

Smlouva

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

„Národní kvalifikační rámec v kyberbezpečnosti“

VI20192022161

uzavřená mezi smluvními stranami

Česká republika – Ministerstvo vnitra

a

Masarykova univerzita

Č.j.MV-56522-6/OBVV-2019

Počet stran: 14

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.

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@mvcv.cz

(dále jen „**poskytovatel**“)

a

Masarykova univerzita - Fakulta informatiky

se sídlem: Žerotínovo náměstí 617/9, 601 77 Brno

IČ: 00216224

DIČ: CZ00216224

statutární zástupce: doc. PhDr. Mikuláš Bek, Ph.D., rektor

veřejná vysoká škola uvedená v příloze č. 1 zákona č. 111/1998 Sb., o vysokých školách

adresa pro doručování: sídlo příjemce

kontaktní osoba: manažerka projektu

(dále jen „**příjemce**“)

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

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

Článek 1 Předmět Smlouvy

- 1) Předmětem této Smlouvy je závazek příjemce řešit projekt výzkumu, vývoje a inovací s názvem „**Národní kvalifikační rámec v kyberbezpečnosti**“ a identifikačním kódem „**VI20192022161**“ a závazek poskytovatele poskytnout příjemci na tento projekt účelovou podporu z veřejných prostředků (dále jen "podpora") v rozsahu a za podmínek stanovených Smlouvou.
- 2) Předmětem řešení projektu je experimentální vývoj zaměřený na vytvoření univerzálního a celostního rámce kvalifikací v ČR v oblasti kyberbezpečnosti. Rámec bude klasifikovat jednotlivé kvalifikace a profesní role pracovníků v oblasti kyberbezpečnosti, popisovat jejich požadované vzdělání, schopnosti a dovednosti a bude sloužit jako jednotný podklad pro rozvoj kapacit v této oblasti v ČR. K Rámci bude náležet rovněž akční plán a informační systém, které umožní využití rámce v praxi vzdělávání a nábory odborníků.
- 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 

Článek 5 Doba řešení Projektu

- 1) Příjemce je povinen zahájit řešení Projektu dnem nabytí účinnosti Smlouvy dle Čl. 25 odst. 1 Smlouvy.
- 2) Příjemce je povinen ukončit řešení Projektu nejpozději ke dni 30. 6. 2022.

Článek 6 Uznané náklady, výše podpory a platební podmínky

- 1) Uznané náklady¹ na řešení Projektu se stanovují ve výši **7 436 600,- Kč** (slovy: sedmmilionůčtyřistatřicetšesttisícšestsetkorunčeských). Tato částka zahrnuje podporu ve výši **7 436 600,- Kč** (slovy: sedmmilionůčtyřistatřicetšesttisícšestsetkorunčeských), 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 pořizení 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 plátcí 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 nesouvisí s předmětem řešení projektu,
 - správní poplatky,
 - výdaje související s likvidací příjemce, nedobytné pohledávky,
 - platby příspěvků do soukromých penzijních fondů,
 - peněžitá pomoc v mateřství,
 - ostatní sociální výdaje na zaměstnance, které nejsou zaměstnavatelé povinni odvádět dle zvláštních předpisů (např. dary k životním jubileím, příspěvky na rekreaci, příspěvky na penzijní připojištění, životní pojištění apod.),
 - odstupné,
 - nájemné, kdy příjemce je vlastníkem nemovitosti nebo ji užívá zdarma,
 - výdaje na školení a vzdělávání personálu (pokud se nejedná o odborné akce přímo související s řešením projektu).
- 3) Do uznaných nákladů na pořízení hmotného a nehmotného majetku lze zahrnout pouze část ceny majetku, která odpovídá podílu užití majetku na řešení Projektu.
- 4) Příjemce účtuje doplňkové náklady související s **Projektem metodou kalkulace úplných nákladů (FC - Full Costs)**.
- 5) V případě, že příjemce předpokládá nevyčerpání finančních prostředků daného kalendářního roku, ale využil by je v rámci projektu v roce následujícím, je povinen požádat poskytovatele o schválení využití těchto nespotřebovaných finančních prostředků, a to do 15. listopadu daného kalendářního roku cestou změnového řízení. V případě, že bude jeho žádost poskytovatelem schválena, ponechá si příjemce tyto nespotřebované finanční prostředky na svém účtu. V případě, že žádost nebude poskytovatelem schválena, příjemce tyto nespotřebované finanční prostředky převede obratem na bankovní účet poskytovatele číslo [redacted] při převodu finančních prostředků příjemce uvede do Zprávy pro příjemce: VRÁTKA-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,

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

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

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 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, řádně specifikovaný podle § 8 odst. 4 zákona č. 130/2002 Sb.
- 2) Hmotný a nehmotný majetek nspecifikovaný řádně podle § 8 odst. 4 zákona č. 130/2002 Sb. je příjemce povinen pořizovat postupem podle zákona č. 134/2016 Sb.
- 3) Pokud se v průběhu řešení Projektu vyskytne potřeba pořídit hmotný a nehmotný majetek, postupuje se podle zákona č. 134/2016 Sb.
- 4) Hmotný a nehmotný majetek je příjemce povinen pořizovat za tržní ceny (tj. cena v místě a čase obvyklá). Toto je příjemce povinen poskytovateli doložit.
- 5) Vlastníkem majetku, pořízeného z poskytnuté podpory je ve smyslu ustanovení § 15 odst. 1 zákona č. 130/2002 Sb. příjemce.
- 6) 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 nedostatkem 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 přerušování 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 uložení 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 zákona⁴, 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.

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

- 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 – 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.

Článek 25 Platnost a účinnost Smlouvy

- 1) Smlouva se uzavírá na dobu určitou a nabývá platnosti dnem podpisu obou smluvních stran a účinnosti dnem zveřejnění v registru smluv.
- 2) Smlouva je ukončena dnem 27. 12. 2022.
- 3) Ukončení Smlouvy před datem uvedeným v odstavci 2 tohoto článku je upraveno v ustanovení Článku 21 odst. 4 písm. b) a c) Smlouvy.

Za poskytovatele:

Za příjemce:

JUDr. Petr Novák, Ph.D.

doc. PhDr. Mikuláš Bek, Ph.D.

V Praze dne:

V

dne:



Národní kvalifikační rámec v kyberbezpečnosti

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

Uchazeč: **Masarykova univerzita**

Další účastníci: **0**

Hlavní obor: **IN - Informatika**

Vedlejší obor: **AM - Pedagogika a školství**

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

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS

PID: VI3VS/710

Hlavní obor: IN

Stupeň důvěrnosti: S

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

3b) Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby

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

Národní kvalifikační rámec v kyberbezpečnosti

2.2 Název projektu anglicky

Název projektu anglicky

National cybersecurity workforce qualification framework

2.3 Anotace projektu

Anotace projektu

Cílem projektu je výzkum zaměřený na vytvoření univerzálního a celostního rámce kvalifikací v ČR v oblasti kyberbezpečnosti. Rámec bude klasifikovat jednotlivé kvalifikace a profesní role pracovníků v oblasti kyberbezpečnosti, popisovat jejich požadované vzdělání, schopnosti a dovednosti a bude sloužit jako jednotný podklad pro rozvoj kapacit v této oblasti v ČR. K Rámci bude náležet rovněž akční plán a informační systém, které umožní využití rámce v praxi vzdělávání a náborem odborníků.

2.4 Anotace projektu anglicky

Anotace projektu anglicky

The aim of the project is research focused on creating a universal and holistic framework of qualifications in the Czechia in the field of cyber security. The framework will classify individual professional roles of cyber security workforce, describe their required knowledge, skills and abilities and will serve as a single basis for capacity development in this area in the Czechia. Proposed Action Plan and software will allow the use of the framework in the training and recruitment of workforce.

2.5 Kategorie činnosti

Kategorie činnosti

experimentální vývoj

2.6 Předpokládané datum zahájení projektu

Předpokládané datum zahájení projektu

01.07.2019

2.7 Datum ukončení projektu

Datum ukončení projektu

30.06.2022

2.8 Projekt má více uchazečů

Projekt má více uchazečů

NE

2.9 Klíčová slova

Klíčová slova

kyberbezpečnost; kvalifikace; rámec kvalifikací; vzdělávání; informační a bezpečnostní technologie

2.10 Klíčová slova anglicky

Klíčová slova anglicky

cyber security; qualification; qualification framework; education; information and security technologies

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS

PID: VI3VS/710

Hlavní obor: IN

Stupeň důvěrnosti: S

3. Identifikace uchazeče

3.1 Název uchazeče

Název uchazeče Masarykova univerzita
Organizační jednotka 14330 - Fakulta informatiky

3.2 Právní forma

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

3.3 IČ

IČ 00216224

3.4 DIČ

DIČ CZ00216224

3.5 Sídlo uchazeče

Státní příslušnost CZ - Česká republika			
Kraj Jihomoravský	Obec Brno		
Ulice Žerotínovo náměstí	Č. popisné 617	Č. orientační 9	PSČ 60177
Telefon +420549491111	E-mail info@muni.cz		
Web stránka			

3.7 Statutární zástupce/zástupci uchazeče

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

3.8 Kategorie uchazeče

Kategorie uchazeče VO - výzkumná organizace
--

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

<p>Popis předchozích zkušeností uchazeče v oblasti výzkumu a vývoje za posledních 5 let</p> <p>Masarykova univerzita a její fakulta informatiky jako hlavní pracoviště projektu je pravidelným úspěšným uchazečem o projekty VaVal napříč programovými rámci vyhlášenými v ČR, EU i jinde. Spolupracuje s akademickými partnery, s orgány státní a veřejné správy vč. oblasti kyberbezpečnosti, s komerční i neziskovou sférou.</p> <p>V oblasti kyberbezpečnosti a ochrany kritických infrastruktur dlouhodobě spolupracuje s NÚKIB ve výzkumu a vzdělávání (národní technické cvičení CyberCzech), s resorty vnitra, obrany, v energetice s hlavními provozovateli elektrorozvodných soustav na bázi smluvního výzkumu (zejména ČEPS, ČEZd). Je členem Technologické platformy energetická bezpečnost. Provozuje Vědeckotechnický park CERIT, Sdružení průmyslových partnerů, má vyspělý systém transferu technologií, zakládá spin-off společnosti vč. kyberbezpečnosti (např. Flowmon Networks).</p> <p>Univerzita založila ve spolupráci s VUT, CESNET, RHK a průmyslovými subjekty Národní centrum kompetence pro kyberbezpečnost.</p> <p>Pilířem interdisciplinárního výzkumu na MU v kyberbezpečnosti je centrum C4e (Cybersecurity, Cybercrime and Critical Information Infrastructures Centre of Excellence) vč. zahraničních strategických partnerů a expertů.</p>

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS

PID: VI3VS/710

Hlavní obor: IN

Stupeň důvěrnosti: S

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

Identifikátor	Název
VF20102014003	Analýza přirozeného jazyka v prostředí internetu
Oblast výzkumu a vývoje	
Oblastí výzkumu byly vyvinuty a implementovány techniky zpracování přiroz. jazyka umožňující analyzovat jazykové projevy na Internetu, které spadají do působnosti českých bezpečnostních orgánů (neonacismu, rasismu, terorismu) s důrazem na určování autora.	
Výsledky evidované v RIV	
J- článek -Rygl, J. - Hledání autora. 2014. RIV/00216224:14330/14:00073243	
D- Stať ve sborníku - Jakubiček, M. et al., Effective Corpus Virtualization, 2014, RIV/00216224:14330/14:00094187	
V - Vynikající výsledky projektu s mezinárodním významem.	

