (AC – Additional Costs).** Výše celkových doplňkových nákladů příjemce Projektu účtovaných metodou kalkulace dodatečných nákladů (AC - Additional Costs) nesmí po celou dobu řešení Projektu překročit 10 % celkových uznaných přímých nákladů Projektu příjemce.

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  (při převodu finančních

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

prostředků příjemce uvede do Zprávy pro příjemce: VRATKA-NESPOTŘEBOVANÉ PROSTŘEDKY, kód projektu, svůj název).

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

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

8) V případě, že příjemci zůstanou nevyužité finanční prostředky daného kalendářního roku, s výjimkou postupu podle odstavce 5 až 7 tohoto článku, je povinen tyto prostředky poskytovateli vrátit do 15. února následujícího roku převedením na bankovní účet poskytovatele číslo [redacted] (při převodu finančních prostředků příjemce uvede do Zprávy pro příjemce: VRATKA-NEVYUŽITÉ PROSTŘEDKY, kód projektu, svůj název). Tyto prostředky budou poskytovatelem odvedeny do státního rozpočtu.

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

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

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

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

13) Pokud příjemce uplatňuje rozdílný hospodářský rok, provádí vyúčtování nákladů na Projekt a poskytnuté podpory k 31. prosinci daného kalendářního roku a při uzávěrce

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

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 Článku 7 odst. 1 písm. d) Smlouvy. Oznámení o změně řešitelského týmu musí obsahovat formulář čerpání osobních nákladů, který je s formulářem pro personální změnu zveřejněn na webových stránkách Ministerstva vnitra. Při postupu příjemce v rozporu s tímto ustanovením, bude postupováno dle ustanovení Článku 20 odst. 3 Smlouvy.

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

9) Příjemce je povinen každou zahraniční pracovní cestu, jejíž náklady přesáhnou 100 000,- Kč, předložit s předstihem nejméně 30 kalendářních dnů před zahájením zahraniční pracovní cesty se zdůvodněním poskytovateli ke schválení. Nejpozději do 30

kalendářních dnů po ukončení cesty je příjemce povinen předložit poskytovateli podrobnou zprávu o jejím průběhu a výsledcích ve vztahu k řešení Projektu.

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

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

Článek 12
Zprávy

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

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

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

4) Závěrečnou zprávu z řešení Projektu předloží příjemce do 30 kalendářních dnů ode dne ukončení řešení Projektu uvedeného v Článku 5 Smlouvy. Závěrečná zpráva z řešení Projektu zahrnuje zejména informaci o dosažených cílech, výsledcích, způsobu jejich využití a výstupech Projektu. Součástí závěrečné zprávy je vyúčtování nákladů na Projekt a poskytnuté podpory za celé období řešení Projektu ve struktuře Rozpočtu. Přílohou závěrečné zprávy jsou materiály, kterými příjemce dokládá, že výsledky existují a jejich funkčnost, jako jsou například technická dokumentace, rozhodnutí nebo certifikace výsledků.

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

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

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

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

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

Článek 13
Kontroly

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

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

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

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

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

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

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

Článek 14
Nákup a vlastnictví majetku pořízeného pro řešení Projektu

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

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

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

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

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

Článek 15
Práva k výsledkům Projektu a jejich využití

1) Práva k výsledkům Projektu patří příjemci.

2) Při využití výsledků Projektu je příjemce povinen postupovat v souladu s ustanovením § 16 odst. 4 zákona č. 130/2002 Sb., 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,
   c) Příloha č. 3 – Upravený rozpočet.

7) Smlouva se vyhotovuje ve dvou stejnopisech, z nichž poskytovatel i příjemce obdrží po jejich podpisu jedno vyhotovení.

8) Smluvní strany prohlašují a podpisem Smlouvy stvrzují, že jimi uvedené údaje, na jejichž základě je uzavřena Smlouva a poskytnuta podpora poskytovatelem, jsou správné, úplné a pravdivé.

9) Smluvní strany prohlašují, že si tuto Smlouvu přečetly, s jejím obsahem souhlasí a že byla sepsána na základě jejich pravé a svobodné vůle, a na důkaz toho připojují své podpisy.

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

Článek 25
Platnost a účinnost Smlouvy

1) Smlouva se uzavírá na dobu určitou a nabývá platnosti dnem podpisu obou smluvních stran a účinnosti od 1. 7. 2019, pokud právní předpis nestanoví jinak.

2) Smlouva je ukončena dnem 27. 2. 2023.

3) Ukončení Smlouvy před datem uvedeným v odstavci 2 tohoto článku je upraveno v ustanovení Článku 21 odst. 4 písm. b) a c) Smlouvy.

Za poskytovatele:

JUDr. Petr Novák, Ph.D.

V Praze dne:

Za příjemce: Ing. Jan Gruntorád, CSc.

Digitálně podepsal Ing. Jan Gruntorád, CSc.
Datum: 2019.06.07 10:16:40 +02'00'

Ing. Jan Gruntorád, CSc.

V dne:

Elektronický podpis - 7.6.2019
Certifikát autora podpisu :
Jméno : JUDr. Petr Novák, Ph.D.
Vydal : PostSignum Qualified C...
Platnost do : 30.4.2020 10:17:21-000 +02:00

Adaptivní ochrana před DDoS útoky

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

Uchazeč: **CESNET, zájmové sdružení právnických osob**

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
2e) Rozvoj ICT, telematiky a kybernetické ochrany 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

Adaptivní ochrana před DDoS útoky

2.2 Název projektu anglicky

Název projektu anglicky

Adaptive protection against DDoS attacks

2.3 Anotace projektu

Anotace projektu

Projekt je zaměřen na výzkum a vývoj v oblasti pokročilé obrany před útoky na dostupnost služeb, tzv. DDoS útoky. Rychlá adaptace na měnící se vektor útoku, automatizace postupů uživatele, využívání externích informačních zdrojů jsou velmi důležité schopnosti, které nabízí možnosti zlepšení současného stavu a budou v rámci projektu rozvíjeny, aby byla docílena efektivní reakce na útok nejen z pohledu přesnosti, ale i z pohledu snížení personální a finanční náročnosti.

2.4 Anotace projektu anglicky

Anotace projektu anglicky

The project undertakes research into advanced protection against distributed denial of service attacks. Rapid adaptation to an evolving vector of attack, automation of user tasks, exploitation of external information resources are key capabilities that offer scope for improvement over the current situation. The project will address these topics to achieve an effective response to the attack from the accuracy as well as from human-resources and financial perspective.

2.5 Kategorie činnosti

Kategorie činnosti

průmyslový výzkum

2.6 Předpokládané datum zahájení projektu

Předpokládané datum zahájení projektu

01.09.2019

2.7 Datum ukončení projektu

Datum ukončení projektu

31.08.2022

2.8 Projekt má více uchazečů

Projekt má více uchazečů

NE

2.9 Klíčová slova

Klíčová slova

kybernetika;útok;ochrana;mitigace

2.10 Klíčová slova anglicky

Klíčová slova anglicky

cybernetic;attack;protection;mitigation

3. Identifikace uchazeče

3.1 Název uchazeče

Název uchazeče
CESNET, zájmové sdružení právnických osob

3.2 Právní forma

Právní forma
ZSP - zájmové sdružení právnických osob (§ 20f až 21 občanského zákoníku), občanské sdružení, …

3.3 IČ

IČ
63839172

3.4 DIČ

DIČ
CZ63839172

3.5 Sídlo uchazeče

Státní příslušnost			
CZ - Česká republika			
Kraj	Obec		
Praha	Praha 6		
Ulice	Č. popisné	Č. orientační	PSČ
Zikova	1903	4	160 00
Telefon	E-mail		
+420224352994	info@cesnet.cz		
Web stránka			
www.cesnet.cz			

3.7 Statutární zástupce/zástupci uchazeče

Titul před jménem	Jméno	Příjmení	Titul za jménem
Ing.	Jan	Gruntorád	CSc.
Pracovní pozice osoby na pracovišti			
ředitel sdružení			
Telefon	Fax	E-mail	
+420224352975		jan.gruntorad@cesnet.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

CESNET má s výzkumem a vývojem v oblasti bezpečnosti mnohaleté zkušenosti dané potřebou zajistit bezproblémový chod a rozvoj e-infrastruktury CESNET. Projekty, výzkumné záměry a veřejné zakázky, které CESNET řeší v posledních letech, daly vzniknout řadě špičkových technologií, detekčních nástrojů a systémů, které monitorují stav sítě CESNET2 a její perimetr, odhalují anomálie v síťovém provozu a poskytují správcům podporu a informace nutné k nalezení zdroje problému, jeho úspěšné eliminaci a k prevenci. Některé z těchto technologií jsou jako služba poskytovány i mimo e-infrastrukturu CESNET, některé výsledky byly úspěšně komercializovány (rodina akceleračních karet COMBO, hardwarově akcelerovaná sonda FlowMon) a bylo uděleno několik patentů (např. americké patenty US8923300, US8582967, US8630035).

V roce 2003 byl sdružením CESNET založen tým CESNET-CERTS, první bezpečnostní CSIRT tým v ČR. CESNET-CERTS byl v roce 2004 přijat světovou komunitou a v lednu 2008 dosáhl akreditace u úřadu Trusted Introducer. V letech 2007 – 2010 v rámci plnění grantu Ministerstva vnitra ČR s názvem Kybernetické hrozby z hlediska bezpečnostních zájmů ČR (VD20072010B01) vybudoval CESNET modelové pracoviště CSIRT.CZ, které v prosinci 2010 MV ČR prohlásilo za Národní CSIRT ČR.

CESNET je členem řady národních i mezinárodních organizací, platforem a projektů zabývající se kyberbezpečností – TF-CSIRT, ENISA, EGI, Pracovní skupina CSIRT.CZ, NIX.CZ, CZ.NIC, Géant, Internet 2 a je zakládajícím členem projektu Fenix.

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

V současnosti se CESNET výzkumem a vývojem v oblasti bezpečnosti zabývá v projektech: VI20162019029 - Sdílení a analýza bezpečnostních událostí v ČR, VI20172020079 - Zabezpečená brána pro internet věcí, VI20172020064 - Adaptivní řízení sběru a analýzy dat ve vysokorychlostních sítích.

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

Identifikátor	Název
TA03010561	Distribuovaný systém pro komplexní monitorování vysokorychlostních sítí

Oblast výzkumu a vývoje

AP-Aplikovaný výzkum progresivní technologie v oblasti monitoringu 40/100G Ethernetu se zaměřením na vývoj měřicích hardwarově akcelerovaných sond a software pro sběr dat z těchto sond, a jejich centralizované ukládání, vizualizace a vyhodnocení.

Výsledky evidované v RIV

- Software: IPFIX collector (2013) RIV/63839172:_____/13:10130228
- Článek ve sborníku: Memory Efficient IP Lookup in 100 Gbps Networks. 23rd International Conference on Field Programmable Logic and Applications (FPL'13) RIV/63839172:_____/13:10130212
- Funkční vzorek: Sada firmware modulů pro práci se 100 Gb/s Ethernetem RIV/63839172:_____/13:10130230

Identifikátor	Název
MSM6383917201	Optická síť národního výzkumu a její nové aplikace

Oblast výzkumu a vývoje

AP-Aplikovaný výzkum, IF-Infrastruktura VaV v oblasti počítačových sítí a vědecko-výzkumných aplikací, jejíž integrální součástí je vývoj, testování a implementace nových vyspělých přenosových a síťových technologií, protokolů, nástrojů a služeb.

Výsledky evidované v RIV

- USA patent US8582967B2: Device for multicast of optical signals in the internet and other networks RIV/63839172:_____/13:10130246
- CZ patent 300812: Modulární programovatelná platforma pro vysokorychlostní hardwarové zpracování paketů RIV/63839172:_____/09:10130350
- Prototyp: NetCOPE Development Platform RIV/63839172:_____/09:00006821

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

Oblast výzkumu a vývoje

Cílem projektu je vyvinout inovativní technologické řešení pro zpracování a analýzu extrémního objemu specifických síťových údajů o IP tocích. Řešení bude umožňovat sběr a uchování dat na různé úrovni detailu a následně jejich zpracování a analýzu.

Výsledky evidované v RIV

RIV/00216224:14610/17:00094410 - Systém pro sběr, uchování a analýzu síťových dat velkého rozsahu (2017)
RIV/27730450:_____/15:#0000011 - Software pro cloudové zpracování síťových dat o IP tocích (2015)
RIV/27730450:_____/16:N0000001 - Software pro masivně paralelní zpracování velkého objemu síťových dat na dynamické úrovni detailu (2016)

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

Identifikátor	Název
Kodek JPEG2000	Kodek JPEG 2000 pro grafické procesory GPU

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

Komercializace v oblasti GPU akcelerovaného zpracování videa. Komercializace proběhla modelem spin-offu, přičemž vazba na sdružení je vyjádřena převodem výkonu autorských práv za úplatu na nově vzniklou společnost Comprimato Systems s.r.o.