Identifikátor	Název
VG20102014031	Experimentální vývoj bezpečnostní softwarové platformy se systémem detekce průniku a režimy ochrany soukromí pro bezdrátové senzorové sítě
Oblast výzkumu a vývoje	
Oblastí výzkumu bylo zvýšení bezpečnosti státu a občanů s využitím nových technologií a poznatků v oblasti bezpečnosti bezdrátových senzorových sítí, které slouží k monitorování a identifikaci škodlivých jednání a ochraně proti nezákonným jednáním.	
Výsledky evidované v RIV	
R - Software - Matyáš et al. WSNProtectLayer -Software for securing wireless sensor network applications. It provides security aware layer that encompasses key distribution, privacy protection and intrusion detection functionality. 2014. RIV/00216224:14330/14:00073222	

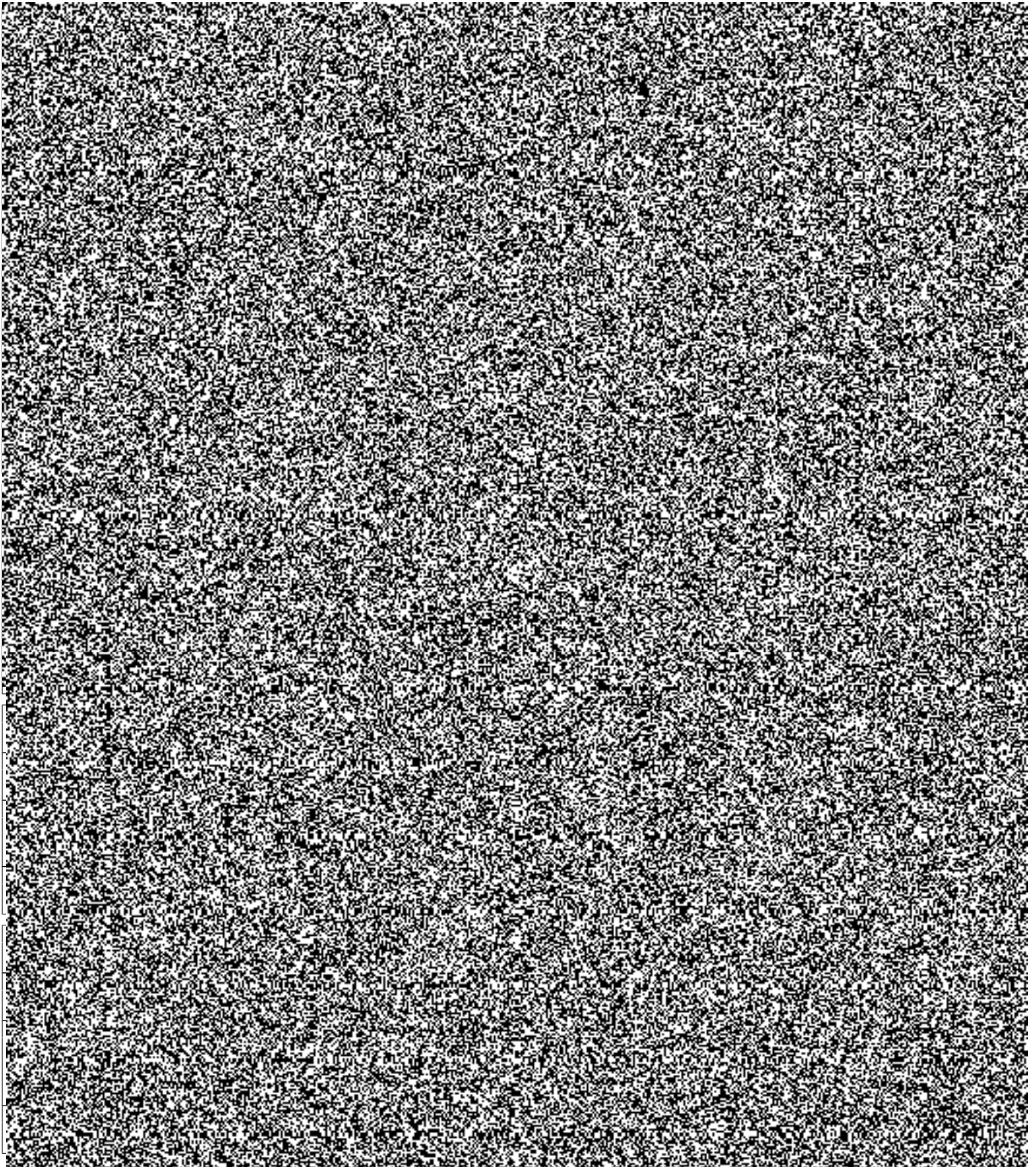
Identifikátor	Název
VG20132015103	Kybernetický polygon
Oblast výzkumu a vývoje	
Výzkum a vývoj unikátního prostředí pro analýzu hrozeb ohrožujících bezpečnost kritických informačních infrastruktur. V prostředí polygonu lze provádět komplexní scénáře útoků vedených proti kritickým infrastrukturám a analyzovat jejich průběh.	
Výsledky evidované v RIV	
G – Funkční vzorek – Čegan, J. et al. KYPO – Kybernetický polygon. 2015. (RIV/00216224:14610/15:00080536).	
D – Článek ve sborníku – Čeleda, P. et al. KYPO – A Platform for Cyber Defence Exercises. 2015. (RIV/00216224:14610/15:00080539).	
D – Článek ve sborníku – Kouřil, D. et al. Cloud-based Testbed for Simulation of Cyber Attacks. 2014. (RIV/00216224:14610/14:00073216).	

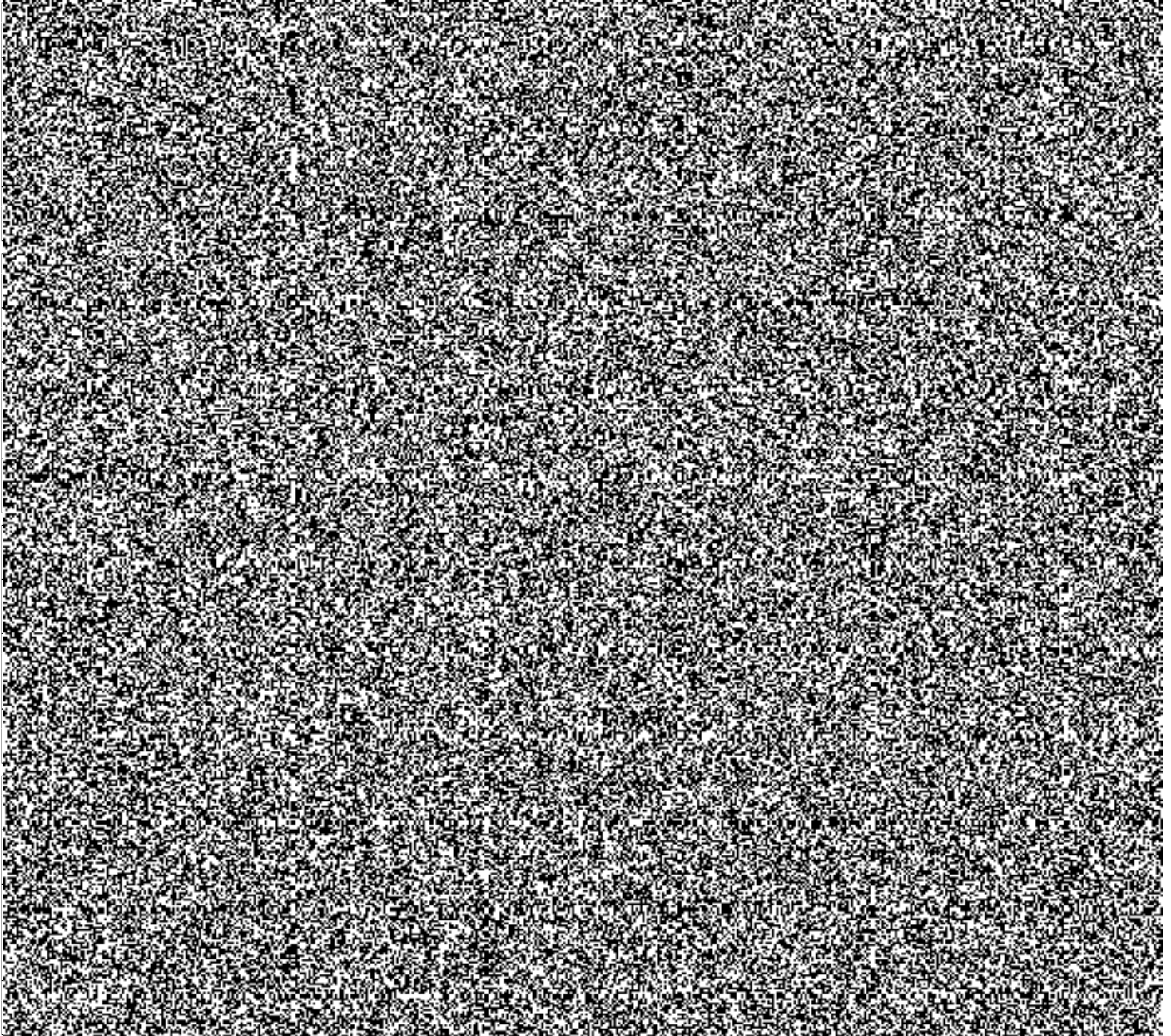
3.11 Výsledky projektů výzkumu a vývoje uchazeče, které byly nebo jsou prokazatelně úspěšně využívány komerčně

Identifikátor	Název
ČEZ	Celkové závěry a doporučení k projektu přípravných rešerší k AMM
Kým a po jakou dobu komerčně využíván, případně číslo patentu nebo jiného typu právní ochrany	
Celkové závěry a doporučení jsou shrnutím výstupů Zpracování projektu přípravných rešerší k AMM, kterou Masarykova univerzita ve spolupráci s ČVUT v Praze v rámci České akademické expertní skupiny vypracovala v průběhu druhého pololetí roku 2015. Jejím cílem bylo zodpovědět s využitím dostupných pramenů, výstupů předchozích projektů odběratele a vlastního know-how dodavatele otázky definované v zadání rešerší.	
V - Výzkumná zpráva - Pitner et al., Celkové závěry a doporučení k projektu přípravných rešerší k AMM, 2015, RIV/00216224:14330/15:00085208	

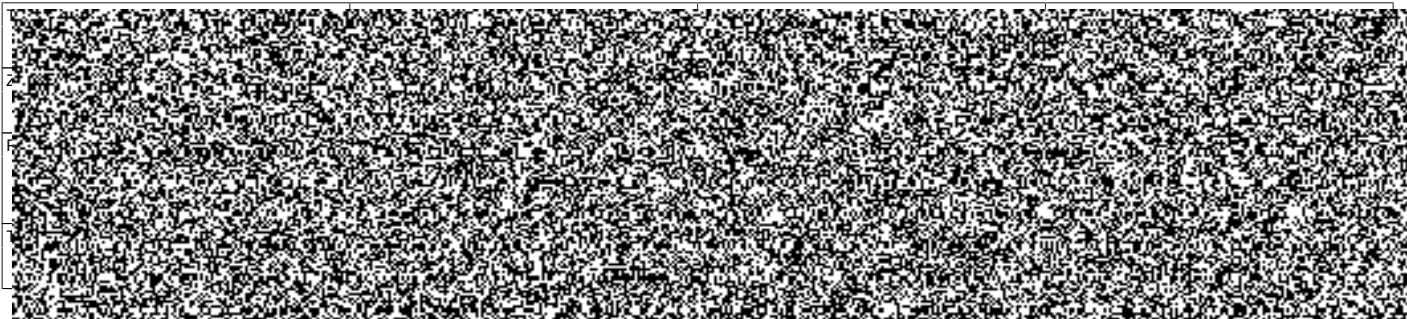
Identifikátor	Název
ČEZ	Studie pro bezpečné poskytování dat z elektroměru zákazníkovi v místě spotřeby
Kým a po jakou dobu komerčně využíván, případně číslo patentu nebo jiného typu právní ochrany	
Projekt smluvního výzkumu řešil problematiku vhodných technologií, základního procesního rámce a omezení pro bezpečné poskytování dat zákazníkovi v místě spotřeby tak, aby byly splněny požadavky Doporučení 2012/148/EU. Požadavkem bylo navrhnout doporučený rozsah poskytovaných dat, vhodné přenosové technologie a protokoly vč. jejich zabezpečení. Součástí bylo technologické porovnání možností, analýza plnění funkčních požadavků v zemích EU evt. dalších, jakož i požadavků realizátorů "chytrých domů". Bylo navrženo možné řešení ke zvážení.	
V - Výzkumná zpráva - Pitner et al., Studie pro bezpečné poskytování dat z elektroměru zákazníkovi v místě spotřeby, 2016, RIV/00216224:14330/16:00094112	

3.12 Řešitelský tým projektu

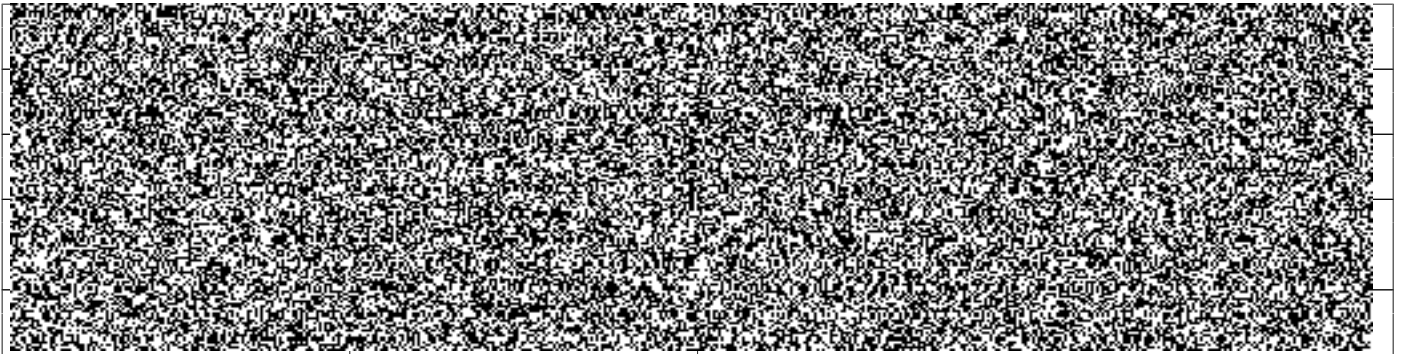




3.13 Manažer projektu



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

V současné době je zjevné, že lidských zdrojů v oblasti kybernetické bezpečnosti je nejen v rámci ČR znatelný nedostatek. Tento stav ovlivňuje bezpečnost nejen v jednotlivých organizacích, ale i celkovou bezpečnostní situaci státu, který bez dostupných odborných kapacit není schopen efektivní ochrany kybernetického prostoru. Budování těchto kapacit je pak závislé na dostupnosti příslušného vzdělávání. V současné době je však vzdělávání v oblasti kybernetické bezpečnosti (vč. kybernetické obrany a stíhání kybernetické kriminality) roztržštěné a existující potřeby pokrývá jen z části. Proto je současným trendem rozvoj vzdělávání v oblasti kyberbezpečnosti postavený na analytickém posouzení rozsahu potřebných lidských zdrojů v jednotlivých kvalifikacích a identifikaci vhodného rozsahu a úrovně vzdělávání těchto kvalifikací. Příkladem tohoto přístupu může být NICE Framework z USA, kurikula ACM CSec a obecně v ICT pak rámec .

Cílem předkládaného projektu je proto realizovat výzkum zaměřený na popis a kategorizaci jednotlivých kvalifikací v oblasti kybernetické bezpečnosti, identifikaci nezbytných kapacit v jednotlivých kvalifikacích, návrh rozsahu jejich znalostí a schopností, analýzu dostupného vzdělávání v ČR v oblasti kybernetické bezpečnosti, GAP analýzu zaměřenou na mezery v dostupných vzdělávacích programech a návrh nového obsahu vzdělávacích programů v oblasti kybernetické bezpečnosti.

Přínos projektu pro bezpečnostní praxi bude spočívat především v tom, že poskytne celostní pohled na potřebné lidské zdroje v kybernetické bezpečnosti a poskytne vzdělávacím institucím vodítko k sestavování nezbytných vzdělávacích programů za účelem pokrytí identifikované poptávky. To povede ke zvýšení dostupnosti odborné pracovní síly v oblasti kybernetické bezpečnosti a v důsledku ke zlepšení bezpečnostní situace na úrovni organizací i státu.

5.2 Dílčí cíle projektu

Dílčí cíle projektu

- Vytvoření taxonomie kvalifikací – bude provedena analýza existujících řešení a výzkumných výsledků v zahraničí, šetření potřeb v rámci bezpečnostních složek v ČR a identifikace charakteru a struktury relevantních subjektů v ČR. Na základě těchto aktivit bude navržena taxonomie kvalifikací v kybernetické bezpečnosti, která bude strukturovanou formou identifikovat potřebné kvalifikace v technických i netechnických oborech na úrovni organizací i státu.
- Návrh modelu kompetencí – k jednotlivým rolem/kvalifikacím identifikovaným v první fázi budou přiřazeny odborné kompetence, které jsou předpokladem k výkonu příslušné role v kybernetické bezpečnosti.
- Návrh rámce kvalifikací v kybernetické bezpečnosti – rámec kvalifikací bude obsahovat navrženou taxonomii a kompetence jednotlivých kvalifikací, rozšířené o identifikaci požadovaných vzdělávacích kapacit na základě existující poptávky po jednotlivých kvalifikacích.
- Realizace analýzy dostupného vzdělávání v ČR – na základě šetření a dotazníků bude identifikována aktuální nabídka dostupných vzdělávacích programů, kurzů a cvičení v oblasti kybernetické bezpečnosti, které mohou být využity k budování nezbytných kapacit popsaných v rámci.
- GAP analýza – bude porovnávat požadavky na vzdělávání popsané v rámci s existující nabídkou a na základě tohoto porovnání budou identifikovány kvantitativní i kvalitativní mezery z hlediska dostupného vzdělávání v oblasti kyberbezpečnosti.
- Akční plán pro budování vzdělávacích kapacit - za účelem efektivního uplatnění výsledků projektu bude cílem rovněž vytvořit akční plán, který uživatelům a cílovým skupinám poskytne informace o možném praktickém uplatnění výsledků výzkumu na úrovni podpory a rozvoje vzdělávání, naboru a hodnocení zaměstnanců v kyberbezpečnosti.
- Interaktivní software pro práci s rámcem kvalifikací - podobně za účelem efektivního uplatnění rámce kvalifikací bude vytvořen interaktivní softwarový nástroj k usnadnění práce s ním.

5.3 Hlavní výsledky projektu

Kód	Druh výsledku	Počet
N	metodika	2
R	software	2

5.4 Vedlejší výsledky projektu

Kód	Druh výsledku	Počet
D	článek ve sborníku	2
J	článek v odborném periodiku (časopise)	1

5.5 Popis současného stavu problematiky řešené oblasti

Popis současného stavu problematiky řešené oblasti

V průběhu posledních několika dekád byla podstatná část lidských aktivit v různých oborech přesunuta do takzvaného kyberprostoru, což pro společnost vedle zjevných přínosů představuje rovněž zásadní bezpečnostní riziko. Roste množství a sofistikovanost kybernetických útoků i rizik vyplývajících z nefungujících či chybně fungujících informačních a komunikačních systémů. Ruku v ruce s tímto vývojem dramaticky roste zájem o specialisty v oblasti kyberbezpečnosti. Ten se projevuje v rostoucí poptávce po talentech - vysoce kvalifikovaných zaměstnancích v kyberbezpečnosti schopných reagovat na stále různorodější a sofistikovanější hrozby (technických specialistech na bezpečnost informačních a komunikačních technologií) a zodpovědných za budování architektury systému kybernetické bezpečnosti na úrovni organizací i státu (tedy např. právníků, politologů, administrativních zaměstnancích, manažerech apod.). Těmto trendům se věnuje nespočet publikací z posledních let, přičemž jednou z nejaktuálnějších je studie Centra pro kybernetickou bezpečnost a vzdělávání (<https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf>) publikovanou v loňském roce, která předpokládá že v roce 2022 bude rozdíl mezi poptávkou po pracovnících v kyberbezpečnosti a jejich dostupností 350tisíc osob. Klíčovým faktorem při zajišťování kybernetické bezpečnosti státu i organizací v soukromém i veřejném sektoru proto stále více bude budování pracovní síly, a významnou roli tedy bude hrát vhodně konstruovaný a

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS

PID: VI3VS/710

Hlavní obor: IN

Stupeň důvěrnosti: S

Popis současného stavu problematiky řešené oblasti

Škálovaný systém vzdělávání na mnoha stupních vzdělávání - od osvěty a základních dovedností na úrovni základních škol, přes již specializované školy střední v některých profesích, pak ale především na úrovni terciální plus postgraduální a profesního dalšího vzdělávání. Požadavek na budování personálních kapacit a související požadavek na rozvoje vzdělávání v oblasti kyberbezpečnosti ostatně zohledňují i strategické dokumenty na úrovni EU i ČR. Ve sdělení „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“ Evropská komise konstatuje, že „vzdělávání v oblasti kybernetické bezpečnosti by se mělo rozvíjet na všech úrovních, počínaje pravidelnou odbornou přípravou pracovníků v kybernetických oborech, další odbornou přípravou pro všechny odborníky v oboru IKT a novými specifickými učebními osnovami v oblasti kybernetické bezpečnosti“, přičemž toto vzdělávání „by se nemělo omezovat na odborníky v IT, ale mělo by se začlenit do učebních osnov pro jiné obory, jako je strojírenství, řízení podniků nebo právo, a také do odvětvových vzdělávacích programů“. Česká republika si pak v Národní strategii kybernetické bezpečnosti České republiky za jeden z hlavních cílů stanovuje „modernizovat stávající vzdělávací programy na základní a středoškolské úrovni a podporovat na vysokoškolské úrovni nové studijní programy, které budou přímo vytvářet experty na kybernetickou bezpečnost“.

Aby však těchto cílů mohlo být dosaženo je nutné nejdříve provést několik kroků – předně definovat jaká pracovní síla je a bude v oblasti kyberbezpečnosti poptávána, jaká je a bude její dostupnost a po jakém typu vzdělávání bude největší poptávka, teprve poté lze realizovat smysluplné kroky směrem k budování lidských zdrojů. V současné době je dostupných studií zaměřených na analýzu těchto otázek minimum nejen na úrovni ČR, ale i v EU a světě. Na úrovni EU se problematice vzdělávání v kyberbezpečnosti věnuje agentura ENISA (European Network and Information Security Agency), která se ve svých studiích zaměřuje především na analýzu existující dostupné nabídky vzdělávání, nikoliv však na problematiku dostupnosti pracovních sil z hlediska kvantitativního i kvalitativního. V ČR je pak gestorem oblasti kybernetické bezpečnosti Národní úřad pro kybernetickou a informační bezpečnost, který poskytuje toliko seznam dostupného vzdělávání v kyberbezpečnosti a ani ze strany akademických institucí nebyly potřebné studie zpracovány. Ve světě se pak za nejlépe zpracovaný materiál dá považovat takzvaný NICE (Národní iniciativa pro vzdělávání v kyberbezpečnosti) Rámec pracovní síly v kyberbezpečnosti z USA. Tento rámec definuje stromovou strukturu, která na nejvyšší úrovni definuje 7 kategorií kvalifikací, které jsou dále rozříděny do jednotlivých specializací, které obsahují konkrétní pracovní role v oblasti kyberbezpečnosti. Pro tyto jednotlivé role jsou pak definovány úkoly, které má v rámci organizace každá role vykonávat a znalosti, schopnosti a dovednosti, kterými by měl příslušný pracovník zastávající příslušnou roli disponovat. První podoba Rámce NICE byla zveřejněna v roce 2011 a od té doby prošel několika revizemi. V praxi je tento rámec využíván na úrovni pracovníků jako zdroj informací o tom, jakými kvalifikačními předpoklady by měli disponovat, chtějí-li se ucházet o práci v příslušné roli, na úrovni organizací a státních orgánů jako pomůcka využitelná při formulaci požadavků na jednotlivé kandidáty pro pracovní pozice a volbě kritérií při jejich výběru a na úrovni vzdělávacích institucí jako vodítko při konstrukci vzdělávacích programů. Zcela aktuální aktivitou je ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline (2017, 2018), kde jsou výslovně zdůrazňovány interdisciplinární přesahy.

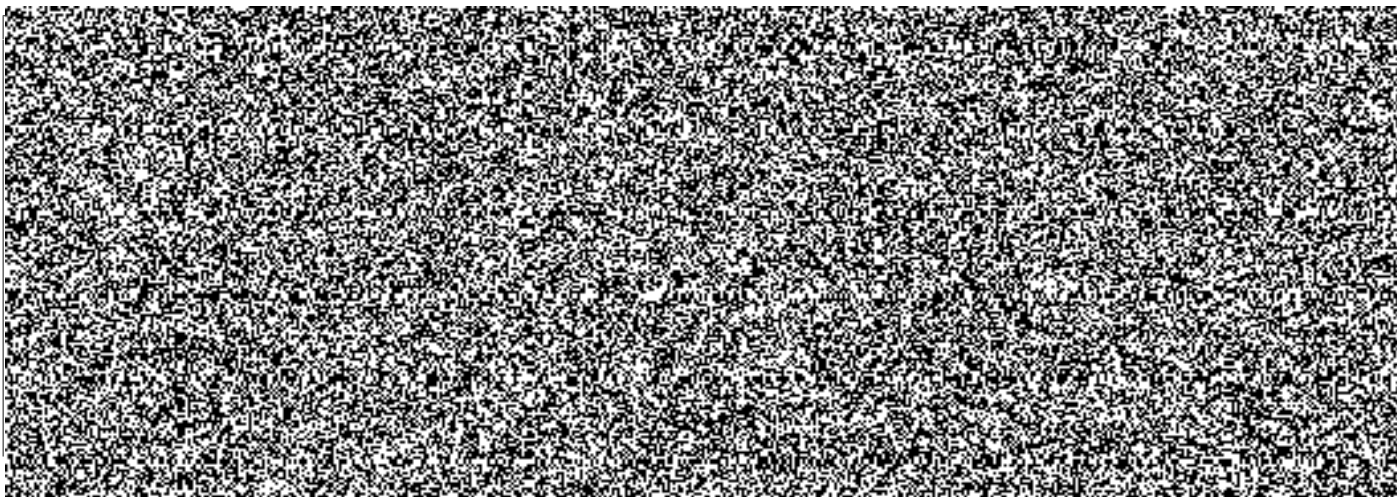
5.6 Přínosy a dopady projektu v oblasti bezpečnosti a cílů stanovených Programem