Identifikátor	Název
COMBO6X	Prototyp karty COMBO6X

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

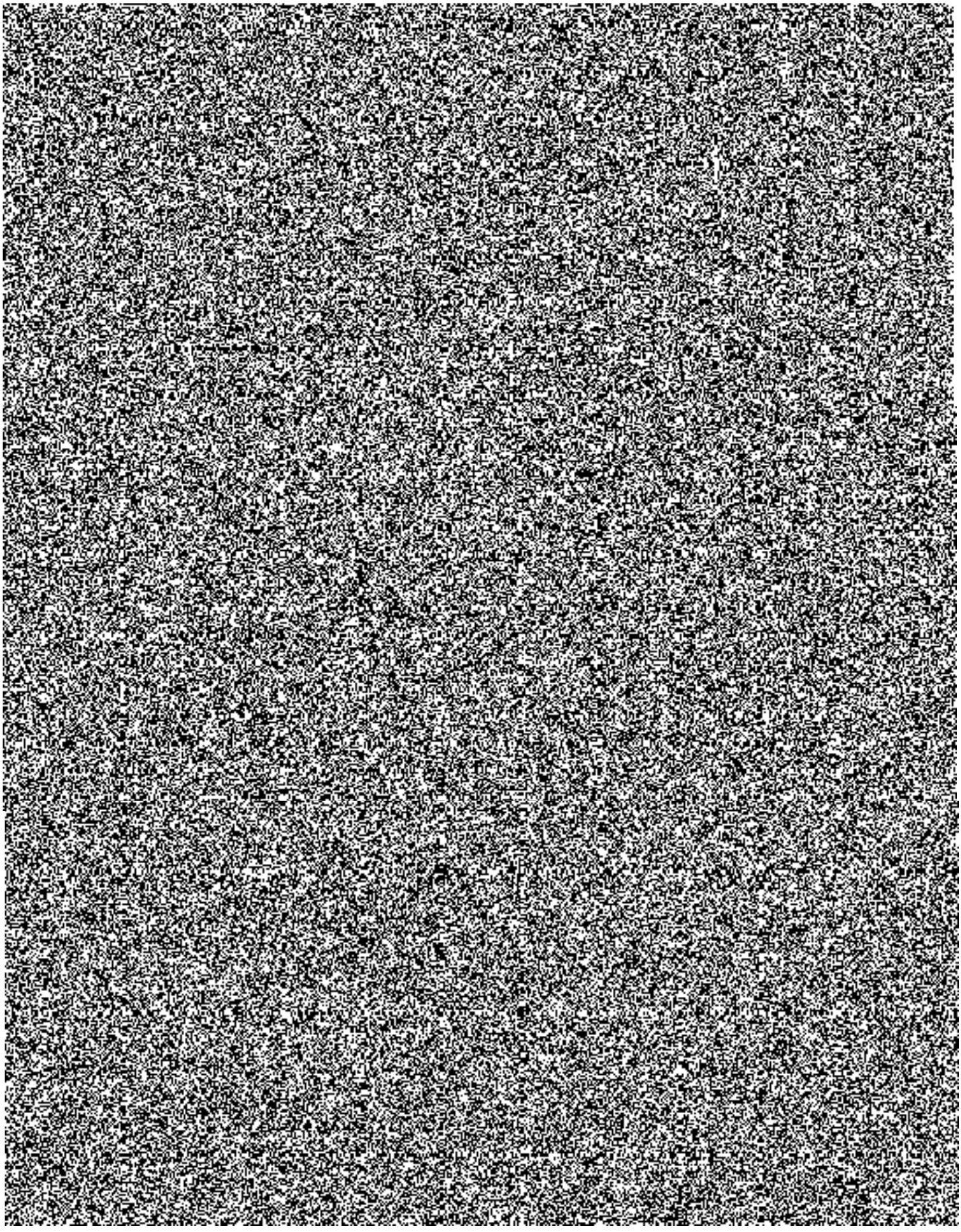
Tento prototyp vytvořený v roce 2005 byl počátkem vývoje celé rodiny akceleračních karet rodiny COMBO a s nimi souvisejících výsledků. Patří mezi ně například prototypy COMBOL-GPS, COMBOI-10G4TXT, COMBOI-100G1 nebo užitný vzor 19987. Dohromady tvoří hardware, firmware a software pro realizaci konfigurovatelných zařízení na monitorování vysokorychlostních sítí. Licencování rodiny produktů COMBO společnosti INVEA-TECH probíhá od roku 2007. Společnost INVEA-TECH (později FlowMon Networks a Netcope Technologies) byla založena jako spin-off za účelem dalšího rozvoje a komerčního uplatnění karet COMBO, jehož výsledkem je například aktuálně komerčně úspěšná karta COMBO-CG. Výsledek COMBO-CG byl oceněn v soutěži Česká hlava 2016 cenou Ministerstva průmyslu a obchodu.

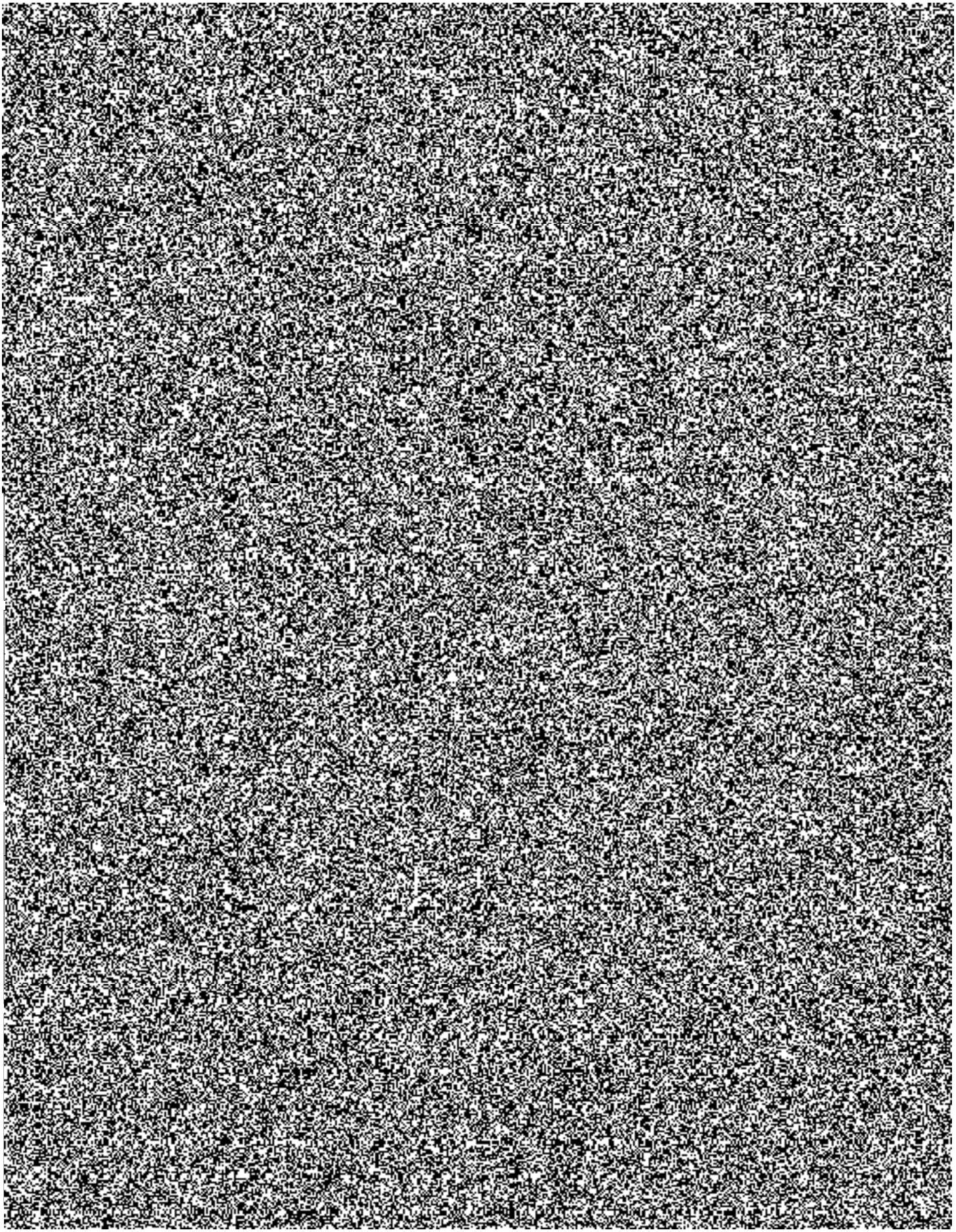
Identifikátor	Název
303954	Zapojení pro rychlou analýzu hlaviček paketů přenášených po datové sběrnici

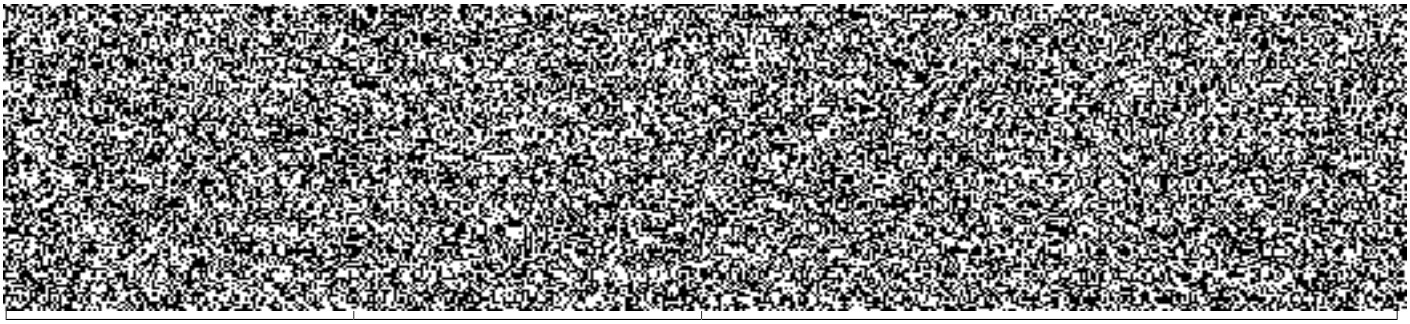
Kým a po jakou dobu komerčně využíván, případně číslo patentu nebo jiného typu právní ochrany

Od svého vytvoření v roce 2012 představuje tento výsledek důležitou součást firmwarů pro rodinu produktů COMBO. Úřad průmyslového vlastnictví ČR mu v květnu 2013 udělil patentovou listinu číslo 303954. Úřad pro patenty a ochranné známky USA mu v prosinci 2014 udělil patentovou listinu číslo 8923300. V rámci smlouvy o transferu technologií byl výsledek licencován společnosti INVEA-TECH a.s. (později Netcope Technologies a.s.), která jej integrovala do svých hardwarově akcelerovaných řešení pro monitorování vysokorychlostních sítí.

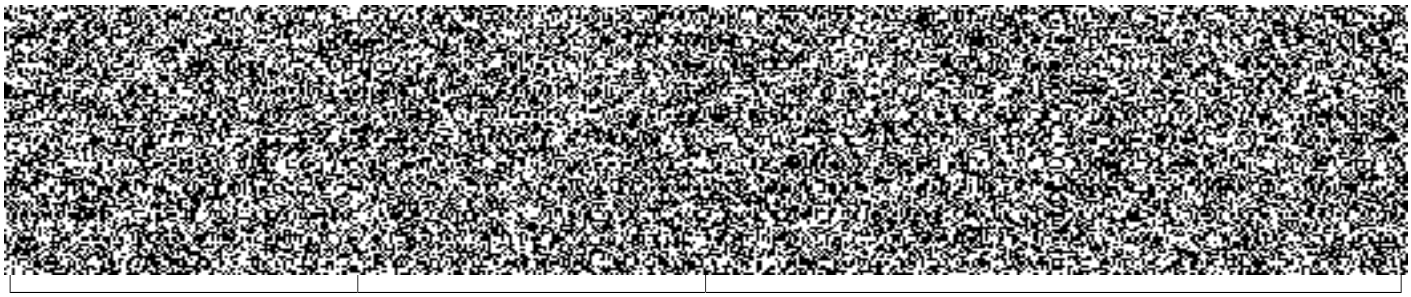
3.12 Řešitelský tým projektu



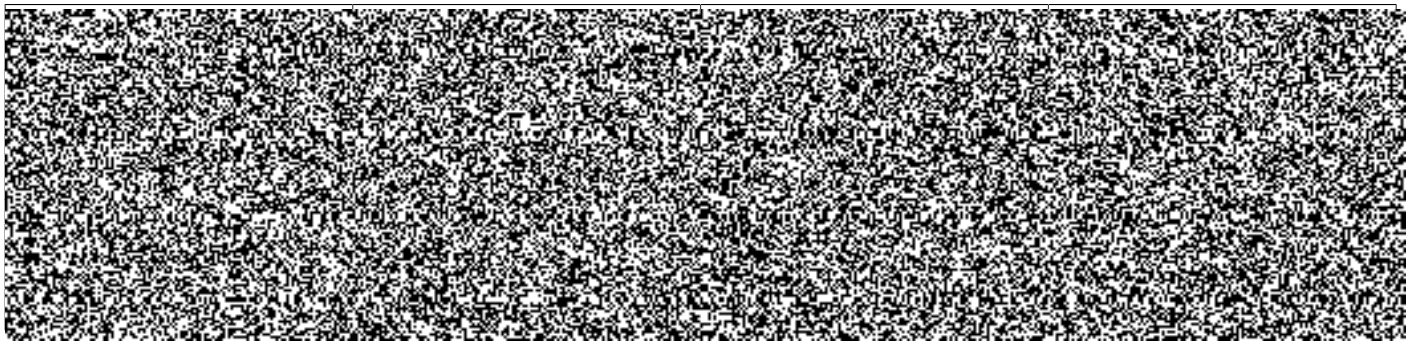




3.13 Manažer projektu



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

Útoky typu DDoS, tj. odepření služby, stále rostou na intenzitě a sofistikovanosti a představují tak neustálou a rostoucí hrozbu pro národní kybernetický prostor. Hlavním cílem projektu je proto vyvinout a ověřit adaptivní a otevřený systém pro čištění síťového provozu na vysokých rychlostech (100 Gb/s a vyšší). Tento systém bude realizovat široké množství mitigačních procedur, které bude schopen adaptivně aplikovat dle vývoje útoku. Tím se bude významně odlišovat od současných řešení, která autonomně nedokáží dostatečně do hloubky analyzovat útok, rozpoznat klíčové vlastnosti útoku a aplikovat adekvátní postupy a naopak vyžadují značnou expertní znalost operátora a to nejen znalost daného síťového provozu a útoku, ale i detailní znalost daného zařízení pro mitigaci. Za účelem vyšší míry autonomie bude systém sledovat široké množství údajů o provozu, vytvářet modely, simulovat dopady mitigace na provoz, aplikovat reputační informace a k tomu využívat vhodných algoritmů strojového učení tak, aby byla reakce na útok maximálně efektivní ať už automatizovanými prostředky či rozhodnutím experta s maximální asistencí systému. Otevřenost zamýšleného systému bude spočívat nejen v dostupnosti zdrojového kódu např. z důvodu bezpečnostního auditu, ale i v možnosti modulárně celý systém rozvíjet tak, aby bylo možné řešení využívat k mitigaci aktuálních útoků i po skončení projektu. Snadné využití systému bude dále podpořeno intuitivním uživatelským rozhraním a podporou různých způsobů zapojení systému do infrastruktury.

5.2 Dílčí cíle projektu

Dílčí cíle projektu

Adaptivní a semi- či plně automatizovaná reakce na útok. Dílčím cílem projektu je zkoumat a vyvíjet rozhodovací a asistenční algoritmy, které dokáží samy zvolit vhodné mitigační procedury a podporovat dodatečnými informacemi rozhodování uživatele systému. Rozhodování bude adaptivně přizpůsobovat konfiguraci, pravidla mitigace a výběr mitigačních technik nejen na základě detekovaného typu a velikosti útoku, ale i na základě efektivity čištění síťového provozu a na základě vytížení zdrojů systému čištění.