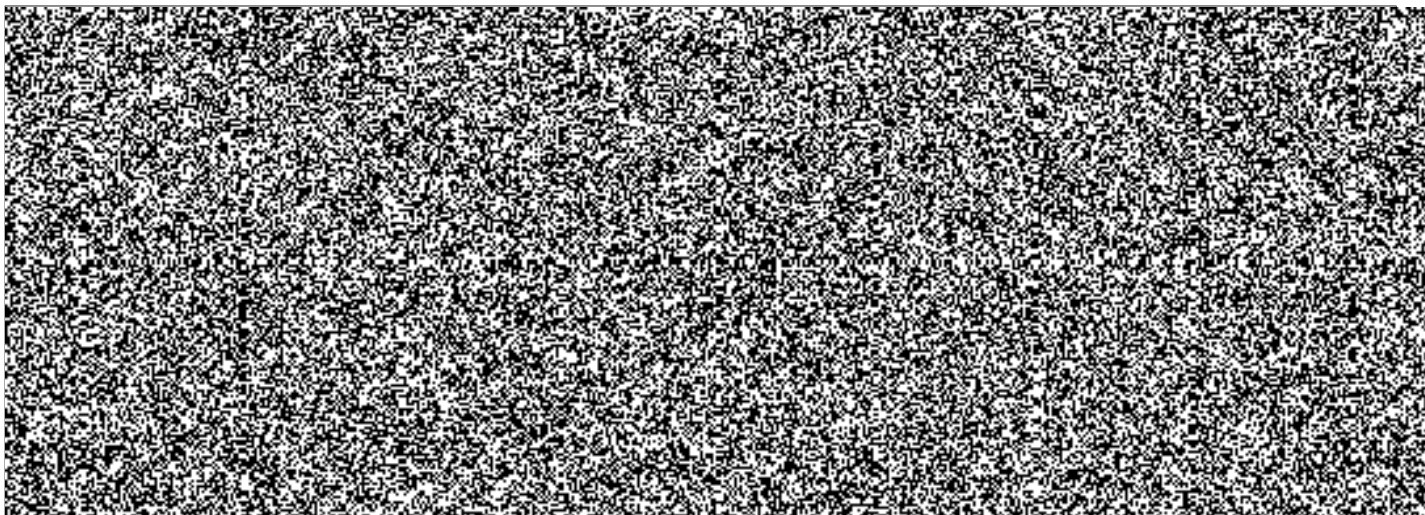
Přínosy a dopady projektu v oblasti bezpečnosti a cílů stanovených Programem

Realizace projektu bude mít přímý vliv na bezpečnostní praxi v kontextu závazků a úkolů, které plynou ze strategických cílů EU v oblasti kybernetické bezpečnosti, Strategie České republiky pro oblast kybernetické bezpečnosti a Zákona č. 181/2014 Sb. o kybernetické bezpečnosti a souvisejících prováděcích právních předpisů. Mezi konkrétní přínosy a praktické dopady projektu v oblasti bezpečnosti patří:

- Vytvoření systematizovaného přehledu kvalifikací v oblasti kybernetické bezpečnosti umožní z celospolečenského hlediska posuzovat stav personálních kapacit v kyberbezpečnosti v České republice a efektivně na jejich vývoj reagovat. Na základě vytvořené taxonomie bude totiž možné efektivně měřit (ne)dostupnost pracovníků v jednotlivých kvalifikacích/rolích a vhodně pak upravovat politiku vzdělávání na úrovni organizace, jednotlivých sektorů, či přímo na úrovni státu. Tato reaktivní schopnost pak významně posílí bezpečnost i konkurenceschopnost ČR i v mezinárodním srovnání.
- Díky formulaci požadavků na vzdělání, schopnosti a dovednosti jednotlivých kvalifikací/rolí budou mít organizace v soukromém i veřejném sektoru zjednodušené postavení při budování svých kapacit v kybernetické bezpečnosti. Vytvořený rámec bude totiž sloužit jako inspirace při formulaci požadavků na kvalifikaci poptávaných pracovních sil i při hodnocení jednotlivých uchazečů. Kromě toho bude organizacím Rámec sloužit rovněž při volbě vhodného dodatečného vzdělávání pro stávající personál.
- Díky jasné identifikaci potřebných znalostí v jednotlivých rolích, budou výsledky projektu sloužit rovněž vzdělávacím institucím při konstrukci vzdělávacích programů a tvorbě obsahu kurzů a cvičení a rovněž státu a jeho orgánům při konstrukci mechanismů podpory vzdělávání v oblasti kyberbezpečnosti. To povede k větší dostupnosti kvalitativně i kvantitativně vhodně nastavených vzdělávacích kapacit na všech úrovních školství či na komerčním trhu se vzděláním.
- Primárním cílem projektu je pochopitelně podpořit vlastní schopnost ČR budovat personální kapacity v oblasti kyberbezpečnosti. Díky výše zmíněným dopadům lze předpokládat podstatné zvýšení adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby, vzhledem k větší dostupnosti odborných kapacit v oblasti kyberbezpečnosti.

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





5.8 Způsob a podíl zapojení jednotlivých účastníků do realizace projektu

Způsob a podíl zapojení jednotlivých účastníků do realizace projektu

Masarykova univerzita se na řešení projektu podílí sama. Řešitelský tým se skládá z pracovníků Fakulty informatiky, Právnické fakulty, Fakulty sociálních studií a Ústavu výpočetní techniky, kteří již mají zkušenosti s problematikou řešení projektů bezpečnostního výzkumu MV ČR a jsou schopni realizovat navrhovaný projekt se zohledněním požadavku na celostní a multioborový přístup k realizaci jednotlivých aktivit. Budou sestaveny specializované skupinky z řešitelů, kteří disponující patřičnými oborovými znalostmi nezbytnými k vyřešení dílčích cílů projektu. Jelikož je součástí projektu rovněž vytvoření technických výsledků v podobě databáze a software, budou řešitelé zajišťovat také technický návrh a vývoj s využitím existující infrastruktury Masarykovy univerzity.

Masarykova univerzita disponuje potřebným personálním a technologickým zázemím pro řešení projektu. V rámci univerzitního centra CERIT Scientific Cloud (CERIT-SC - OP VaVpI reg. č. CZ. 1.05/3.2.00/08.0144) bude poskytnuta výpočetní a síťová infrastruktura pro vývoj a testování vytvářeného software. Pilotní nasazení výsledků projektu bude provedeno řešitelským týmem s využitím infrastruktur Masarykovy univerzity. Výsledky projektu budou dále zpřístupněny uživatelům a široké veřejnosti s využitím vhodných licenčních nástrojů. Výsledky budou využity i přímo na straně Masarykovy univerzity jako podkladový materiál při návrhu a úpravách vzdělávacích programů v oblasti kyberbezpečnosti a to jak na úrovni vysokoškolských oborů tak v rámci multioborového profesního vzdělávání.

Při realizaci projektu budou využity rovněž rozsáhlé zkušenosti a kontakty řešitelů projektu na významné výzkumné a výkonné organizace v zahraničí, především bude využito mechanismů spolupráce a předávání informací s Univerzitou ve Vídni a výzkumným centrem AIT v Rakousku a s Národním institutem pro standardy a technologie a výzkumným centrem S2ERC v USA.

5.9 Intenzita podpory

Intenzita podpory - Masarykova univerzita / Fakulta informatiky

MU je výzkumná organizace a v souladu se zadávací dokumentací uplatňuje úhradu způsobilých nákladů ve výši 100 % způsobilých nákladů projektu.

5.10 Předpokládání uživatelé výsledků

Předpokládání uživatelé výsledků

Předpokládáními uživateli výsledků projektu jsou především orgány a osoby podle Zákona o kybernetické bezpečnosti č. 181/2014 Sb. Dále pak orgány veřejné moci vykonávající aktivity v oblasti kyberbezpečnosti, kybernetické obrany a kybernetické kriminality.

- Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. NÚKIB v souladu s dikcí zákona mimo jiné zajišťuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti a zpracovává a vládě ke schválení předkládá národní strategii kybernetické bezpečnosti. V rámci strategie a na ní navázaného akčního plánu pak NÚKIB mimo jiné navrhuje činnosti směřující k zajištění rozvoje vzdělávání v oblasti kyberbezpečnosti. NÚKIB tak výsledky projektu může využít pro realizaci těchto odpovědností a rovněž pro něj bude přínosem lepší dostupnost pracovní síly v oblasti kyberbezpečnosti.
- Ministerstvo obrany – v rámci resortu MO je Vojenské zpravodajství pověřeno budováním Národního centra kybernetických sil a tomu odpovídajícím úkolům z Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. Další prvek kybernetické bezpečnosti resortu MO tvoří Centrum CIRC. Jeho úkolem je proaktivní identifikace bezpečnostních hrozeb a incidentů, jejich analýza a následné reportování zjištěných událostí a postupů řešení k relevantním partnerům. Podobně jako další ústřední orgány státní správy, i MO vyjádřilo zájem o rozšíření dostupnosti pracovních sil v oblasti kyberbezpečnosti a o podporu při jejich budování a nábore.
- Policie ČR – policie ČR v rámci svojí působnosti realizuje vyšetřování kybernetické kriminality a nakládá s elektronickými důkazy, pro tyto aktivity musí být nebytně vybavena odbornými kapacitami schopnými orientace v oblasti kyberbezpečnosti a nakládání s informačními a komunikačními technologiemi při zajišťování důkazů a vyšetřování trestné činnosti. Policie rovněž realizuje vzdělávání a nábor pracovníků pro potřeby centrálních a detašovaných pracovišť se zaměřením a počítačovou kriminalitu. Výsledky projektu tak bude moci využít nejen ke specifikaci pracovní náplně a výběru pracovníků, ale rovněž k sestavování plánu vzdělávání a spolupráci na vzdělávání s akademickými institucemi.
- Provozovatelé kritických informačních infrastruktur – povinné osoby provozující informační infrastruktury ve smyslu zákona o kybernetické bezpečnosti mají povinnost zajistit personální kapacity pro realizaci povinností vyplývajících ze zákona z dalších českých a evropských právních předpisů, především za účelem detekce bezpečnostních událostí, řešení incidentů, ochrany svých infrastruktur a spolupráce s ústředními orgány

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS

PID: VI3VS/710

Hlavní obor: IN

Stupeň důvěrnosti: S

Předpokládání uživatelé výsledků

státní správy v oblasti kyberbezpečnosti. Zvýšení dostupnosti pracovních sil v kyberbezpečnosti tak bude významným prvkem podporujícím ochranu významných a kritických infrastruktur a kvalifikaci pracovníků, kteří ji zajišťují.

- Vzdělávací instituce – vzdělávací instituce na všech úrovních vzdělávání i komerční poskytovatelé školení a cvičení využijí výsledky výzkumu k návrhům a úpravě svých vzdělávacích aktivit a produktů za účelem produkce odborníků v kyberbezpečnosti. Dobrý přehled o dostupnosti pracovníků v jednotlivých kvalifikacích i náplň jejich práce a rozsah znalostí, schopností a dovedností bude sloužit jako silný nástroj k efektivnímu zaměření příslušných vzdělávacích produktů.

Výsledky projektu budou využitelné i dalšími organizacemi a firmami řešícími problematiku kybernetické bezpečnosti a bezpečnostního výzkumu. Cílem uchazeče je vytvořit a dále rozvíjet plánované výsledky tak, aby mohly být jednoduše využity třetími stranami.

Výsledky budou zpřístupněny tak, aby jejich využívání nebylo v rozporu se zájmy České republiky a negativně neovlivňovalo bezpečnost České republiky a jejích občanů.