Flexibilní reakce na útok. Dílčím cílem projektu je implementovat širokou paletu mitigačních procedur od zdrojově velmi náročných a přesných, až po zdrojově méně náročné, ale více plošné, tedy i méně přesné. Široká paleta různorodých procedur umožní volit mezi těmito procedurami, čímž zajistí flexibilitu a určitou míru univerzálnosti vzhledem k budoucím útokům.

Vyšší míra spolupráce s externími systémy a podpora uživatele. Dílčím cílem projektu je systém čištění co nejvíce napojit na své okolí. Prvním směrem je napojení na externí zdroje dat, jako jsou například reputační databáze. Druhým směrem je interakce s uživatelem, kdy je potřeba jak usnadnit rozhodování uživatele (například modelování dopadů na síťový provoz při volbě určité mitigační procedury), tak i poskytnout rozhraní, na které je uživatel zvyklý, tedy nejen GUI, ale i rozhraní příkazové řádky, které zkušenému uživateli nabízí další flexibilitu při práci se systémem. Třetím směrem je pak podpora protokolů, které zjednoduší zapojení systému do existující infrastruktury.

V neposlední řadě je dílčím cílem projektu vybudovat experimentální laboratorní prostředí, ve kterém bude možné opakovaně měřit výkonové charakteristiky systému a validovat chování nejen jednotlivých algoritmů, ale i celého řešení.

5.3 Hlavní výsledky projektu

Kód	Druh výsledku	Počet
F	výsledky s právní ochranou – užitný vzor, průmyslový vzor	1
R	software	3

5.4 Vedlejší výsledky projektu

Kód	Druh výsledku	Počet
D	článek ve sborníku	2

5.5 Popis současného stavu problematiky řešené oblasti

Popis současného stavu problematiky řešené oblasti

DDoS útoky neustále rostou a vyvíjejí se z pohledu své intenzity i způsobu provedení. Již v roce 2016 dosáhly největší DDoS útoky intenzity 1 Tb/s. Útoky této intenzity jsou schopny zahltit služby i velkých poskytovatelů služeb s velmi dobrou konektivitou. K útokům jsou zneužívány kritické služby internetu (např. DNS), ale i rozsáhlé botnety (jako v případě botnetu Mirai). DDoS se postupně staly předmětem kyberkriminality na několika úrovních, od tzv. hacktivism přes konkurenční boj a vydírání, ovlivňování veřejného mínění, až po terorismus a jeden ze způsobů vedení války. Navíc v průběhu posledních pěti let došlo k profesionalizaci útočníků a k přesunu k tzv. DDoS průmyslu, kdy je možné si DDoS koupit jako službu (DDoS-for-hire).

Zatímco generovat DDoS útok je v dnešní době velmi snadné, mitigovat tyto útoky je náročné a to jak z pohledu expertní znalosti, tak i z pohledu finančních a dalších zdrojů. Z pohledu zdrojů přistupují poskytovatelé služeb k navýšení výpočetních zdrojů, které jsou dostupné pro službu, v ideálním případě i k distribuci služby do více lokalit, a k navýšení kapacity konektivity, což s sebou nese značné pořizovací a provozní náklady. Z pohledu expertní znalosti pak boj proti DDoS útokům vyžaduje analytické znalosti pro odhalení a identifikaci útoku a znalosti síťových prvků případně systému DDoS čištění tak, aby došlo alespoň ke zmírnění dopadu útoku.

Pro omezení DDoS útoku jsou používány i stávající směrovače, kdy pomocí techniky tzv. Remotely-Triggered Black Hole je provoz směřující na definovaný cílový prefix přesměrován či zahozen. Ve výsledku dojde sice k úspěšnému DDoS, neboť je zahozen veškerý provoz směřující na daný cíl, ale jsou typicky zachráněny ostatní služby sdílející s napadenou službou svou konektivitu. Na směrovačích podporujících BGPFlow-Spec lze navíc dynamicky vytvářet pravidla pro jemnější filtraci a omezení provozu, nicméně stále je třeba počítat s tím, že omezení bude typicky aplikováno jak na provoz útočníka, tak na provoz legitimních uživatelů služby.

Popis současného stavu problematiky řešené oblasti

Z tohoto důvodu jsou pro mitigaci nasazována dedikovaná zařízení, která jsou schopna analyzovat provoz více do hloubky a aplikovat složitější postupy mitigace. V oblasti mitigace DDoS útoků pomocí dedikovaného zařízení se pohybuje několik celosvětově významných výrobců zařízení, především Arbor, Radware a A10. Největší nevýhodou těchto zařízení jsou velmi vysoké náklady na jejich pořízení (typicky se cena pro řešení s propustností kolem 100Gb/s blíží milionu dolarů). Další nevýhodou je uzavřenost řešení. Tato uzavřenost se projeví ve chvíli, kdy zákazník potřebuje doplnit určitou funkcionalitu do produktu. Uzavřené řešení není možné rozšiřovat vlastním vývojem a je nutné čekat na termíny stanovené výrobcem na začlenění požadované funkcionality nebo přijmout extrémně vysoké náklady na začlenění dané funkcionality. V neposlední řadě je správná konfigurace zařízení klíčová a vyžaduje expertní znalost síťového provozu i samotného zařízení.

V případě provozování menších služeb je pořízení dedikovaného mitigačního zařízení značně neekonomické a provozovatelé služeb přechází na model ochrana jako služba. Mezi největší hráče patří Cloudflare, Akamai, tedy obecně provozovatelé velkých datových center, velcí operátoři a hostitelé samotných služeb. Typicky tito hráči zakoupí dedikované zařízení, takže nevýhody uzavřeného zařízení přetrvávají, plus další nevýhodu může představovat zpracování síťového provozu třetím subjektem (tedy problémy typu řešení odpovědnosti, možnost úniku informací apod.).

CESNET se na tento stav rozhodl reagovat vývojem vlastního řešení pro čištění provozu, kdy platforma tohoto řešení vychází z předchozích projektů zaměřených na pasivní monitoring síťového provozu. Platforma sestává ze specializované síťové karty s hardwarovou akcelerací zpracování síťového provozu na FPGA a výkonného serveru, ve kterém je karta standardně přes PCI-Express sběrnici připojena. Zařízení je experimentálně nasazeno v síti CESNET, kde bylo použito pro mitigaci jednoduchých amplifikačních DDoS útoků (DNS a memcache). Podobně jako u komerčních řešení je automatizace a expertní podpora značně omezena.

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

Přínosy a dopady projektu v oblasti bezpečnosti a cílů stanovených Programem

Stěžejní přínosy a dopady projektu a jeho výsledků očekáváme v několika oblastech - v oblasti bezpečnosti, ekonomiky, ve společenské oblasti a dále v oblasti vzdělávání a know-how.

Bezpečnostní přínosy a dopady

Nasazením vyvinutého řešení do síťové infrastruktury CESNET, NIX.CZ a NÚKIB dojde k pokrytí významných částí českého kyberprostoru. Výsledky projektu tak povedou ke zvýšení odolnosti národního kyberprostoru vůči DDoS útokům, konkrétně k ochraně samotné síťové infrastruktury a služeb na ní provozovaných.

Pro stávající bezpečnostní praxi bude nejvýznamnějším přínosem posun od žádného nebo velmi disruptivního způsobu obrany jako je ostrovní model či technika tzv. Remotely-Triggered Black Hole, k technikám, které jsou schopny selektivně odlišit provoz od útočníka od provozu od legitimního uživatele. Dalším významným přínosem budou pokročilé schopnosti řešení v oblasti adaptivity a automatizace, především usnadnění analýzy informací vztahujících se k útoku, navržení mitigačních postupů včetně simulace dopadů a zkrácení reakční doby od začátku útoku. Důležitým přínosem bude rovněž lepší schopnost interakce s uživatelem využívající informace od třetích stran, povelování zařízení přes různá konfigurační rozhraní a jednodušší nasazení do infrastruktury.

Ekonomické přínosy a dopady

Z ekonomického hlediska představují DDoS útoky asymetrickou hrozbu. Náklady na útok jsou o mnoho řádů nižší než náklady na ochranu proti útokům. Ekonomickým přínosem výsledků projektu bude řádově nižší cena než je cena současných řešení. Stejně tak nízké provozní náklady na provozování dosaženého výsledku přináší ekonomické výhody oproti řešením, která jsou založena na distribuci ochrany nebo na distribuci samotné chráněné služby na velké množství uzlů.

Projekt a jeho výsledky přispívají k profilaci ČR jakožto vysoce schopného hráče v oblasti počítačové a síťové bezpečnosti, která se již promítla v úspěšných start-up firmách jako např. AVG (akvizice Benson Oak Capitals), Cognitive Security (akvizice Cisco) či INVEA-TECH, respektive Flowmon Networks. Očekáváme, že vedlejším dopadem projektu bude pokračování tohoto trendu, kdy potenciální ekonomický přínos představuje možný vznik spin-off společnosti, která bude komercializovat výsledky projektu, převezme podporu výsledků od sdružení CESNET a bude výsledek dále rozvíjet a nabízet širokému okruhu zákazníků.

Společenské přínosy a dopady

Využívání online služeb jako jsou například email, online bankovnictví, telefonie, zprávy, videostreaming, webové služby a mnoho dalších, se stalo nedílnou součástí nejen pracovního, ale i soukromého aspektu lidského života. Dostupnost služeb využívající síťovou infrastrukturu je ale neustále ohrožena hrozbou útoků. Navíc u některých služeb je jejich dostupnost naprosto kritická a jejich výpadek může způsobit nejen materiální škody, ale také i škody na zdraví. Ze společenského hlediska je proto přínosem předkládaného projektu možnost selektivně blokovat nelegitimní síťový provoz, který způsobuje nedostupnost služeb. Zvýšení obranyschopnosti síťové infrastruktury tak následně povede k dalšímu rozvoji služeb, a to jak v komerčním, tak i ve veřejném sektoru.

Oblast vzdělávání a know-how

V neposlední řadě se na řešení projektu budou podílet také Ph.D. studenti, kteří tak získají možnost uplatnit výsledky svého výzkumu v reálné praxi a získat tak zpětnou vazbu a důležitou zkušenost pro svůj další profesní rozvoj. Procesem zapojování Ph.D studentů do praxe tak rovněž vzniká a rozšiřuje se vysoce kvalifikovaná pracovní síla, která je dále schopna inovovat a vyvíjet nová řešení. Dopadem projektu je tak uchovávání a rozvoj znalosti a know-how v České republice.

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

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

Realizace projektu bude využívat a navazovat na doposud vyvinutou experimentální verzi zařízení pro mitigaci amplifikačních útoků (vizte kapitolu Současný stav). Účelem projektu je dosažení hlavního a vedlejších cílů, tj. dosáhnout produkčního řešení s pokročilými parametry

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

překonávajícími stávající komerční řešení, které bude pilotně nasazené v infrastruktuře. Pro dosažení výše uvedených cílů byla realizace projektu naplánována jako kombinace vodopádového a inkrementálního modelu vývoje.

Z hlediska vodopádového modelu je projekt rozdělen do čtyř zastřešujících etap. První etapa je naplánována na konec roku 2019. Během této etapy dojde k dokumentaci aktuálního stavu existujícího zařízení, bude navrženo jeho rozšíření a stanovena specifikace tomu odpovídajícího testovacího prostředí. Do této etapy rovněž vstupuje detailní analýza potřeb plánovaných uživatelů, která dále rozšíří samotný návrh zařízení.

Druhá etapa naváže na první v roce 2020. V této etapě budou vyvinuta základní rozhraní a různé typy mitigačních procedur různé výpočetní a paměťové složitosti směřující do oblasti mitigace L3 až L7 DDoS útoků včetně možnosti za běhu měnit jejich parametry. Zároveň bude vytvořeno základní testovací prostředí. Paralelně k tomu budou zkoumány vhodné algoritmy směřující k podpoře uživatele, adaptivitě a automatizaci reakce.

Třetí etapa je naplánována na rok 2021. V třetí etapě proběhne kompletní cyklus vývoje vhodných algoritmů na základě výzkumné činnosti z předchozí etapy. Dále bude rozšířena a dokončena realizace jak rozhraní, tak testovacího prostředí.

Finální čtvrtá etapa má za cíl sestavit celý systém jako plně funkční celek na vhodné hardwarové platformě, která bude vybrána na začátku této etapy (minimálně předpokládáme novou generaci karet). Dále bude v rámci etapy dokončena vývojářská a uživatelská dokumentace. Rovněž bude zpracován plán nasazení do peeringového uzlu i do dalších typů zapojení tak, aby bylo podpořeno využití výsledků uživateli. Projekt bude završen validací funkčního vzorku pilotním nasazením v peeringovém uzlu.

V rámci inkrementálního vývoje budeme již od druhé etapy projektu provádět pravidelné sestavování, testování a vydávání výsledků jako balíků pro potřeby ověřování výsledků v laboratorním prostředí, sestavování experimentálních verzí zařízení pro potřeby zápůjček a získávání zpětné vazby od uživatelů. Výstupy se budou promítat do úprav detailních plánů činností vývojového týmu a přispějí k dosažení plánovaného osmého stupně vyspělosti dle přílohy 4.2.3.

V rámci výzkumných aktivit směřujících do oblasti podpory uživatele plánujeme využít poznatků v oblasti hybridních doporučujících systémů, které na základě obsahu historie uživatele a jeho podobnosti k ostatním uživatelům dokáží nabídnout relevantní obsah a ten vhodně vizualizovat. Tento obsah bude tvořen nejen doporučenými akcemi, ale i kontextem získaným z externích informačních zdrojů skrze strojová rozhraní. Z pohledu mitigačních technik a jejich automatizace a adaptivity reakce plánujeme aplikovat podobnostní vyhledávání, korelační a shlukovací algoritmy pro odvozování mitigačních a řídicích pravidel, a dále budeme zkoumat možnosti využití strojového učení za běhu, kdy trénovací sadou bude přímo zpětná vazba vyjadřující úspěšnost mitigace v simulovaném režimu či testovacím prostředí. Přestože deep learning metody se více uplatňují v oblasti rozpoznávání obrazu, budeme zkoumat možnosti využití deep learning, např. tzv. attention networks, pro modelování běžných a rozpoznání anomálních paketů a spojení z pohledu jejich obsahu.

5.8 Způsob a podíl zapojení jednotlivých účastníků do realizace projektu

Způsob a podíl zapojení jednotlivých účastníků do realizace projektu

Sdružení CESNET disponuje potřebným technickým vybavením, infrastrukturou, zkušenostmi s výzkumem a vývojem vysokorychlostních síťových zařízení a praxí s provozem a zajištěním kybernetické bezpečnosti ve velké síťové infrastruktuře.

Sdružení CESNET provozuje rozsáhlou síť CESNET2. K síti je aktuálně připojeno 26 českých vysokých škol, Akademie věd ČR a několik stovek dalších institucí, které se zabývají vědou, výzkumem a vývojem (například nemocnice, knihovny, výzkumné ústavy a další). Síť CESNET2 tak využívá přes 400 tisíc uživatelů z ČR. Síť CESNET2 je připojena do 9 zahraničních sítí a peeringových uzlů, mj. do českého peeringového centra NIX.CZ. Vzhledem k významu sítě je kladen velký důraz na monitoring a ochranu samotné infrastruktury, provozovaných služeb a připojených uživatelů. Sdružení CESNET je jedním ze zakládajících členů projektu Fenix (http://fe.nix.cz).

Řešení a koordinaci řešení zjištěných bezpečnostních incidentů v síti CESNET2 provádí bezpečnostní tým CESNET-CERTS. CESNET-CERTS byl založen již v roce 2004 jako první CERT v ČR a má dlouholeté zkušenosti v oblasti sběru, zpracování a reakce na bezpečnostní incidenty vztahujících se k síti CESNET2. CESNET je vzhledem ke své vysokorychlostní síti a připojeným organizacím, které provozují služby na výkonném hardware, zajímavým testovacím hřištěm pro DDoS útočníky. Pokud útok bude úspěšný vzhledem k organizaci zapojené v síti CESNET, pak bude velmi pravděpobobně úspěšný i v komerčním prostředí.

DDoS útoky řeší CESNET-CERTS ve spolupráci se síťovým operačním centrem. Síťoví administrátoři získali praktické zkušenosti s reakcí na DDoS útoky vedené proti síti sdružení CESNET. S postupně narůstající intenzitou a množstvím těchto útoků administrátoři zaváděli do sítě adekvátní opatření pro zmírnění jejich dopadů, a to od základních opatření typu Remotely-Trigged Black Hole, přes rate limiting, až po přesměrování potenciálně závadného provozu k experimentálně nasazenému zařízení pro mitigaci amplifikačních DDoS útoků (vizte kapitolu Současný stav).

Výzkumně-vývojové oddělení sdružení CESNET má bohaté zkušenosti s vývojem hardwarově akcelerovaných síťových prvků, především pak pasivních sond pro monitoring provozu. Stejně tak má zkušenosti s tzv. softwarovou akcelerací zpracování síťového provozu v počítači za pomoci knihovny DPDK.

Řešitelský tým je složen z vhodné kombinace členů s expertními znalostmi z výše uvedených domén a využije tak své znalosti a zkušenosti pro kvalitní řešení projektu a dosažení plánovaných výsledků.

Sdružení CESNET dále disponuje vybavením pro výzkum a vývoj hardwarově akcelerovaných síťových prvků. Součástí vybavení jsou vysokorychlostní generátory síťového provozu, které budou využity k ověření vlastností vyvíjených technologií. Jako další materiální zabezpečení projektu lze uvést vysokorychlostní generátor paketů Spirent Test Center, dále farmu překladových serverů a licence na vývojový software Xilinx Vivado, OrCAD PCB Designer a OrCAD Capture CIS.

5.9 Intenzita podpory

Intenzita podpory - CESNET, zájmové sdružení právnických osob

CESNET, z. s. p. o. byl na základě Rozhodnutí MŠMT ze dne 7. září 2017, č. j. MSMT-24091/2017-2 zapsán do seznamu výzkumných organizací, proto v souladu se zadávací dokumentací k vyhlášení třetí veřejné soutěže ve výzkumu, experimentálním vývoji a inovacích Programu bezpečnostního výzkumu ČR v letech 2015 až 2022, odst. 5.5.2 uplatňuje úhradu způsobilých/uznaných nákladů do výše 100% způsobilých/uznaných nákladů projektu.

5.10 Předpokládaní uživatelé výsledků

Předpokládaní uživatelé výsledků

Typickými uživateli výsledků budou provozovatelé scrubbingových center, peeringových uzlů či Internet eXchange Pointů (IXP), datových center, dále významní telekomunikační operátoři, silové složky a národní sítě pro výzkum a vzdělávání. Všichni tito uživatelé mají možnost lépe čelit DDoS útokům než samotné koncové sítě či služby, neboť disponují vysokou síťovou konektivitou, která je schopna často přenést samotný útok až do koncové sítě a ke koncové službě, kde způsobí samotné odepření služby.

Konkrétními plánovanými uživateli výsledků, kteří se budou pasivně podílet na projektu, jsou Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) a největší český IXP NIX.CZ.

NÚKIB plánuje realizovat projekt Národního scrubbing centra (NSC), kde bude možné přímo uplatnit výsledky tohoto projektu vzhledem k tomu, že potřeby NÚKIB budou reflektovány již v návrhu výsledků. Pokročilá funkcionalita usnadní práci s výsledkem a bude vyžadovat nižší zapojení lidských zdrojů. Automatizací a adaptivitou se přirozeně sníží reakční čas na útok a zvýší se efektivita, neboť výsledek připraví uživateli relevantní podklady a navrhne způsoby vhodné mitigace, které uživatel pouze schválí a ve vybraných ověřených případech povolí plnou automatizaci reakce. Další výhodou výsledků pro NÚKIB je rozšiřitelnost a nezávislost. K výsledkům budou dostupné zdrojové kódy a vývojářská dokumentace, což umožňuje snazší audit výsledku a zvyšuje uplatnitelnost z hlediska dlouhodobého použití. V případě, že by NÚKIB naplánoval využít služeb CESNET pro podporu a rozvoj v budoucnu, bude moci výsledek dále uzpůsobovat a rozvíjet i po skončení projektu vlastními silami, což poskytuje nezávislost na výrobci a jeho plánu rozvoje. Přestože konkrétní architektura NSC není nyní známa, díky standardním síťovým rozhraním a podpoře širokého množství konfiguračních, povelovacích a směrovacích protokolů bude nasazení do výsledného prostředí přímočaré, například napojení výsledku na systém sond, který je v rámci veřejné soutěže v současné době nasazován do síťové infrastruktury státní správy.

Sdružení NIX.CZ je největším neutrálním IXP v České republice a řadí se mezi deset největších IXP v Evropě. V současné době je do NIX.CZ připojeno více než 150 sítí s vlastním autonomním systémem. NIX.CZ již v minulosti řešil potřebu reagovat na útoky typu DDoS na základě útoků z března roku 2013. Jako obrana proti těmto DDoS útokům byla představena tzv. bezpečná VLAN projekt FENIX. Smyslem projektu je umožnit v případě DoS útoku dostupnost internetových služeb v rámci subjektů zapojených do této aktivity a odpojením se od zbylé části Internetu a tím zablokování DDoS útoku ale i dostupnosti mimo FENIX. To se ukazuje velkým omezením a existuje tak potřeba FENIX rozvinout o řešení, které nebude mít dopady na konektivitu a bude schopné selektivně dle přání individuálních členů čistit jim příslušný provoz. Těmto parametrům odpovídají výsledky předkládaného projektu. Z pohledu zapojení v peeringovém uzlu bude zařízení schopné napojit se na směrovací protokol BGP a na základě těchto informací správně přeposílat provoz do cílové destinace. Další výhodou výsledku je podpora multitenant, tj. oddělení uživatelů a možnost využití zařízení více organizacemi zároveň.

Sdružení CESNET bude rovněž uživatelem výsledků, neboť již během řešení projektu bude rozvíjet a aktualizovat zařízení experimentálně nasazené ve své síti. Pilotní nasazení v páteřní síti hraje významnou roli pro další evropské sítě národního výzkumu a vzdělávání. Tyto sítě jsou organizovány v rámci evropského projektu GÉANT, kde probíhá k výzkum a vývoj a rovněž dochází k výměně zkušeností mezi provozovateli národních sítí. Je tedy pravděpodobné, že nasazení v páteřní síti CESNET bude mít za následek adopci tohoto řešení i u ostatních národních sítí vědy a vzdělávání.

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 2019													
1.1 Analýza a návrh mitigačních metod Identifikace vhodných existujících metod mitigace, včetně analýzy metod v IDS a návrhu začlenění IDS do celého systému. Sběr a reflektování uživatelských požadavků jako rozšíření návrhu.	CESNET, zájmové sdružení právnických osob									x	x	x	x
1.2 Sběr požadavků na uživatelské a strojové rozhraní Definice požadavků na různá periferní rozhraní celého systému od UI a GUI přes strojová rozhraní pro předávání naučených profilů, předávání příkazů, export statistik, konfiguraci až po rozhraní vůči směrování v síti.	CESNET, zájmové sdružení právnických osob									x	x	x	x
1.3 Specifikace základního laboratorního prostředí pro validaci Specifikace způsobu zapojení testovacích zařízení, odvození a popis testovacích scénářů, návrh nástrojů pro experimenty, jako jsou např. sw pro generování provozu, sledování statistik automatizaci překladu a testování.	CESNET, zájmové sdružení právnických osob									x	x	x	x
Rok 2020													
2.1 Realizace mitigačních procedur Implementace a testování vybraných mitigačních procedur především pro heuristické metody pro blokování L3/L4 útoků.	CESNET, zájmové sdružení právnických osob	x	x	x	x	x	x	x	x	x	x	x	x
2.2 Realizace základního laboratorního prostředí	CESNET, zájmové sdružení právnických osob	x	x	x	x	x	x	x	x				

Název činnosti	Uchazeč	0bdobí, kdy je činnost uskutečňována											
		1	2	3	4	5	6	7	8	9	10	11	12
Instalace a propojení zařízení a linek pro vytvoření lab. prostředí, konfigurace síťových prvků, implementace software pro samotné generování experimentů, pro vyhodnocování úspěšnosti mitigačních procedur a pro průběžné testování kvality kódu.													
2.3 Vývoj základního rozhraní Návrh, implementace a testování základních rozhraní směrem k uživateli (příkazová řádka) a rozhraní pro konfiguraci, reportování statistik. Prototypování GUI.	CESNET, zájmové sdružení právnických osob	x	x	x	x	x	x	x	x	x	x	x	x
2.4 Výzkum adaptivních a automatizačních postupů Dohledání potenciálně vhodných algoritmů a využitelných postupů v odborné literatuře, nárvh, prototypování a přizpůsobení těchto algoritmů na specifické problémy systému čištění včetně testování metod stroj. učení, sepsání výsledků a publikační činnost.	CESNET, zájmové sdružení právnických osob	x	x	x	x	x	x	x	x	x	x	x	x
2.5 Průběžná integrace Průběžné ale zatím oddělená kompilace, testování a ladění nově vyvíjených software komponent. Pravidelné vydávání stabilních verzí software.	CESNET, zájmové sdružení právnických osob							x	x	x	x	x	x
2.6 Ověření mitigačních heuristik Testování dostupných mitigačních procedur v laboratním prostředí.	CESNET, zájmové sdružení právnických osob									x	x	x	x
Rok 2021													
3.1 Průběžná integrace Průběžné sestavování, testování a ladění nově vyvíjených software komponent. Pravidelné vydávání stabilních verzí software. Akcelerace kritických částí.	CESNET, zájmové sdružení právnických osob	x	x	x	x	x	x	x	x	x	x	x	x
3.2 Rozšíření testovacího prostředí Rozšíření software o další schopnosti, např. generování aplikačních útoků. Dále rozšíření o testování výkonnosti jednotlivých částí i celého systému.	CESNET, zájmové sdružení právnických osob	x	x	x	x	x	x	x	x	x	x	x	x
3.3 Vývoj adaptivních a automatizačních postupů Návrh rozhraní a detailní funkcionality komponent zajišťujících adaptivnost mitigačních metod a automatizaci jejich volby včetně realizace pokročilých mitigačních procedur. Následná implementace a testování až do podoby produkčního software.	CESNET, zájmové sdružení právnických osob	x	x	x	x	x	x	x	x	x	x	x	x
3.4 Vývoj pokročilého rozhraní Návrh, implementace a testování GUI včetně následných úprav dle požadavků uživatelů.	CESNET, zájmové sdružení právnických osob	x	x	x	x	x	x	x	x	x	x	x	x
Rok 2022													
4.1 Finální integrace systému Sestavení a sladění jednotlivých softwarových komponent, sestavení hardwarové platformy, uzpůsobení pro danou platformu. Tvorba instalačních nástrojů a balíků. Tvorba uživ. dokumentace a popis sestavení funkčního vzorku.	CESNET, zájmové sdružení právnických osob	x	x	x	x	x	x	x	x				
4.2 Validace funkčního vzorku Nasazení a měření vlastností a výkonnosti funkčního vzorku nejprve v laboratorním a následně produkčním prostředí peeringového uzlu. Dokumentace výsledků validace.	CESNET, zájmové sdružení právnických osob				x	x	x	x	x				

5.13 Popis rizik projektu a jejich řízení

Popis rizik projektu a jejich řízení

Fluktuace lidských zdrojů. Vyšší míra fluktuace je způsobena tím, že do výzkumu a vývoje projektu jsou zapojeni Ph.D. a magisterští studenti. U studentů lze rovněž předpokládat vyšší míru fluktuace způsobenou například ukončením studia a ukončením činnosti na projektu. Míra rizika byla vyhodnocena jako vysoká. Navržená protiopatření jsou zastupitelnost klíčových řešitelů, průběžné získávání a školení vysoce kvalifikovaných pracovníků v průběhu projektu, průběžně vznikající vývojářská dokumentace, code review a provádění interních kontrolních dnů, využití repositářů a wiki systémů pro uchování dat a sdílení informací.

Nesoulad s požadavky zainteresovaných subjektů. Toto riziko je sníženo složením řešitelského týmu, neboť výsledky projektu budou mimo jiné využívat i samotní řešitelé v rámci sítě sdružení CESNET. Dalším protiopatřením je průběžná konzultace vývoje systému s Národním úřadem pro kybernetickou bezpečnost a dalšími subjekty a jejich zapojení do testování systému. Komunikace se zainteresovanými subjekty započala již před samotným podáním projektu, jak je doloženo přiloženými dopisy vyjadřující zájem o výsledek.

Nedosažení výzkumných záměrů projektu. Míra rizika je střední, v případě cíle na plnou automatizaci mitigace je riziko vysoké. Navržená protiopatření jsou pokrytí činností vysoce kvalifikovanými a zkušenými výzkumníky a vývojáři, konzultace na úrovni univerzit, naplánovaná dedikovaná činnost na výzkum v nejvíce rizikové oblasti.

Nedostatečná spolupráce v rámci týmu. V každém projektu existuje riziko špatné spolupráce ve smyslu řízení, komunikace, předávání know-how či výsledků. Míra rizika je nízká vzhledem k předchozí dobré týmové spolupráci na předchozích projektech. Navržená protiopatření jsou ustavení hierarchie řízení a odpovědnosti ale i komunikace v rámci týmu, pořádání pravidelných schůzí, kde bude docházet k plnému informování ostatních řešitelů o probíhajících aktivitách a výsledcích, a minimálně dvakrát ročně jedno až dvoudenní výjezdní seminář.