5.11 Projekt počítá se subdodávkami

Projekt počítá se subdodávkami

NE

5.12 Harmonogram projektu

Název činnosti	Uchazeč	Období, kdy je činnost uskutečňována											
		1	2	3	4	5	6	7	8	9	10	11	12
Rok 2019													
1.1 Analýza potřebných kvalifikací v kyberbezpečnosti v ČR Tato aktivita bude směřovat k získání uceleného přehledu o kvalifikacích v kybernetické bezpečnosti uplatnitelných nebo potřebných na českém pracovním trhu. Metodou práce bude desk research zaměřený na dostupné podklady v ČR i v zahraničí.	Masarykova univerzita / Fakulta informatiky							X	X	X	X	X	X
1.2 Desk research - sběr a analýza výzkumných výsledků a metodik V této aktivitě budou především ze zahraničních zdrojů sesbírány výzkumné výsledky, metodiky, best practices a další podklady potřebné pro vhodné zacílení výzkumných aktivit projektu a jeho výsledků.	Masarykova univerzita / Fakulta informatiky							X	X	X	X	X	X
1.3 Návrh klasifikace a třídění jednotlivých kvalifikací taxonomie V rámci této aktivity bude navržena struktura taxonomie a třídění jednotlivých kvalifikací do kategorií činností a specializací.	Masarykova univerzita / Fakulta informatiky							X	X	X	X	X	X
1.4 Průzkum trhu se vzděláváním v oblasti kyberbezpečnosti v ČR V této aktivitě bude proveden úvodní průzkum trhu se vzděláváním v kybernetické bezpečnosti v ČR, který bude dvouetapový, přičemž v první etapě v prvním roce bude probíhat sběr dat a v druhém jejich vyhodnocení.	Masarykova univerzita / Fakulta informatiky							X	X	X	X	X	X
1.5 Návrh designu software pro práci s rámcem kvalifikací V této aktivitě bude zvolena technologie a formulovány požadavky na funkcionalitu softwarového nástroje pro práci s Rámcem kvalifikací tak, aby reflektoval požadavky a potřeby cílových skupin a uživatelů výsledků.	Masarykova univerzita / Fakulta informatiky											X	X
Rok 2020													
2.1 Dotazníkový průzkum realizovaný u relevantních organizací Za účelem vhodného zacílení výsledků bude v této aktivitě realizován dotazníkový průzkum u relevantních státních i nestátních organizací zaměřený na získání informací o požadavcích na strukturu a odbornost potřebné pracovní síly v kyberbezpečnosti.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X	X	X	X	X	X	X
2.2 Identifikace potřebných kvalifikací v kyberbezpečnosti v ČR Na základě informací získaných v rešeršní fázi projektu bude sestavena struktura kvalifikací potřebných pro pokrytí aktuální i predikované potřeby po odborné síle v ČR.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X	X	X	X	X	X	X
2.3 Identifikace znalostí a zkušeností kvalifikací taxonomie V rámci této aktivity budou analyzovány požadavky na vzdělání, znalosti a schopnosti požadované pro pracovníků v jednotlivých kvalifikacích/rolích, tyto požadavky identifikovány a zahrnuty do Rámce.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X	X	X	X	X	X	X
2.4 Návrh funkcí software pro práci s rámcem kvalifikací Na základě funkčních požadavků na software pro práci s Rámcem bude v této etapě probíhat návrh konkrétních funkcí a jejich technické parametry po potřeby vývoje software.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X						
2.5 Návrh popisu jednotlivých kvalifikací taxonomie V této aktivitě bude navržen popis charakteru jednotlivých kvalifikací/rolí zahrnutých v taxonomii, který stručně informuje o povaze kvalifikace a očekávaných aktivitách pracovníků ji vykonávajících.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X						
2.6 Vyhodnocení průzkumu trhu se vzděláváním V této aktivitě bude proveden úvodní průzkum trhu se vzděláváním v kybernetické bezpečnosti v ČR, který bude dvouetapový, přičemž v první etapě v prvním roce bude probíhat sběr dat a v druhém jejich vyhodnocení.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X						
2.7 Vývoj software pro práci s rámcem kvalifikací V této etapě bude zahájen vývoj základní struktury software pro práci s Rámcem.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X	X	X	X	X	X	X
2.8 Výzkum dostupné pracovní síly v oblasti kyberbezpečnosti Prostřednictvím průzkumu trhu práce v oblasti kyberbezpečnosti, dotazníkového šetření a analýzy literatury bude proveden výzkum nabídky a poptávky na pracovním trhu v oblasti kyberbezpečnosti, který bude sloužit pro sestavení Rámce a Akčního plánu.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X	X	X	X	X	X	X
2.9 Detailní průzkum dostupného vzdělávání v kyberbezpečnosti V této víceetapové aktivitě bude realizován ve spolupráci se vzdělávacími institucemi průzkum dostupného vzdělávání v kyberbezpečnosti se zaměřením na identifikaci bílých míst. Na závěr detailního průzkumu bude navrženo vhodné rozšíření nabídky vzdělávání	Masarykova univerzita / Fakulta informatiky							X	X	X	X	X	X
2.10 Identifikace rozsahu vzdělání nutného k dosažení kvalifikace	Masarykova univerzita / Fakulta informatiky							X	X	X	X	X	X

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS

PID: VI3VS/710

Hlavní obor: IN

Stupeň důvěrnosti: S

Název činnosti	Uchazeč	Období, kdy je činnost uskutečňována											
		1	2	3	4	5	6	7	8	9	10	11	12
V této víceetapové aktivitě bude na základě výzkumných aktivit projektu identifikován požadavek na vzdělání a charakter pracovníků zastupujících jednotlivé kvalifikace/role. Výsledky budou zahrnuty v Rámci.													
Rok 2021													
3.1 Detailní průzkum dostupného vzdělávání v kyberbezpečnosti V této víceetapové aktivitě bude realizován ve spolupráci se vzdělávacími institucemi průzkum dostupného vzdělávání v kyberbezpečnosti se zaměřením na identifikaci bílých míst. Na závěr detailního průzkumu bude navrženo vhodné rozšíření nabídky vzdělávání	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X	X	X	X	X	X	X
3.2 Identifikace úrovně vzdělání nutného k dosažení kvalifikace V této víceetapové aktivitě bude na základě výzkumných aktivit projektu identifikován požadavek na vzdělání a charakter pracovníků zastupujících jednotlivé kvalifikace/role. Výsledky budou zahrnuty v Rámci.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X	X	X	X	X	X	X
3.3 Implementace a testování software V této aktivitě, která představuje závěrečnou fázi vývoje software pro práci s Rámcem a taxonomií, bude realizována implementace a testování software za účelem přípravy jeho zveřejnění.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X	X	X	X	X	X	X
3.4 Návrh struktury a obsahu Rámce kvalifikací Na základě předchozího výzkumu bude v této aktivitě navržena struktura a obsahové náležitosti Rámce kvalifikací a konzultace návrhu s potenciálními uživateli a cílovými skupinami.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X	X	X	X	X	X	X
3.5 Popis potřebných kvalifikací v kyberbezpečnosti v ČR V této aktivitě bude navržen detailnější popis jednotlivých kvalifikací/rolí v taxonomii a jejich vazby na vzdělání, dovednosti a schopnosti.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X						
3.6 Sestavení návrhu Rámce kvalifikací a konzultace s uživateli V této aktivitě bude na základě navržené struktury a obsahových náležitostí rámce prováděno jeho plnění ve vztahu k jednotlivým kvalifikacím/rolím. Bude probíhat průběžná konzultace navrženého obsahu s uživateli, a průběžně prováděny potřebné úpravy.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X	X	X	X	X	X	X
3.7 Výzkum úrovně kvalifikace v oblasti kyberbezpečnosti Současně s konstrukcí a naplňováním rámce, bude prováděn výzkum aktuální úrovně kvalifikace jednotlivých identifikovaných rolí v praxi a gap analýza navrhovaných kvalifikací a zavedené praxe. Výsledky budou využívány k úpravě Rámce a návrhu Akčního plánu	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X						
3.8 Návrh mechanismu podpory vzdělávání v oblasti kyberbezpečnosti Pro potřeby akčního plánu bude v této etapě proveden průzkum dostupných motivačních nástrojů pro rozšíření vzdělávání a vyplnění nedostatečně pokrytých kurzů a oborů a navržena jejich implementace na úrovni ČR.	Masarykova univerzita / Fakulta informatiky							X	X	X	X	X	X
Rok 2022													
4.1 Identifikace mezer v dostupném vzdělání na základě průzkumu Na základě provedeného průzkumu dostupného vzdělávání budou identifikovány nedostatky v rozsahu nebo formě vzdělávání a navrženo rozšíření nabídky oborů a kurzů pro pokrytí poptávky vyplývající z Rámce kvalifikací.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X						
4.2 Návrh akčního plánu budování pracovní síly v kyberbezpečnosti V této aktivitě bude na základě předchozích výzkumných kroků a analýzy dostupného vzdělávání a pracovních sil navržen mechanismus podpory vzdělávání v oblasti kyberbezpečnosti za účelem vyplnění identifikovaných mezer a sladění Rámce s dostupnou nabídkou.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X						
4.3 Provedení potřebných úprav v návrhu Rámce kvalifikací V této aktivitě bude na základě navržené struktury a obsahových náležitostí rámce prováděno jeho plnění ve vztahu k jednotlivým kvalifikacím/rolím. Bude probíhat průběžná konzultace navrženého obsahu s uživateli, a průběžně prováděny potřebné úpravy.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X						
4.4 Publikace software pro práci s rámcem kvalifikací V této etapě bude publikován software pro práci s Rámcem a Taxonomií.	Masarykova univerzita / Fakulta informatiky	X	X	X	X	X	X						
4.5 Sestavení vzorové kvalifikace a testování Bude vybrána jedna nebo více kvalifikací, která bude ve spolupráci s uživatelem/uživateli testována v reálném prostředí příslušné organizace z hlediska její využitelnosti pro výběr a hodnocení pracovníků a volby dodatečného vzdělávání.	Masarykova univerzita / Fakulta informatiky	X	X	X									

5.13 Popis rizik projektu a jejich řízení

Popis rizik projektu a jejich řízení

Riziko, že navržené postupy a technická řešení nepovedou k dosažení výsledků s očekávanými parametry

Pravděpodobnost: nízká

Závažnost: vysoká

Opatření: Všechny výsledky byly diskutovány s klíčovými osobami řešitelského týmu, kteří mají dlouhodobé zkušenosti v řešené oblasti. Harmonogram projektu obsahuje etapy vývoje zakončené testovacími a integračními etapami, na nichž bude ověřována dosažitelnost výsledků.

Riziko nesprávného odhadu návaznosti aktivit a délky jejich trvání

Pravděpodobnost: nízká

Závažnost: střední

Opatření: Bylo provedeno několik expertních odhadů délky trvání jednotlivých aktivit a jejich návazností. Výsledky byly opakovaně diskutovány a upravovány do stávajícího stavu. Členové řešitelského týmu odpovědní za plánování a řízení projektu jsou proškoleni v projektovém řízení a mají také dostatečné zkušenosti s plánováním a realizací projektů.

Riziko nesprávně odhadnuté náročnosti aktivit projektu

Pravděpodobnost: nízká

Závažnost: střední

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS

PID: VI3VS/710

Hlavní obor: IN

Stupeň důvěrnosti: S

Popis rizik projektu a jejich řízení

Opatření: Bylo provedeno několik expertních odhadů náročnosti aktivit, které byly porovnány a následně dle nich byly nastaveny finální hodnoty. Dále byly aktivity, u kterých hrozí zvýšená náročnost, umístěny v harmonogramu tak, aby prodloužení jejich řešení nezpůsobilo komplikace s realizací výstupů projektu.

Riziko nezájmu potenciálních uživatelů o výstupy projektu a věcné konzultace ke směřování projektu

Pravděpodobnost: nízká

Závažnost: vysoká

Opatření: Zájem potenciálních uživatelů byl prověřen v předcházejících aktivitách a projektech realizovaných uchazečem. Je rovněž vyjádřen v přiloženém dopise vyjadřujícím podporu projektu. Riziko je dále minimalizováno dlouhodobě probíhající spoluprací s uživateli.

Riziko výpadku, přetížení a fluktuace specializovaných zaměstnanců

Pravděpodobnost: střední

Závažnost: nízká

Opatření: Řešitelský tým je sestaven, aby klíčové pozice byly obsaditelné několika členy týmu. Je kladen důraz na sdílení znalostí. Proto je možné vykrytí krátkodobý výpadek jednoho z nich jiným členem týmu. Řešitelský tým má rovněž zkušenosti se získáváním a školením vysoce kvalifikovaných výzkumných a vývojových pracovníků z řad absolventů bakalářského, magisterského a doktorského studia. Je tak možné nahradit zaměstnance při jeho dlouhodobém výpadku nebo odchodu z organizace.

5.14 Doplnující informace k projektu

Doplnující informace k projektu

NÚKIB jako ústřední správní orgán odpovědný za kyberbezpečnost potvrdil formou přiloženého dopisu zájem aktivně spolupracovat a dosáhnout slíbených výsledků projektu.