Nesoulad s legislativou. Systém tedy bude zpracovávat a využívat data a identifikátory, které mohou mít charakter různými právními instituty chráněných údajů (osobní údaje, důvěrné informace, informace, které jsou předmětem telekomunikačního tajemství). Míra rizika je vyhodnocena jako střední. Řešitelský tým ustavil následující protiopatření: komunikace obsahu projektu DPO, autorizace přístupů k reálným datům pouze oprávněným pracovníkům, sledování a přizpůsobení systému nedávno zavedeným regulacím např. NIS, GDPR, eIDAS, ePrivacy a jejich transpozice do národní legislativy (např. NIS a novelizace zákona o kybernetické bezpečnosti), školení zaměstnanců na tyto právní rámce.

5.14 Doplňující informace k projektu

Doplňující informace k projektu

Projekt naváže na projekt TA03010561 "Distribuovaný systém pro komplexní monitorování vysokorychlostních sítí". Při implementaci bude v první fázi využita především karta COMBO-CG vyvinutá v rámci TA03010561. Předkládaný projekt se však zásadně liší od TA03010561:

- Zcela novým konceptem je aktivní zpracování živého provozu, kdy doposud byl vždy zpracováván provoz pouze pasivně bez jeho modifikace.
- Zcela odlišné tematické směrování projektu, předkládaný projekt plánuje řešit oblast mitigace DDoS útoků, zatímco TA03010561 řešil monitoring síťového provozu.

Projekt souvisí s projekty VI20162019029 "Sdílení a analýza bezpečnostních událostí v ČR" a VI20152020026 "Predikce a ochrana před kybernetickými incidenty". Na rozdíl od uvedených se předkládaný projekt zaměřuje na samotnou DDoS obranu, nikoliv na korelaci a sdílení informací o incidentech. Nicméně předkládaný projekt může velmi dobře využít výsledků těchto projektů, např. informace z reputační databáze, která je plánovaným výsledkem VI20152020026.

Projekt svým obsahem souvisí též s běžícím projektem VI20152019001 "Sondy pro analýzu a filtraci provozu na úrovni aplikačních protokolů". V rámci projektu VI20152019001 jsou vyvíjeny sondy pro hloubkový monitoring sítí operujících s 1 a 10 Gb/s Ethernetem. V případě akcelerace zpracování aplikačních protokolů na síťové kartě využije předkládaný projekt relevantních výstupů tohoto projektu.

Projekt TH01010229 "Technologie pro ochranu vysokorychlostních sítí" vyvinul základní firmware, který se používá v experimentálním zařízení pro čištění provozu. Předkládaný projekt tak naváže na projekt TH01010229 využitím firmware a budováním software s pokročilou funkcionalitou.

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 (%)
CESNET, zájmové sdružení právnických osob	**Celkem**	**19 845.815**	**0.025**	**19 845.79**	**100**
	2019	1 524.838	0.008	1 524.83	100
	2020	5 779.47	0.01	5 779.46	100
	2021	7 341.833	0.003	7 341.83	100
	2022	5 199.674	0.004	5 199.67	100
PROJEKT	**Celkem**	**19 845.815**	**0.025**	**19 845.79**	**100**

6.2 Rozpočet projektu

6.2.1 Výpočet maximální míry podpory uchazeče CESNET, zájmové sdružení právnických osob

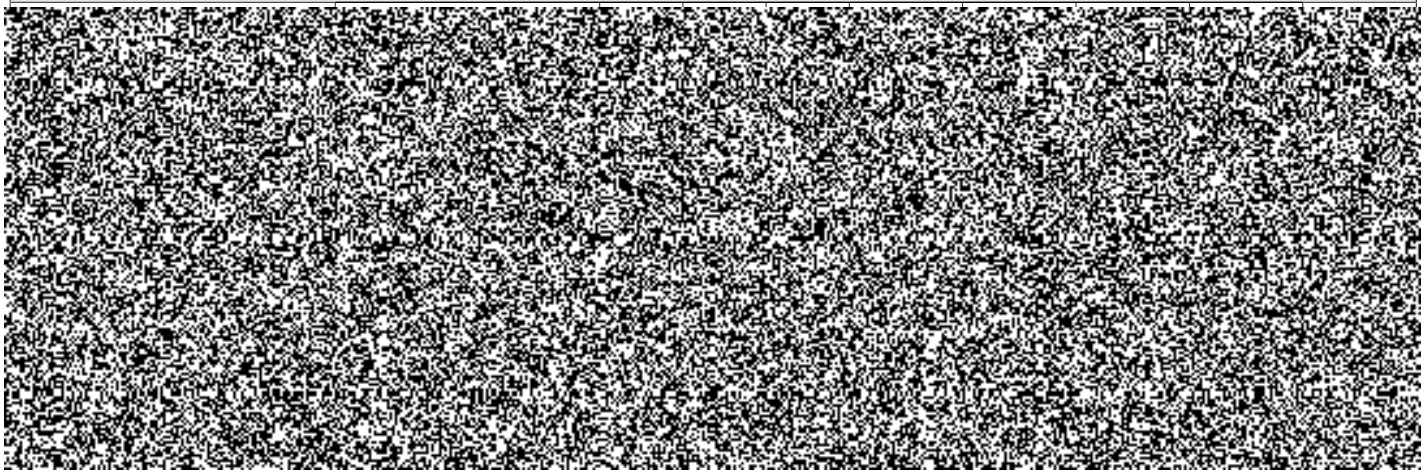
Kategorie uchazeče	výzkumná organizace
Kategorie výzkumu	průmyslový výzkum
Způsobilé náklady uchazeče (tis. Kč)	**19 845.815**

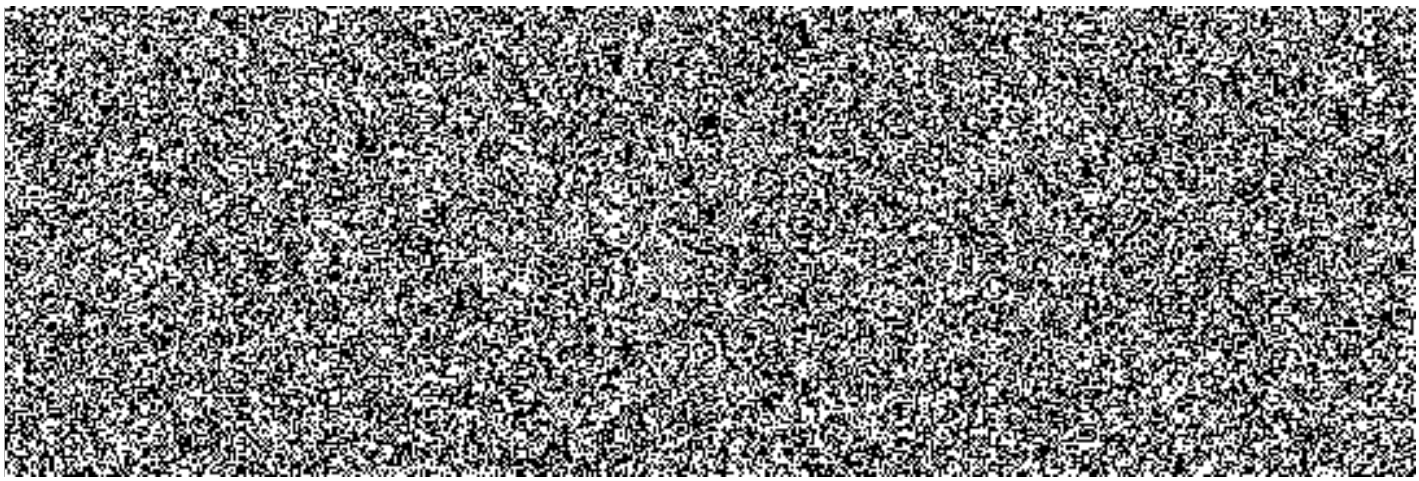
Účastní se projektu alespoň dva nezávislé podniky?	NE
Hradí každý podnik maximálně 70% nákladů projektu?	NE
Účastní se projektu malý nebo střední nebo zahraniční podnik?	NE
Účastní se projektu výzkumná organizace?	ANO
Je podíl výzkumné organizace na celkovém rozpočtu projektu vyšší než 10 %?	ANO
Může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

Základní intenzita podpory (%)	50.00
Bonus (%)	50.00
Maximální intenzita podpory (%)	**100.00**
Maximální výše podpory (tis. Kč)	**19 845.815**

6.2.2 Náklady na mzdy/platy uchazeče CESNET, zájmové sdružení právnických osob

Jméno	Pozice v projektu	Druh pracovní smlouvy	Hodinová mzdová sazba (Kč)	Průměrný počet odprac. hodin měsíčně	Náklady na mzdy/platy v jednotlivých letech trvání projektu (tis. Kč)				Náklady celkem (tis. Kč)
					2019	2020	2021	2022	
Řešitelé									





6.2.3 Náklady uchazeče CESNET, zájmové sdružení právnických osob na pořízení majetku

6.2.4 Rozpočet nákladů uchazeče CESNET, zájmové sdružení právnických osob

Náklady/výdaje uchazeče (tis. Kč)	2019	2020	2021	2022	Celkem
Osobní náklady/výdaje - mezisoučet	**1 386.217**	**5 254.064**	**6 674.394**	**4 646.977**	**17 961.652**
a) mzdy/platy na základě pracovního poměru	675.24	2 358.036	3 230.192	2 250.863	8 514.331
b) osobní náklady/výdaje na základě dohody o pracovní činnosti	353.28	1 525.594	1 705.923	1 172.254	4 757.051
c) osobní náklady/výdaje na základě dohody o provedení práce	0	0	0	0	0
d) povinné pojistné na sociální zabezpečení	257.13	970.907	1 234.029	855.779	3 317.845
e) povinné pojistné na zdravotní pojištění	92.567	349.527	444.25	308.081	1 194.425
f) odvody do FKSP nebo sociálního fondu	0	0	0	0	0
g) cestovné	8	50	60	60	178
Náklady/výdaje na pořízení hmotného a nehmotného majetku - mezisoučet	**0**	**0**	**0**	**0**	**0**
a) dlouhodobý hmotný majetek	0	0	0	0	0
b) dlouhodobý nehmotný majetek	0	0	0	0	0
c) drobný hmotný majetek	0	0	0	0	0
d) drobný nehmotný majetek	0	0	0	0	0
Další provozní náklady/výdaje - mezisoučet	**0**	**0**	**0**	**0**	**0**
Náklady/výdaje na služby - mezisoučet	**0**	**0**	**0**	**80**	**80**
a) subdodávky	0	0	0	0	0
b) ostatní služby	0	0	0	80	80
Audit projektu	0	0	0	80	80
Doplňkové náklady/výdaje - mezisoučet	**138.621**	**525.406**	**667.439**	**472.697**	**1 804.163**
Režie příjemce	138.621	525.406	667.439	472.697	1 804.163
Celkové způsobilé náklady - mezisoučet	**1 524.838**	**5 779.47**	**7 341.833**	**5 199.674**	**19 845.815**
Celková státní podpora - mezisoučet	**1 524.83**	**5 779.46**	**7 341.83**	**5 199.67**	**19 845.79**

6.2.5 Rozpočet nákladů za celý projekt

Náklady/výdaje za celý projekt (tis. Kč)	2019	2020	2021	2022	Celkem
Osobní náklady/výdaje	**1 386.217**	**5 254.064**	**6 674.394**	**4 646.977**	**17 961.652**
Náklady/výdaje na pořízení hmotného a nehmotného majetku	**0**	**0**	**0**	**0**	**0**
Další provozní náklady/výdaje	**0**	**0**	**0**	**0**	**0**
Náklady/výdaje na služby	**0**	**0**	**0**	**80**	**80**
Doplňkové náklady/výdaje	**138.621**	**525.406**	**667.439**	**472.697**	**1 804.163**

Náklady/výdaje za celý projekt (tis. Kč)	2019	2020	2021	2022	Celkem
Celkové způsobilé náklady	**1 524.838**	**5 779.47**	**7 341.833**	**5 199.674**	**19 845.815**
Celková státní podpora	**1 524.83**	**5 779.46**	**7 341.83**	**5 199.67**	**19 845.79**

Souhlas statutárního zástupce uchazeče CESNET, zájmové sdružení právnických osob 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

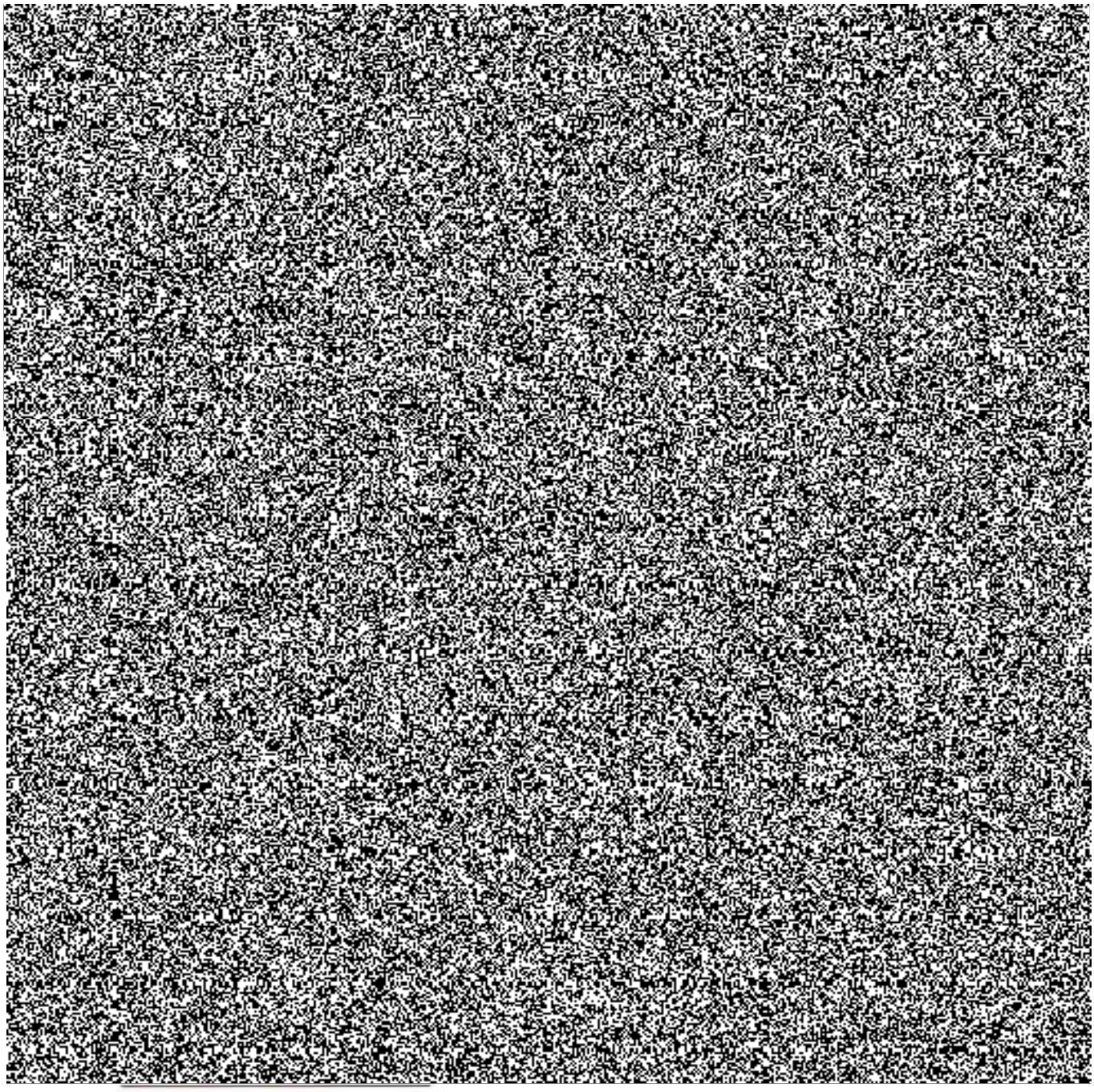
Titul před jménem	Jméno	Příjmení	Titul za jménem	Podpis
Ing.	Jan	Gruntorád	CSc.	