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS

PID: VI3VS/710

Hlavní obor: IN

Stupeň důvěrnosti: S

6. Financování a náklady projektu

6.1 Výše státní podpory projektu podle jednotlivých uchazečů

Uchazeč	Rok	Způsobilé náklady projektu (tis. Kč)	Z toho vlastní zdroje (tis. Kč)	Požadovaná státní podpora (tis. Kč)	Intenzita podpory (%)
Masarykova univerzita / Fakulta informatiky	Celkem	8 748.95	0	8 748.95	100
	2019	1 382.92	0	1 382.92	100
	2020	3 065.03	0	3 065.03	100
	2021	2 966.99	0	2 966.99	100
	2022	1 334.01	0	1 334.01	100
PROJEKT	Celkem	8 748.95	0	8 748.95	100

6.2 Rozpočet projektu

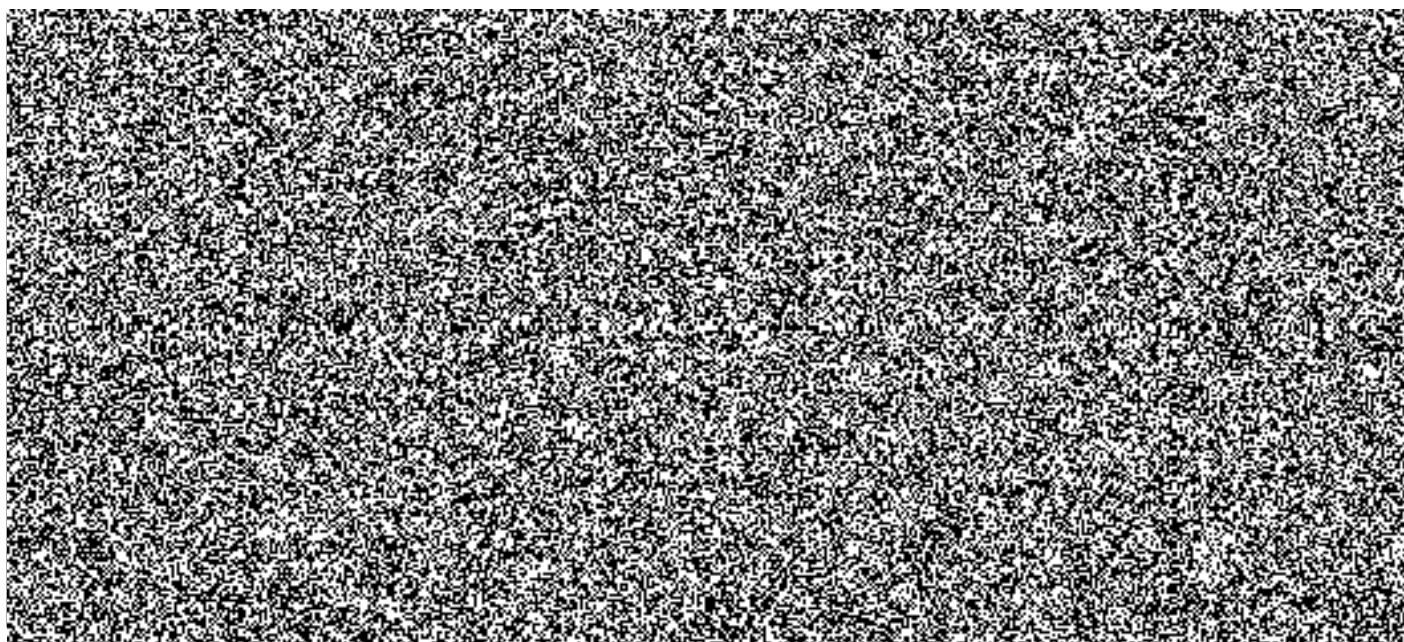
6.2.1 Výpočet maximální míry podpory uchazeče Masarykova univerzita / Fakulta informatiky

Kategorie uchazeče	výzkumná organizace
Kategorie výzkumu	experimentální vývoj
Způsobilé náklady uchazeče (tis. Kč)	8 748.95

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

Základní intenzita podpory (%)	25.00
Bonus (%)	75.00
Maximální intenzita podpory (%)	100.00
Maximální výše podpory (tis. Kč)	8 748.95

6.2.2 Náklady na mzdy/platy uchazeče Masarykova univerzita / Fakulta informatiky



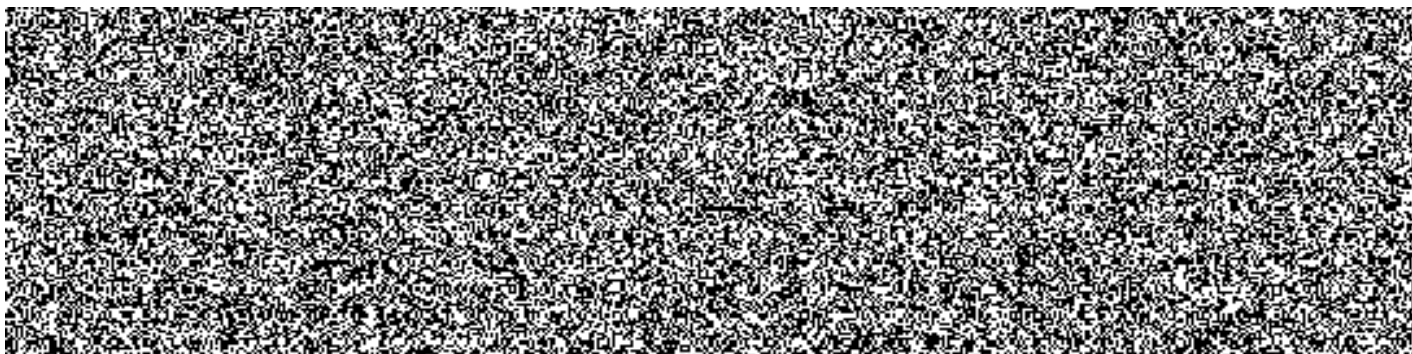
Žádost o poskytnutí účelové podpory

Program: BV III/1-VS

PID: VI3VS/710

Hlavní obor: IN

Stupeň důvěrnosti: S



6.2.3 Náklady uchazeče Masarykova univerzita / Fakulta informatiky na pořízení majetku

6.2.4 Rozpočet nákladů uchazeče Masarykova univerzita / Fakulta informatiky

Náklady/výdaje uchazeče (tis. Kč)	2019	2020	2021	2022	Celkem
Osobní náklady/výdaje - mezisoučet	1 128.46	2 501.06	2 421.06	988.55	7 039.13
a) mzdy/platy na základě pracovního poměru	776.63	1 793.38	1 793.38	732.26	5 095.65
b) osobní náklady/výdaje na základě dohody o pracovní činnosti	0	0	0	0	0
c) osobní náklady/výdaje na základě dohody o provedení práce	0	0	0	0	0
d) povinné pojistné na sociální zabezpečení	194.16	448.35	448.35	183.07	1 273.93
e) povinné pojistné na zdravotní pojištění	69.9	161.4	161.4	65.9	458.6
f) odvody do FKSP nebo sociálního fondu	7.77	17.93	17.93	7.32	50.95
g) cestovné	80	80	0	0	160
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	100	100
a) subdodávky	0	0	0	0	0
b) ostatní služby	0	0	0	100	100
Audit	0	0	0	100	100
Doplňkové náklady/výdaje - mezisoučet	254.46	563.97	545.93	245.46	1 609.82
Režie 18,4%	254.46	563.97	545.93	245.46	1 609.82
Celkové způsobilé náklady - mezisoučet	1 382.92	3 065.03	2 966.99	1 334.01	8 748.95
Celková státní podpora - mezisoučet	1 382.92	3 065.03	2 966.99	1 334.01	8 748.95

6.2.5 Rozpočet nákladů za celý projekt

Náklady/výdaje za celý projekt (tis. Kč)	2019	2020	2021	2022	Celkem
Osobní náklady/výdaje	1 128.46	2 501.06	2 421.06	988.55	7 039.13
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	100	100
Doplňkové náklady/výdaje	254.46	563.97	545.93	245.46	1 609.82
Celkové způsobilé náklady	1 382.92	3 065.03	2 966.99	1 334.01	8 748.95
Celková státní podpora	1 382.92	3 065.03	2 966.99	1 334.01	8 748.95

Žádost o poskytnutí účelové podpory

Program: BV III/1-VS

PID: VI3VS/710

Hlavní obor: IN

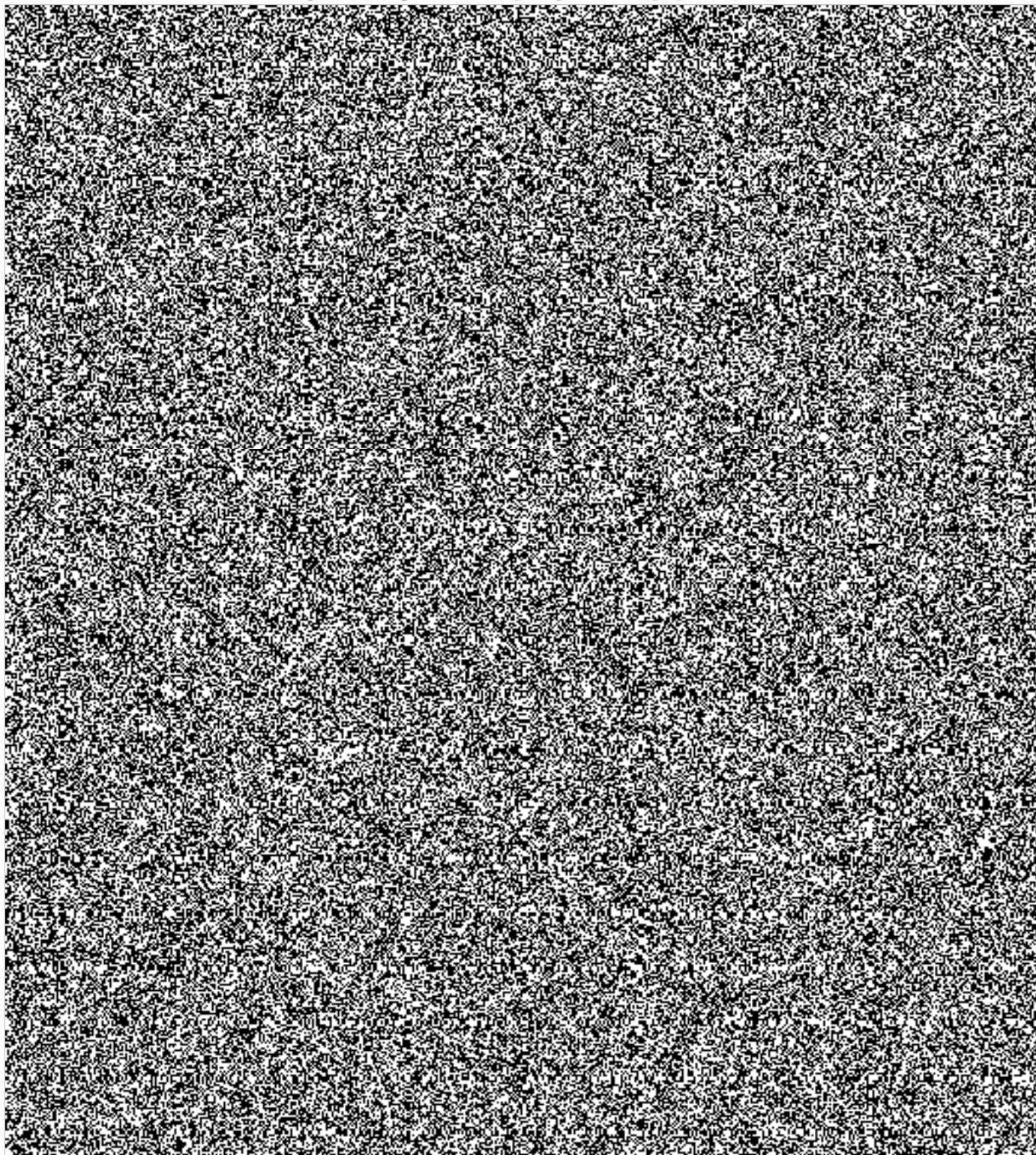
Stupeň důvěrnosti: S

Souhlas statutárního zástupce uchazeče Masarykova univerzita / Fakulta informatiky 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 doc. PhDr.	Jméno Mikuláš	Příjmení Bek	Titul za jménem Ph.D.	Podpis
---------------------------------	------------------	-----------------	--------------------------	--------