Elektronický podpis - 7.6.2019
Certifikát autora podpisu :
Jméno : JUDr. Petr Novák, Ph.D.
Vydal : PostSignum Qualified C...
Platnost do : 30.4.2020 10:17:21-000 +02:00

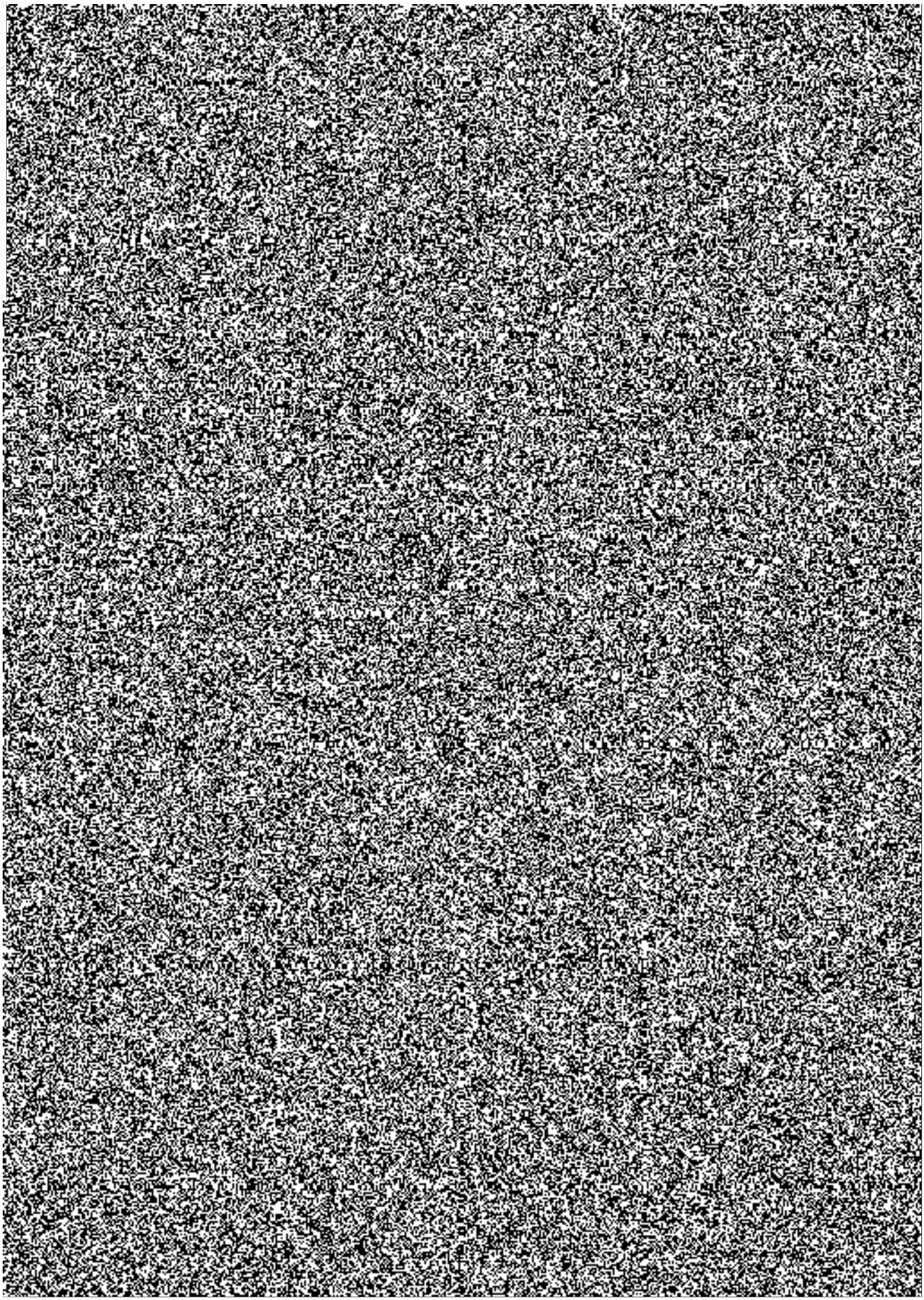
Příloha č. 4.2.2
Počet listů[1]: 12

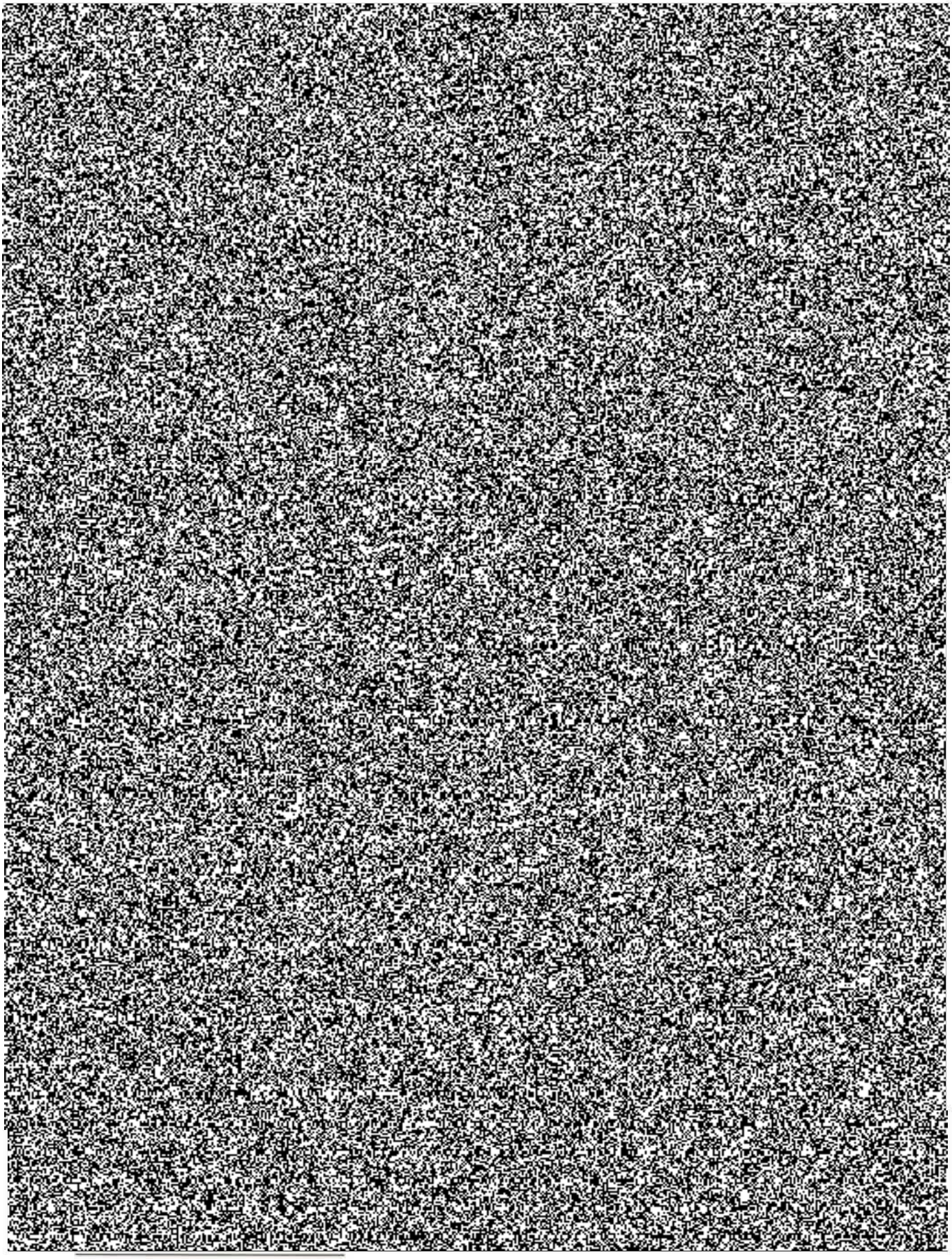
Plán využití výsledků projektu a jejich popis[2]

Název uchazeče: CESNET, z. s. p. o.
Sídlo uchazeče: Zikova 4, 160 00 Praha 6
IČ: 63839172
Název navrhovaného projektu: Adaptivní ochrana před DDoS útoky