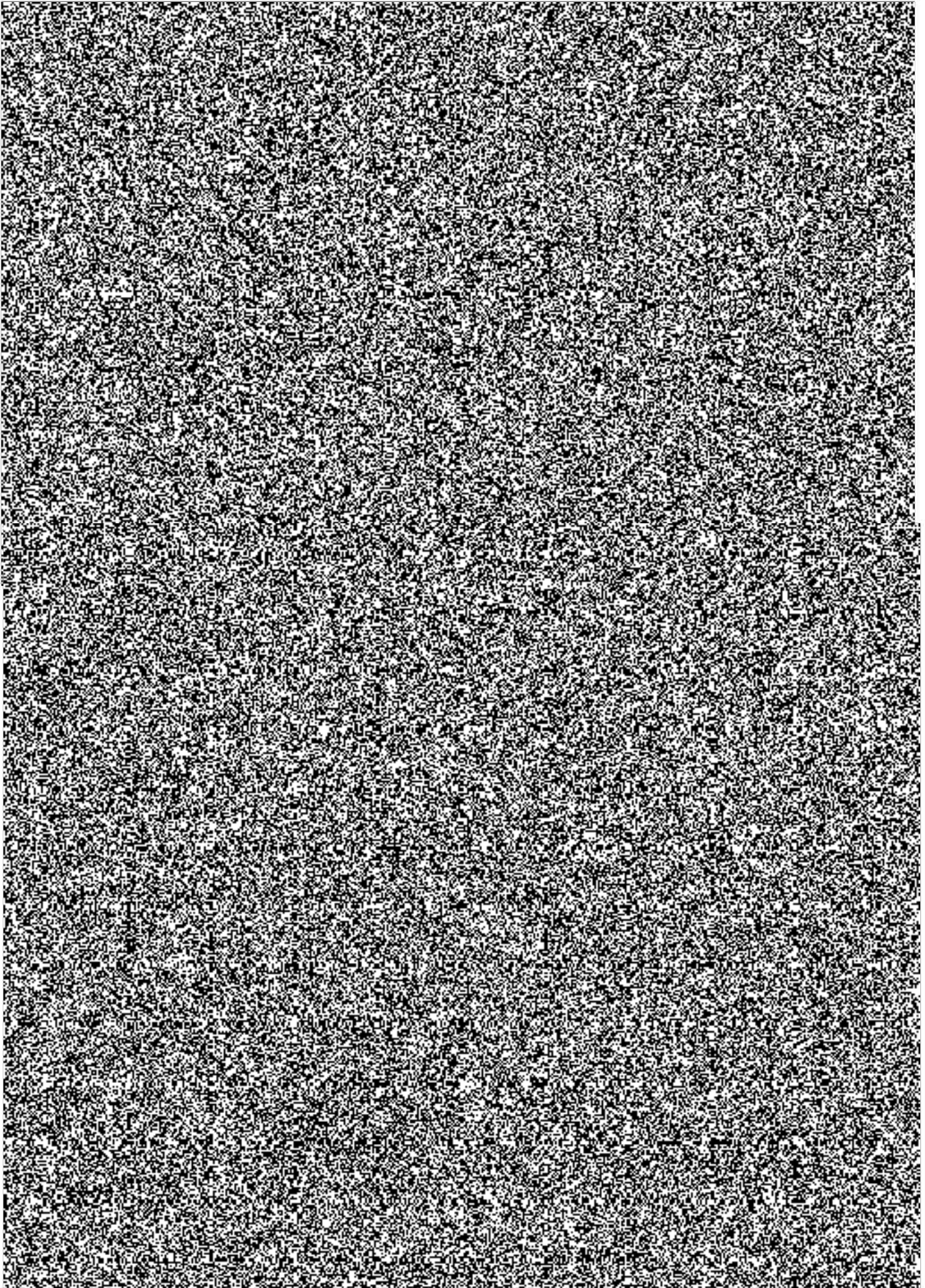
Plán využití výsledků projektu a jejich popis²

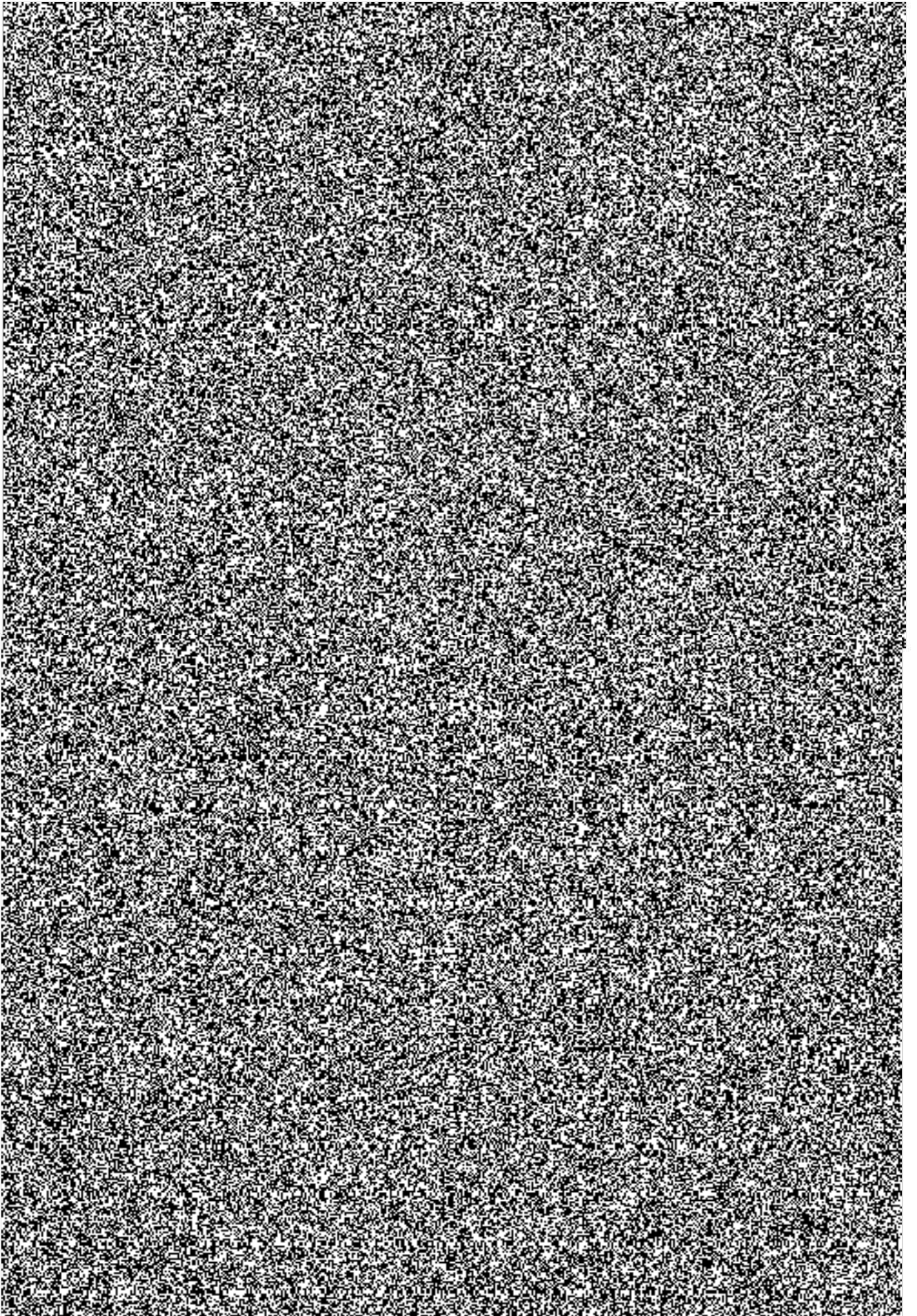


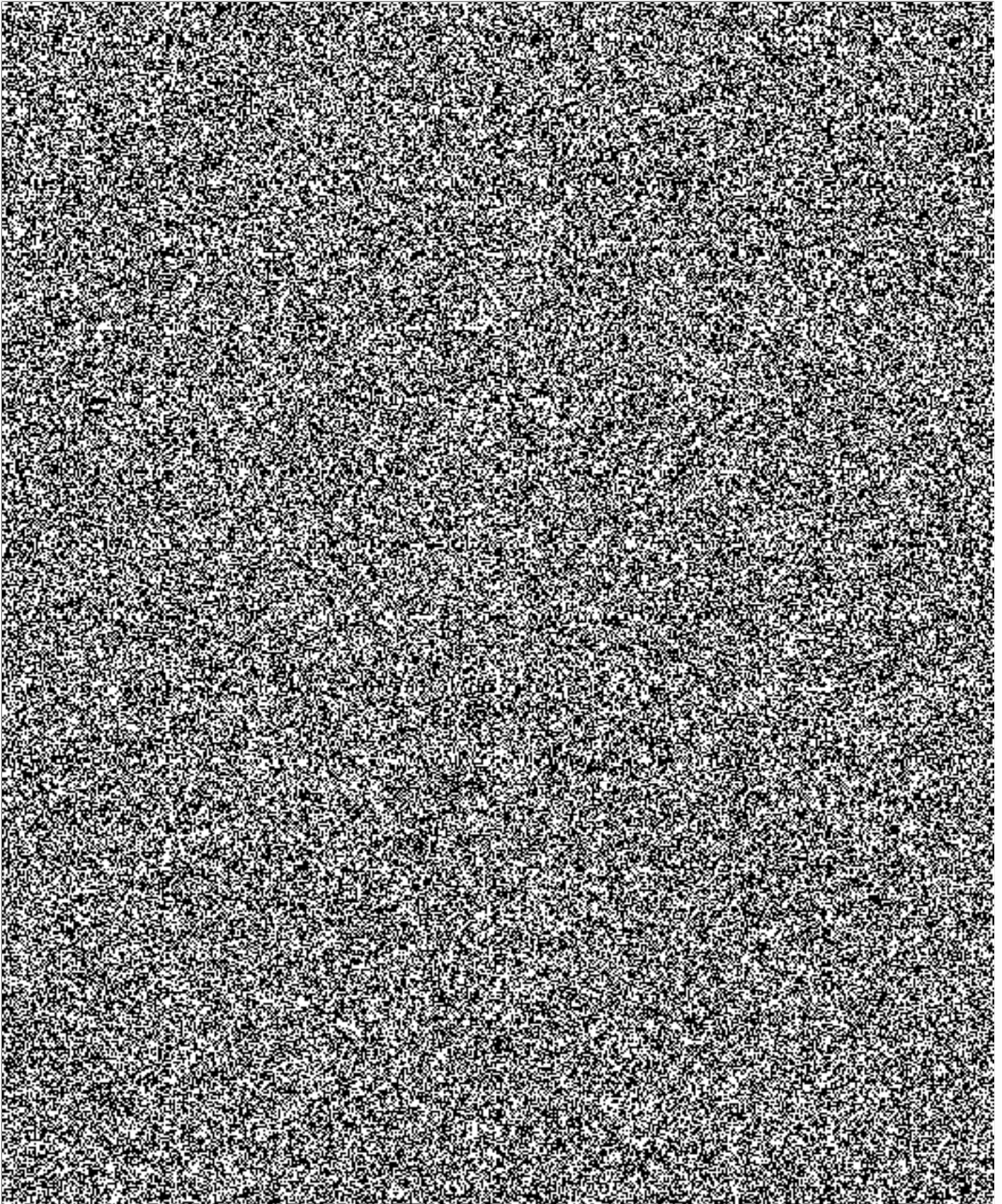
*) Uchazeč záhlaví vyplní, nehodící se škrtněte

¹ Uchazeč list vyplní, aktualizuje Počet listů

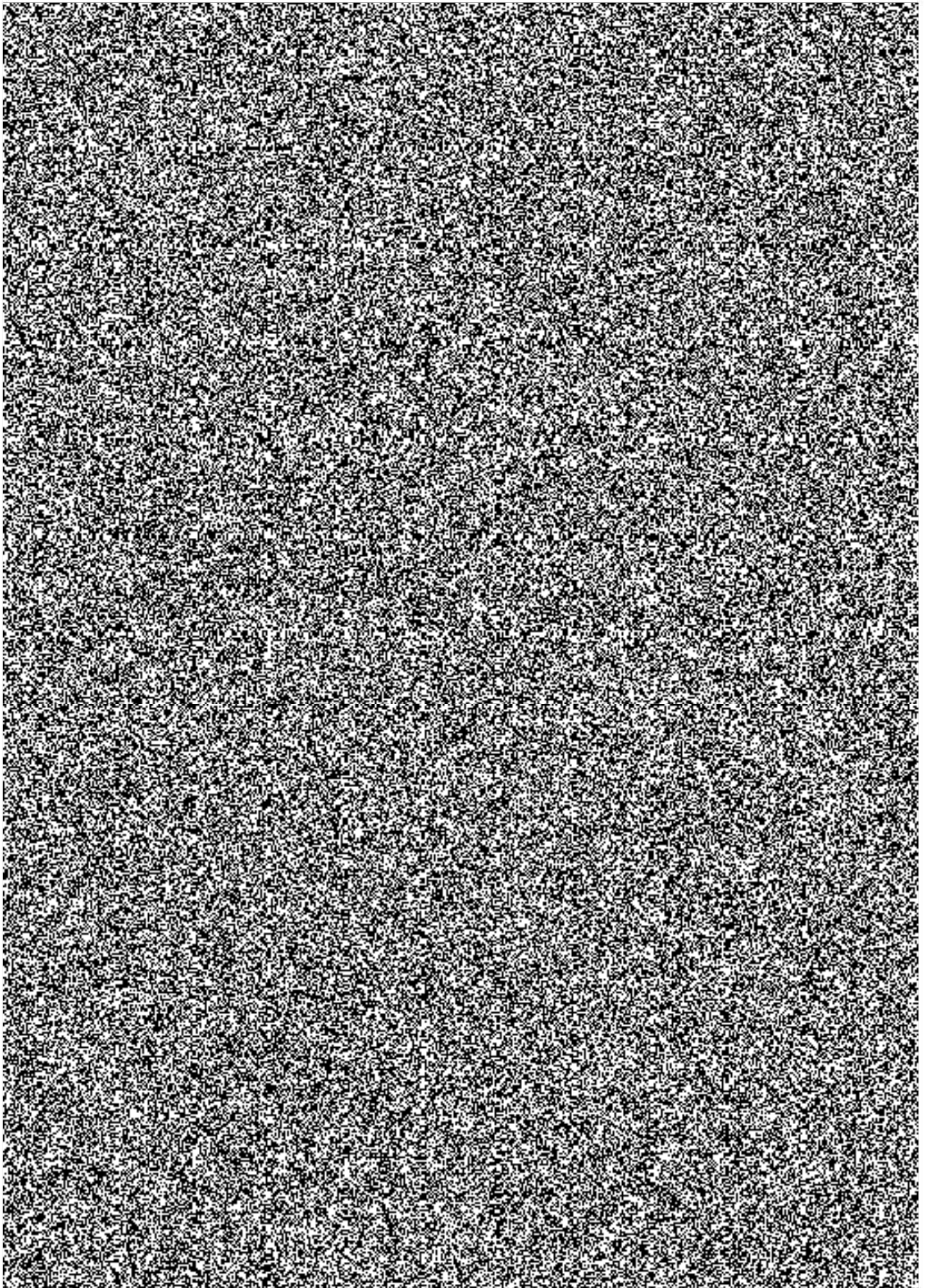
² Povinná příloha pro všechny uchazeče, v případě, že projekt podává více uchazečů, předkládá koordinátor