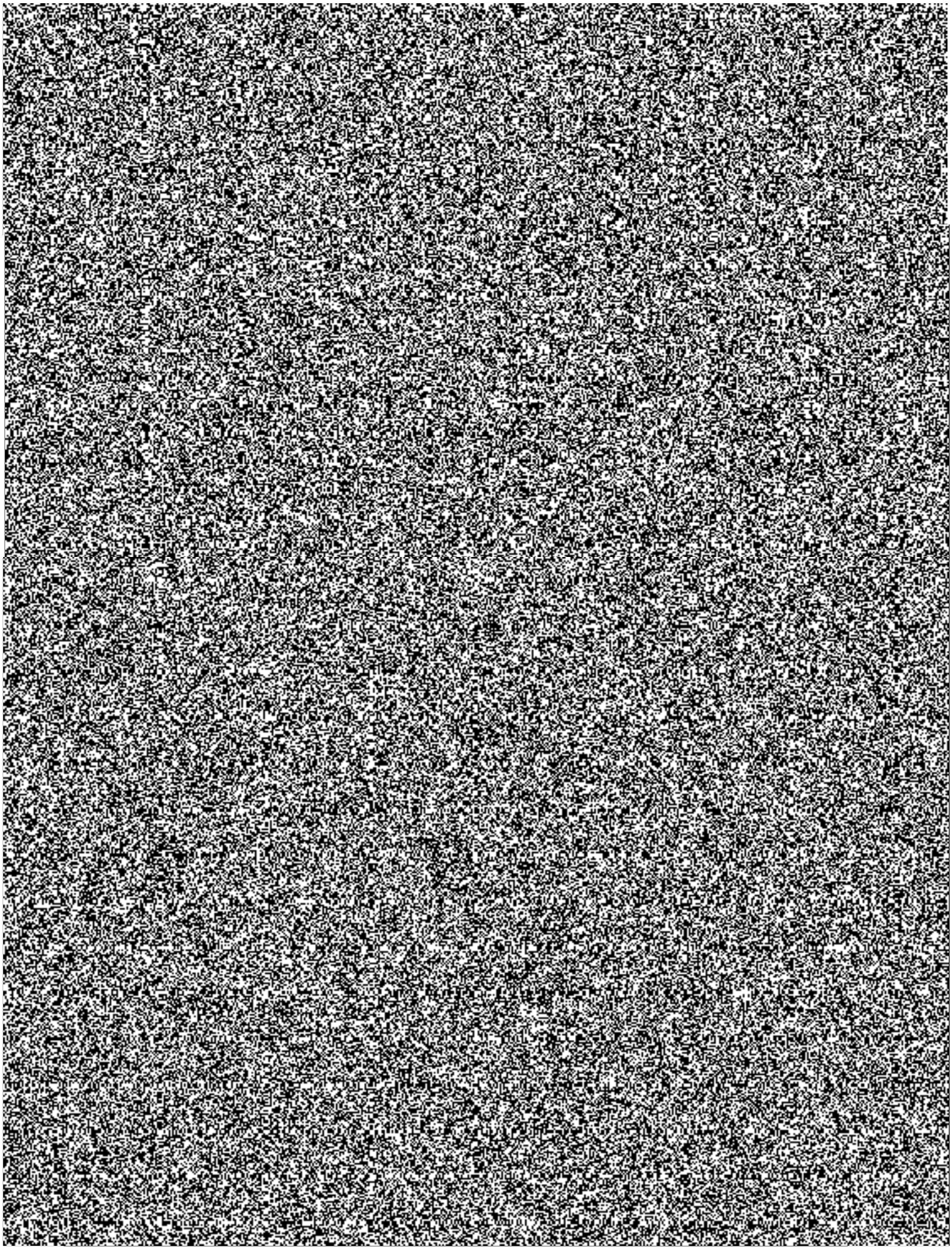


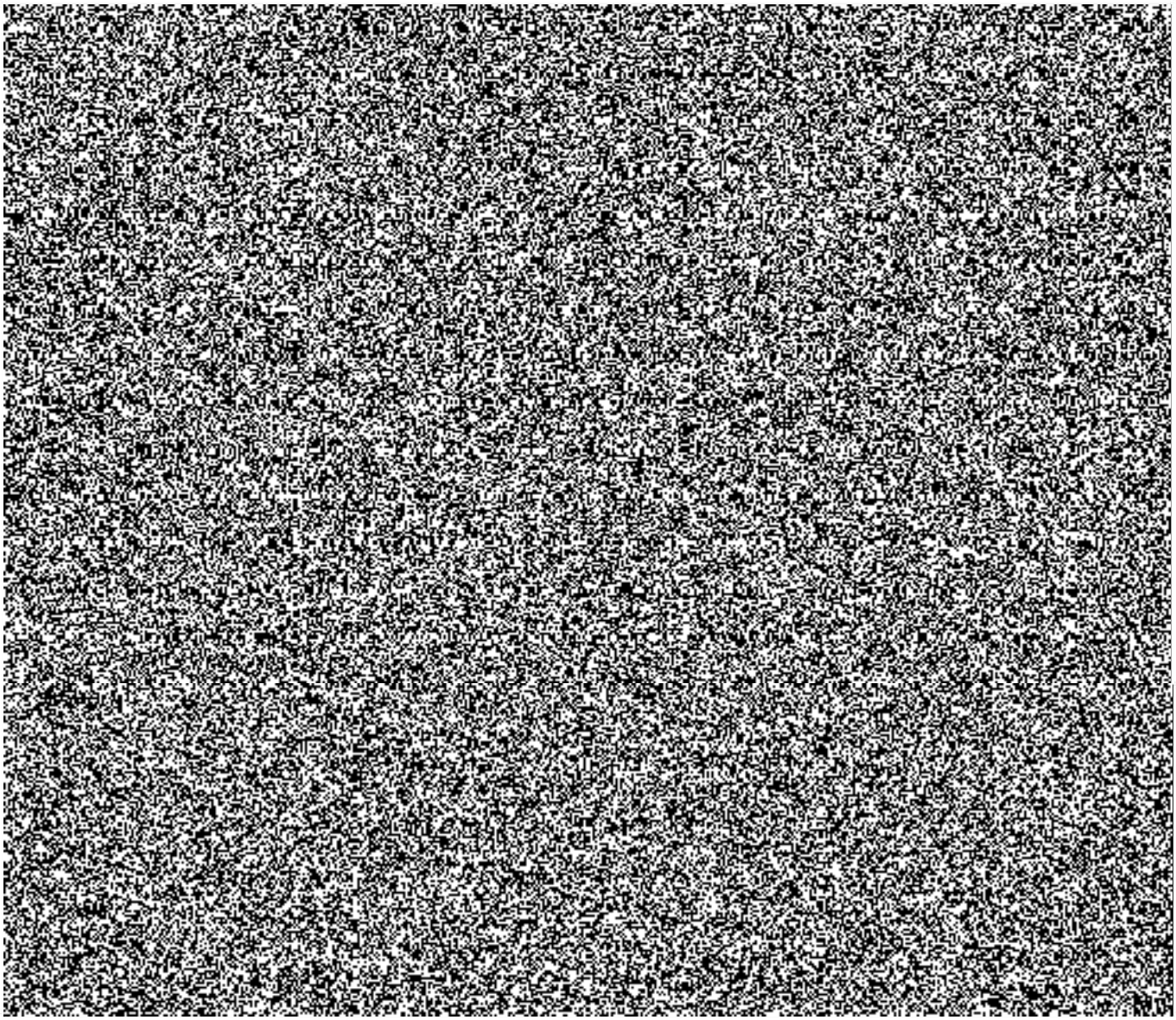
[1]*) Uchazeč záhlaví vyplní, nehodící se škrtněte
Uchazeč list vyplní, aktualizuje Počet listů
[2] Povinná příloha pro všechny uchazeče, v případě, že projekt podává více uchazečů, předkládá koordinátor

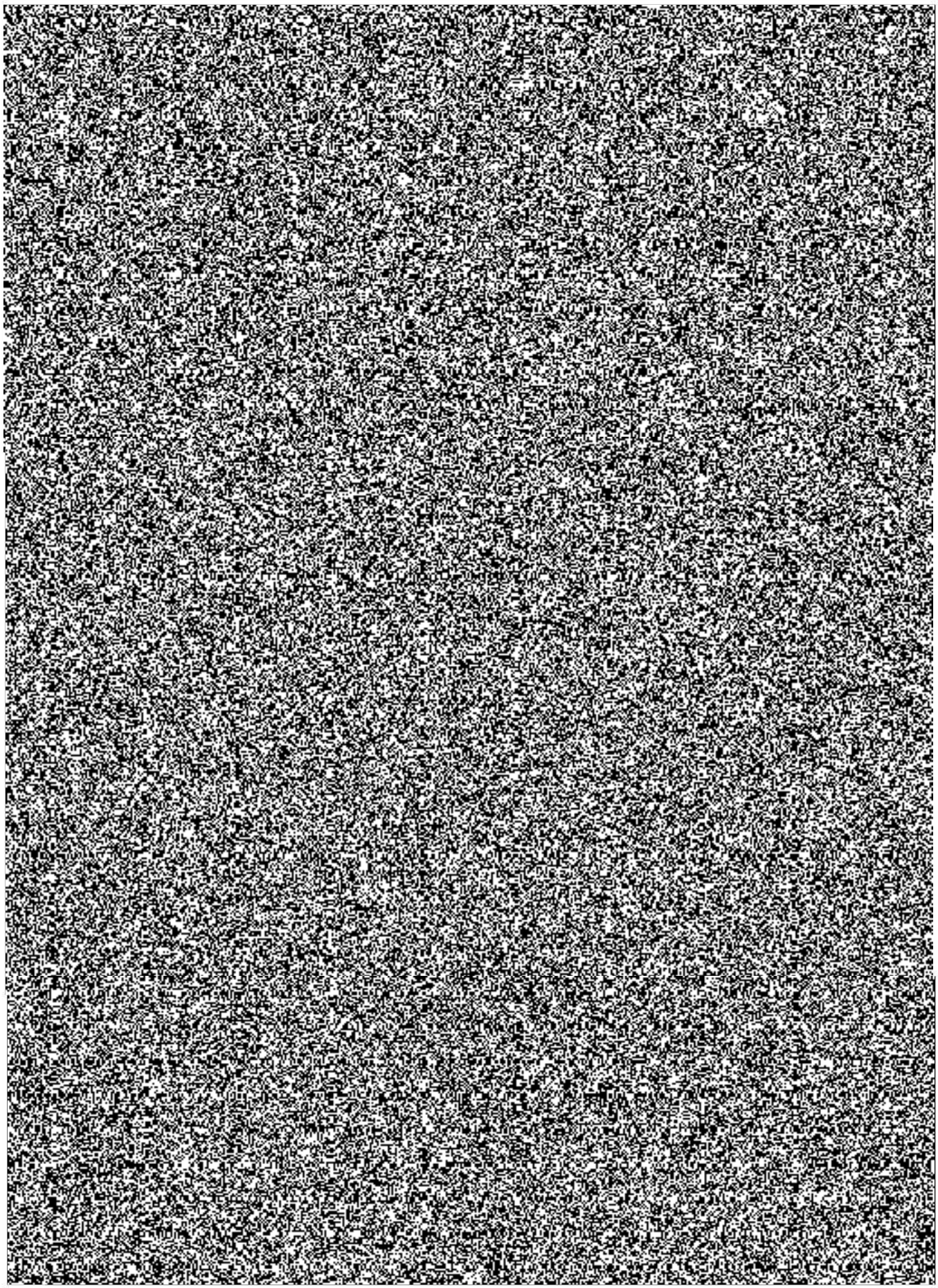


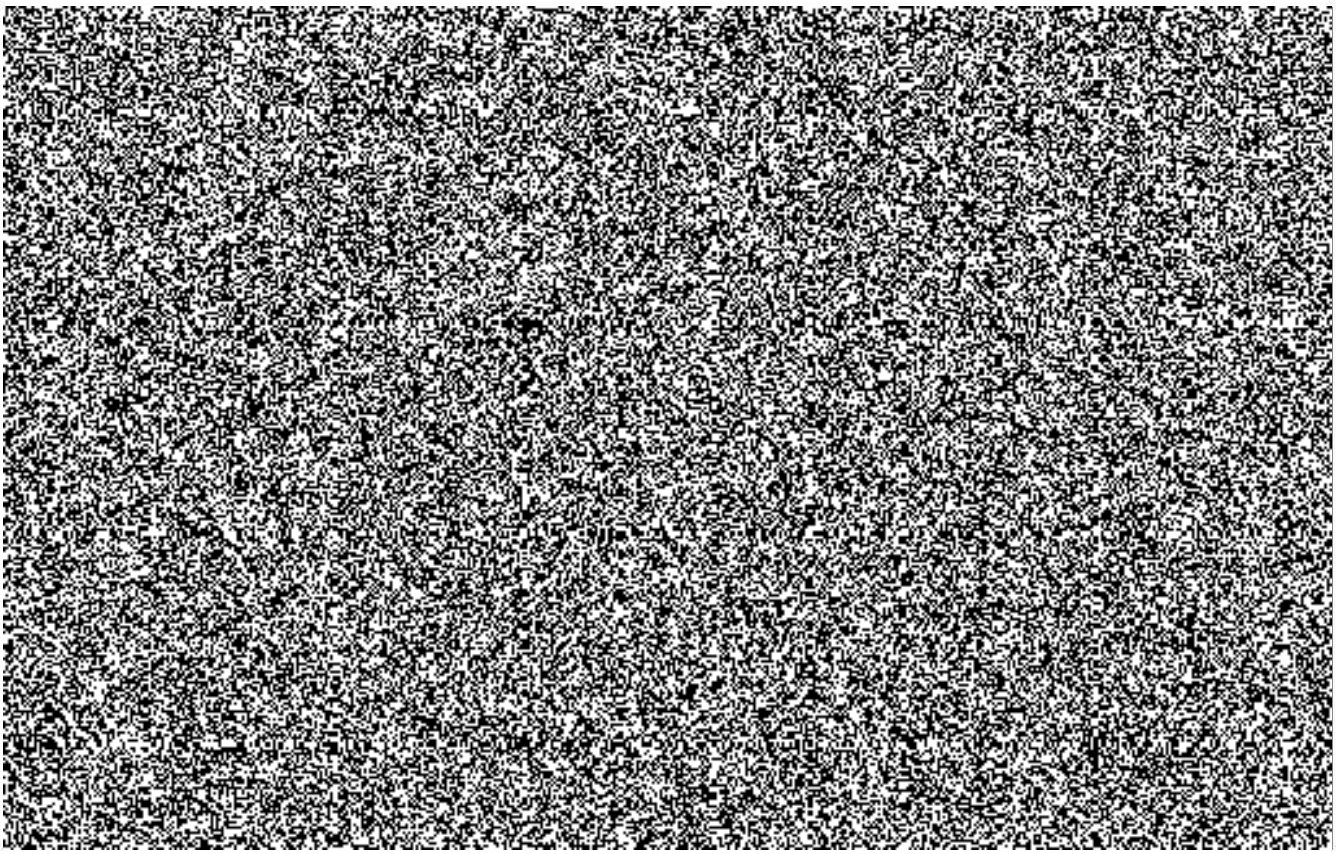


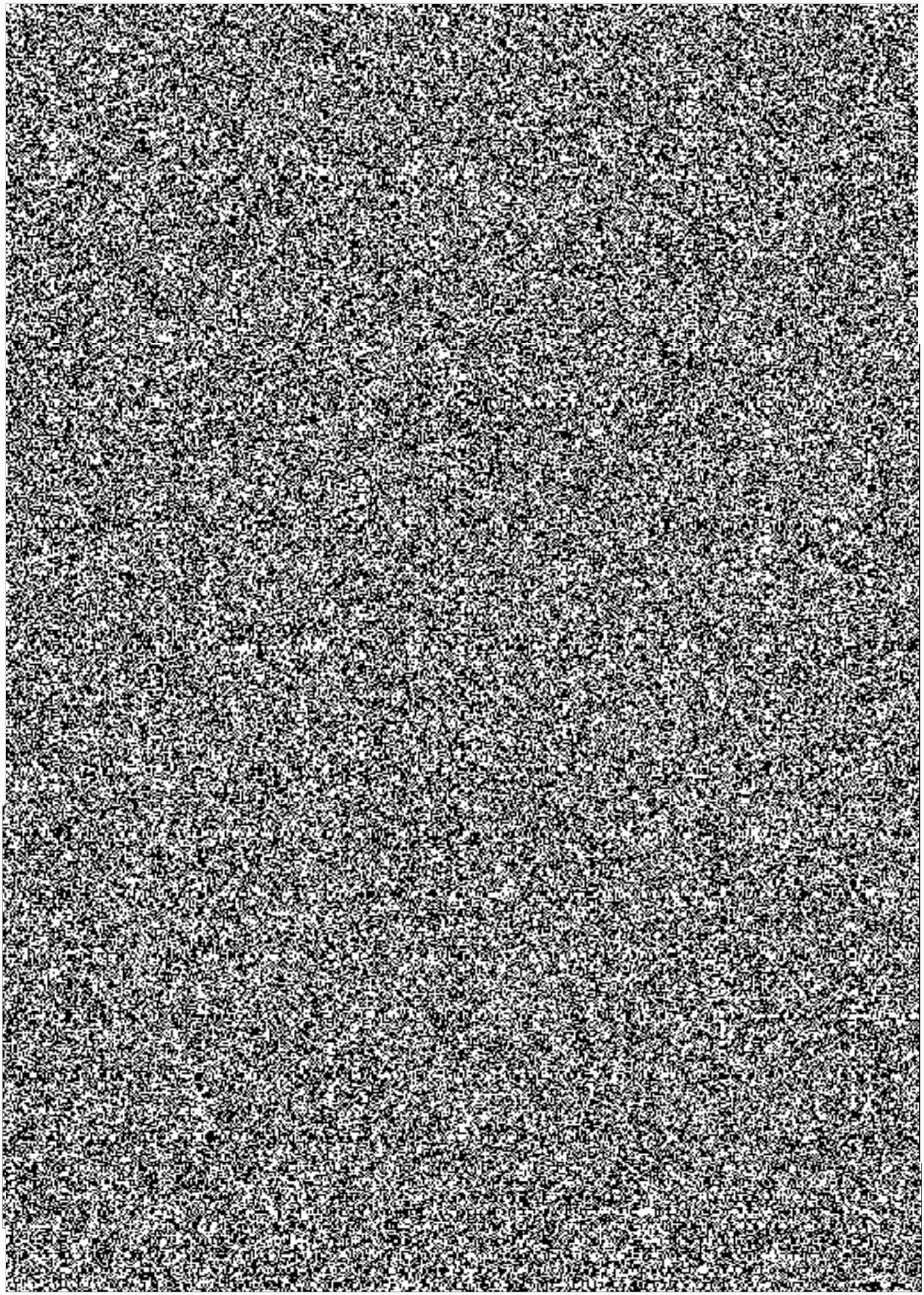
[3] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

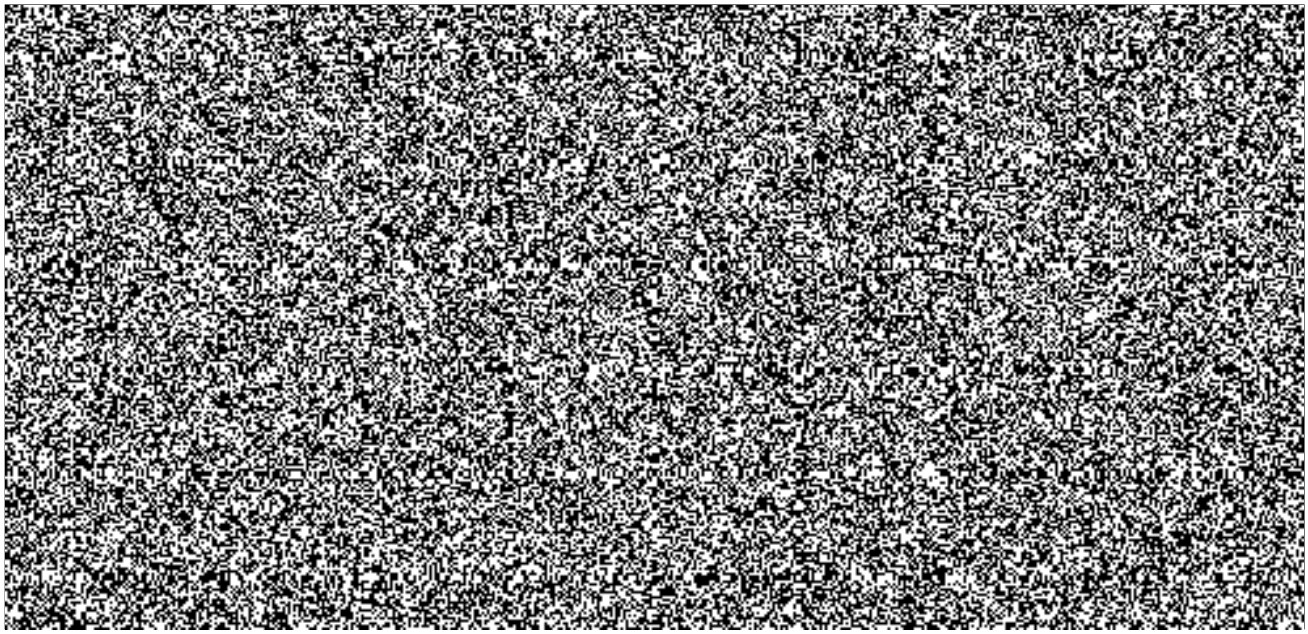






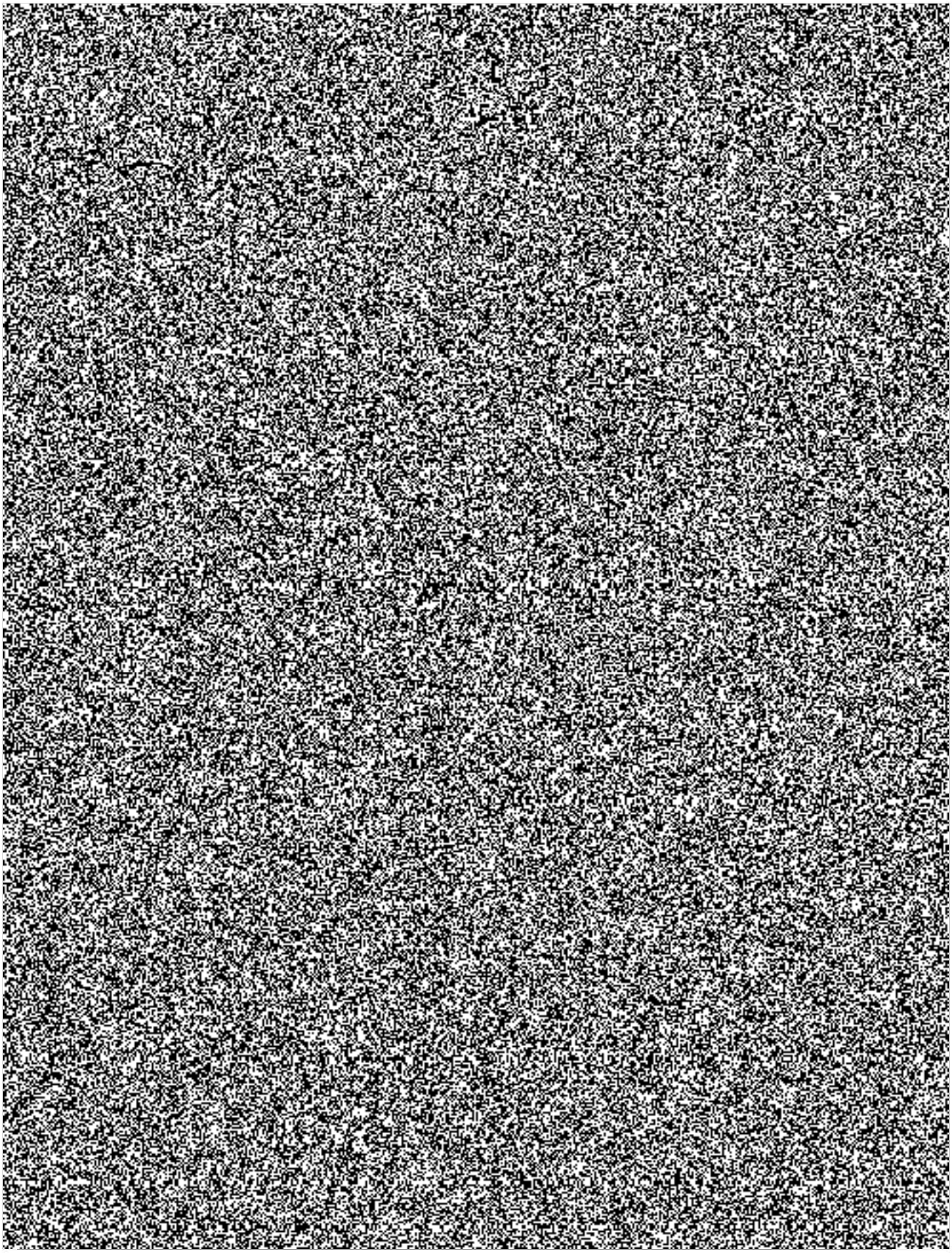


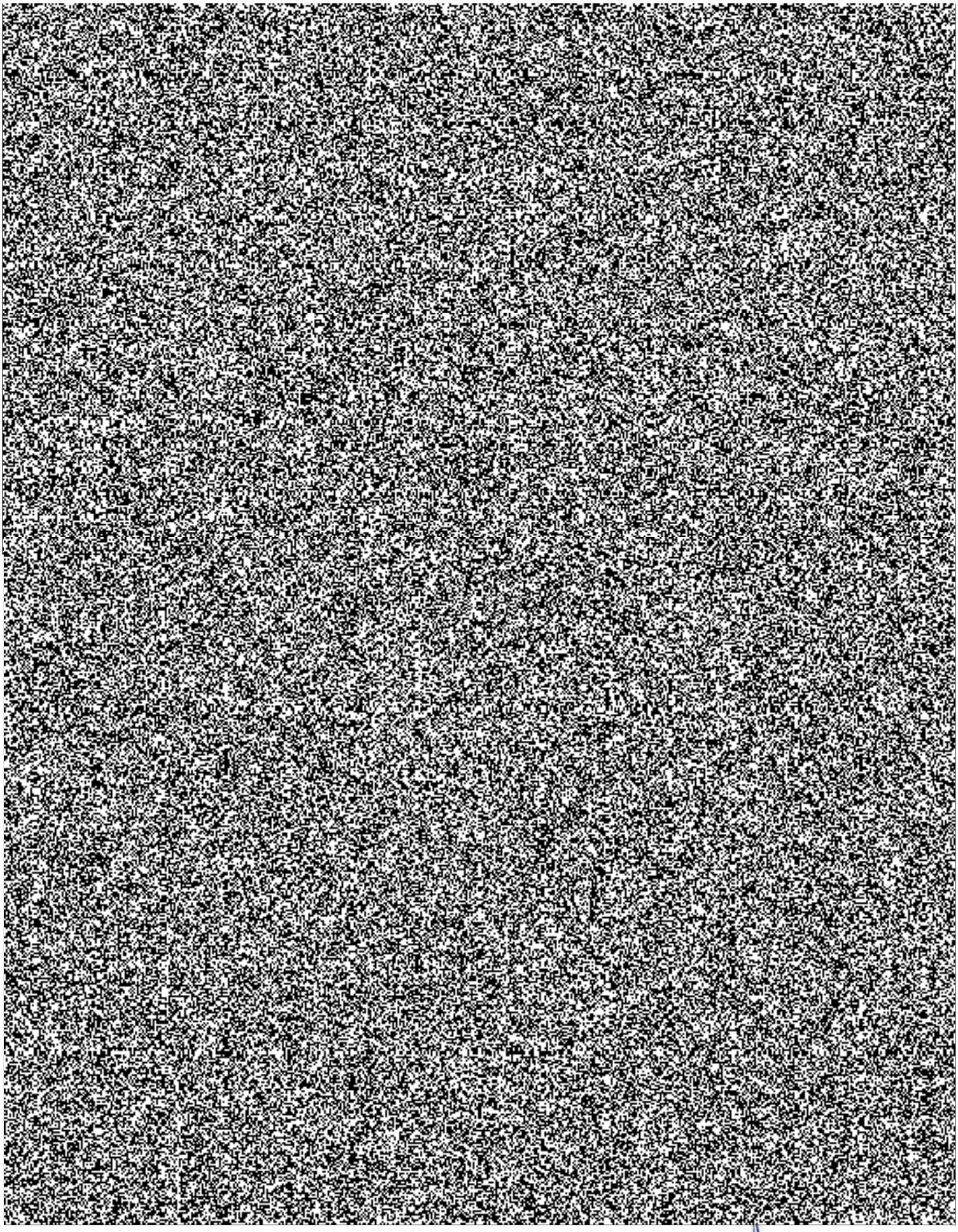




Předběžný název a druh výsledku:

Funkční vzorek zařízení pro čištění síťového provozu; výsledek typu Gfunk - funkční vzorek





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_{uzlt}**
		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

cesnet

JUDr. Petr Novák, Ph.D., ředitel odboru
Ministerstvo vnitra České republiky
Odbor bezpečnostního výzkumu a vzdělávání
Nad Štolou 3
170 34 Praha 7

[redacted]

V Praze dne 24. 5. 2019

[redacted]

ROZPOČET NÁVRHU PROJEKTU VI3VS/734 s názvem „Adaptivní ochrana před DDoS útoky"

Vážený pane řediteli,

na základě výzvy zasíláme v příloze upravený rozpočet návrhu projektu s názvem **„Adaptivní ochrana před DDoS útoky" (VI3VS/734).**

V případě dotazů nás neváhejte kontaktovat.

S pozdravem

[redacted]

Přílohy:
VI3VS-734_ROZPOČET.pdf
VI3VS-734_ROZPOČET.xls

VI3VS/734 - Adaptivní ochrana před DDoS útoky

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 (%)
CESNET, zájmové sdružení právnických osob	**Celkem**				
	2019	1 524,838	0,000	1 524,838	100
	2020	5 779,470	0,000	5 779,470	100
	2021	7 341,833	0,000	7 341,833	100
	2022	5 199,674	0,000	5 199,674	100
PROJEKT	**Celkem**	**19 845,815**	**0,000**	**19 845,815**	**100**

6.2.4 - Rozpočet nákladů uchazeče CESNET, zájmové sdružení právnických osob

Náklady/výdaje uchazeče (v tis. Kč)	2019	2020	2021	2022	Celkem
Osobní náklady/výdaje - mezisoučet	**1 386,217**	**5 254,064**	**6 674,394**	**4 646,977**	**17 961,652**
a) mzdy/platy na základě pracovního poměru	675,240	2 358,036	3 230,192	2 250,863	8 514,331
b) osobní náklady/výdaje na základě dohody o pracovní	353,280	1 525,594	1 705,923	1 172,254	4 757,051
c) osobní náklady/výdaje na základě dohody o provedení	0,000	0,000	0,000	0,000	0,000
d) povinné pojistné na sociální zabezpečení	257,130	970,907	1 234,029	855,779	3 317,845
e) povinné pojistné na zdravotní pojištění	92,567	349,527	444,250	308,081	1 194,425
f) odvody do FKSP nebo sociálního fondu	0,000	0,000	0,000	0,000	0,000
g) cestovné	8,000	50,000	60,000	60,000	178,000
Náklady/výdaje na pořízení hmotného a nehmotného majetku - mezisoučet	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
a) dlouhodobý hmotný majetek	0,000	0,000	0,000	0,000	0,000
b) dlouhodobý nehmotný majetek	0,000	0,000	0,000	0,000	0,000
c) drobný hmotný majetek	0,000	0,000	0,000	0,000	0,000
d) drobný nehmotný majetek	0,000	0,000	0,000	0,000	0,000
Další provozní náklady/výdaje - mezisoučet	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
Náklady/výdaje na služby - mezisoučet	**0,000**	**0,000**	**0,000**	**80,000**	**80,000**
a) subdodávky	0,000	0,000	0,000	0,000	0,000
b) ostatní služby	0,000	0,000	0,000	80,000	80,000
Audit projektu	0,000	0,000	0,000	80,000	80,000
Doplňkové náklady/výdaje - mezisoučet	**138,621**	**525,406**	**667,439**	**472,697**	**1 804,163**
Režie příjemce	138,621	525,406	667,439	472,697	1 804,163
Celkové způsobilé náklady - mezisoučet	**1 524,838**	**5 779,470**	**7 341,833**	**5 199,674**	**19 845,815**
Celková státní podpora - mezisoučet	**1 524,838**	**5 779,470**	**7 341,833**	**5 199,674**	**19 845,815**

6.2.5 - Rozpočet nákladů za celý projekt

Náklady/výdaje uchazeče (v tis. Kč)	2019	2020	2021	2022	Celkem
Osobní náklady/výdaje	**1 386,217**	**5 254,064**	**6 674,394**	**4 646,977**	**17 961,652**
Náklady/výdaje na pořízení hmotného a nehmotného	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
Další provozní náklady/výdaje	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
Náklady/výdaje na služby	**0,000**	**0,000**	**0,000**	**80,000**	**80,000**
Doplňkové náklady/výdaje	**138,621**	**525,406**	**667,439**	**472,697**	**1 804,163**
Celkové způsobilé náklady	**1 524,838**	**5 779,470**	**7 341,833**	**5 199,674**	**19 845,815**
Celková státní podpora	**1 524,838**	**5 779,470**	**7 341,833**	**5 199,674**	**19 845,815**