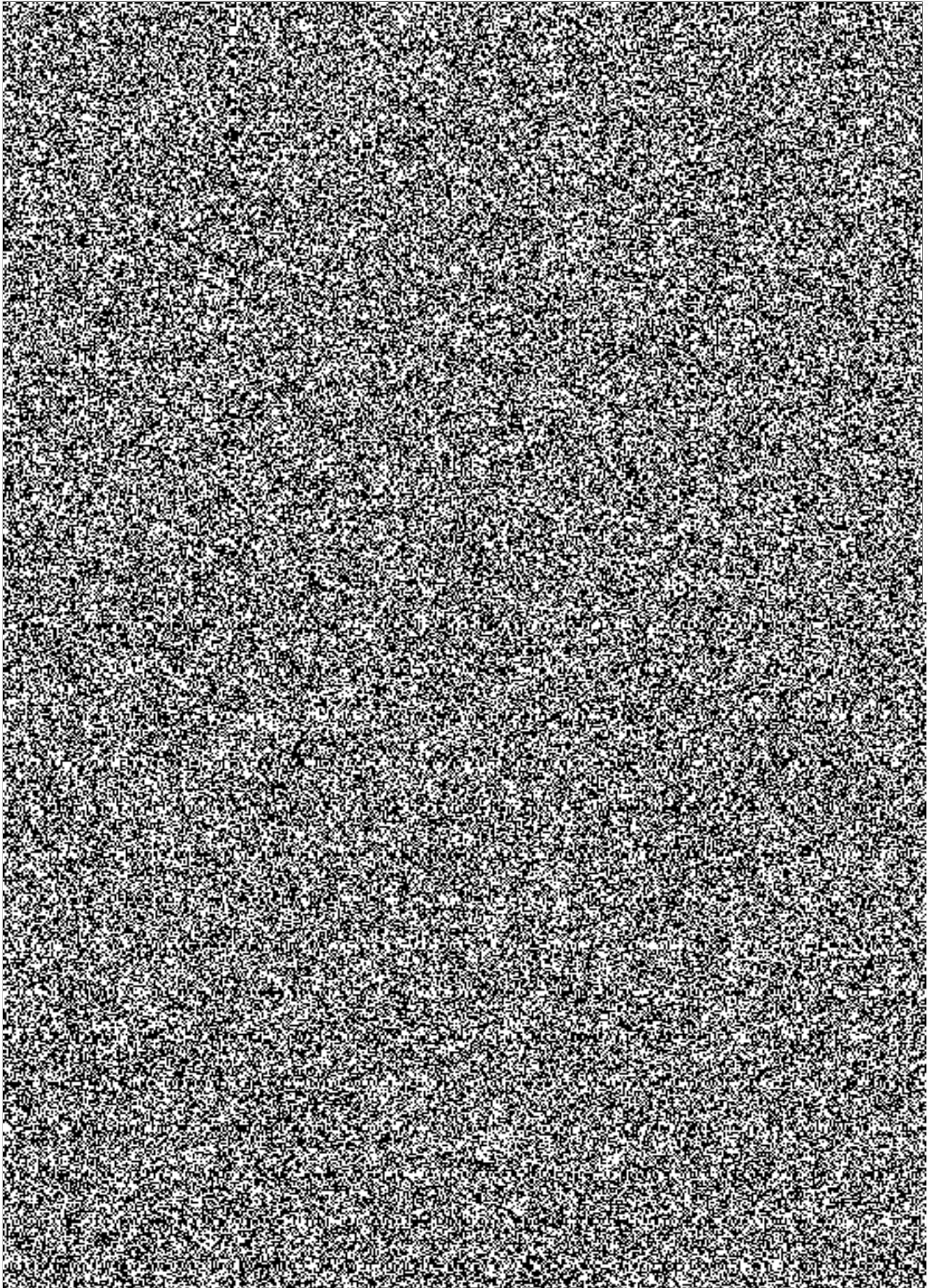




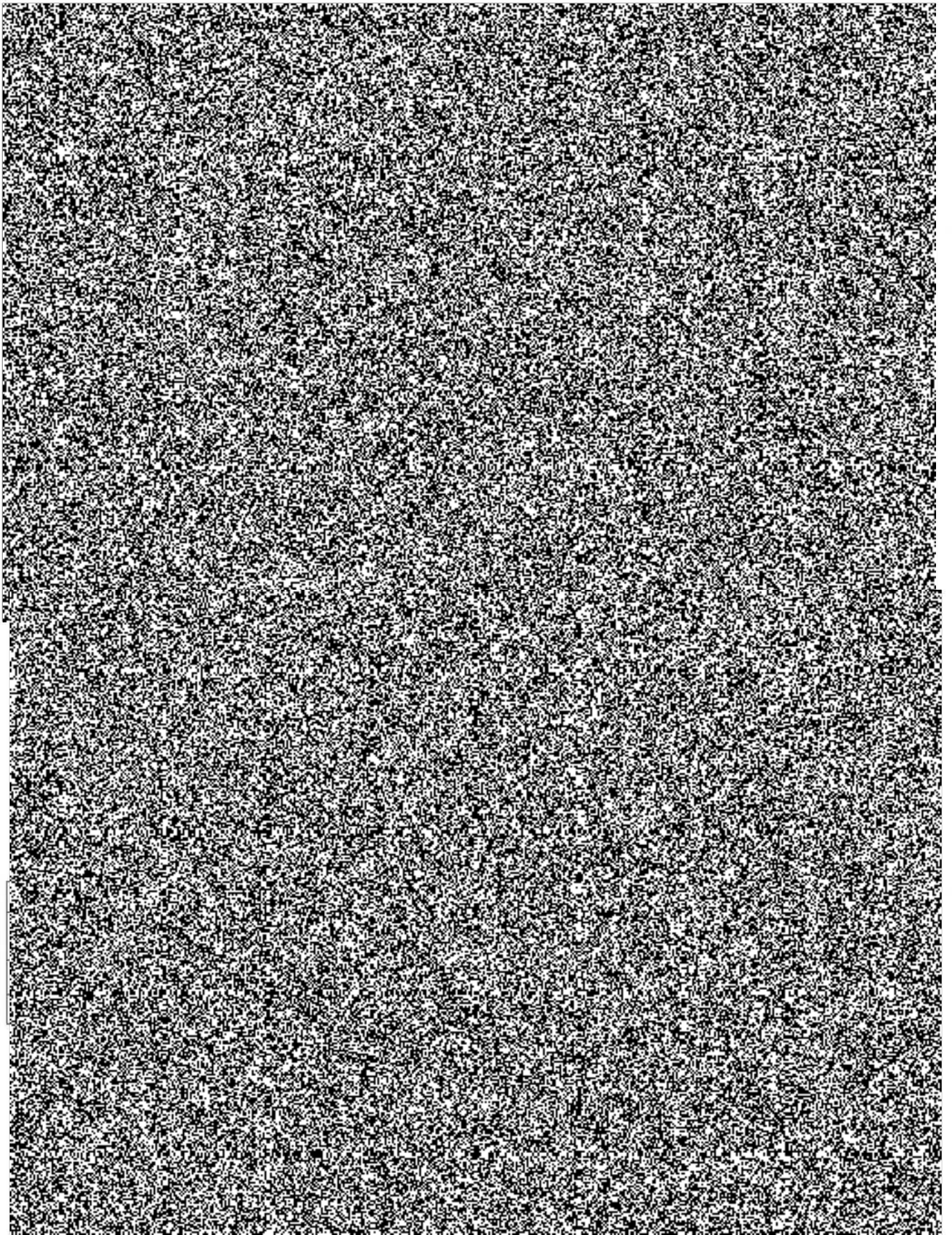


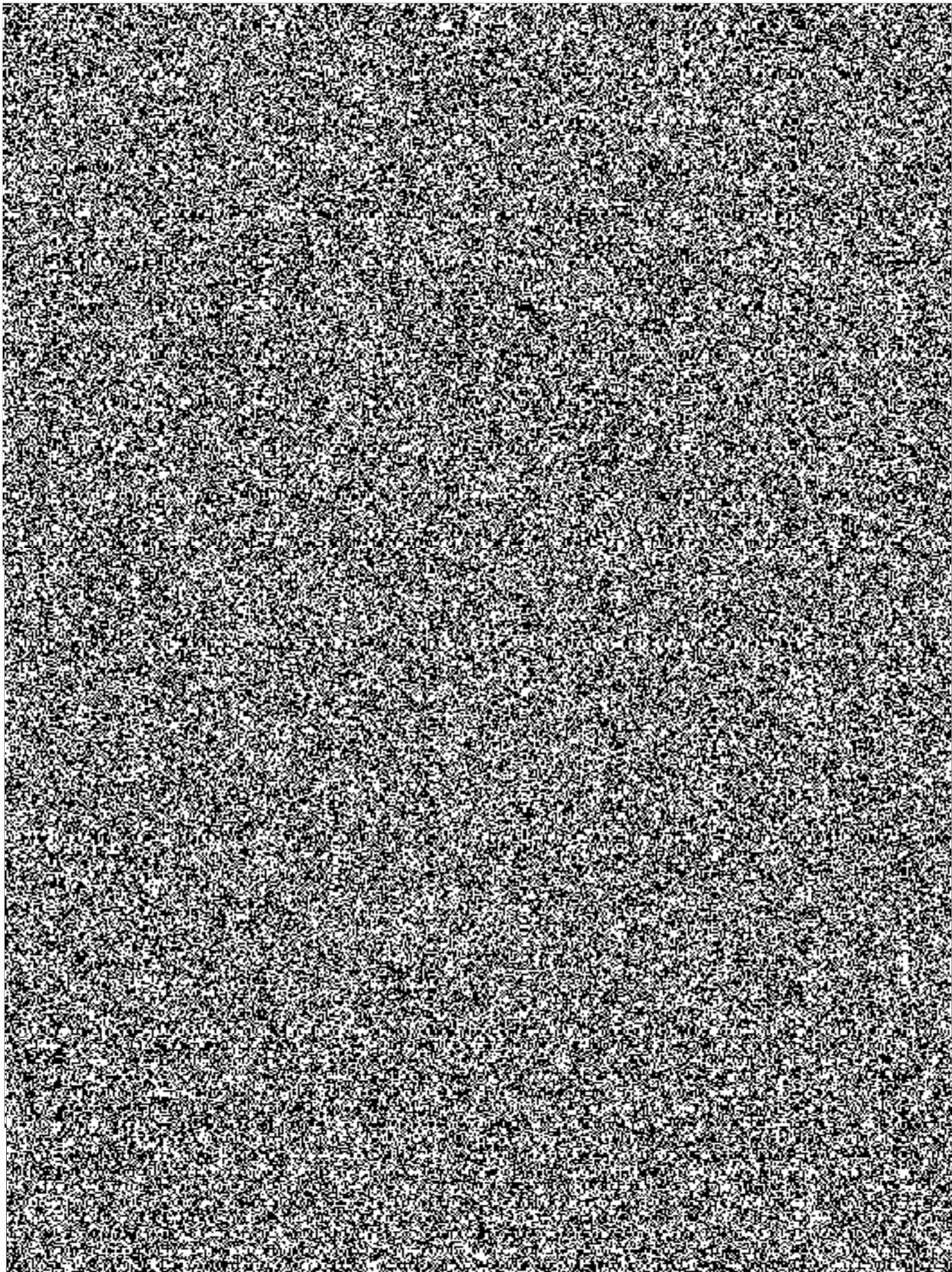
³ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)



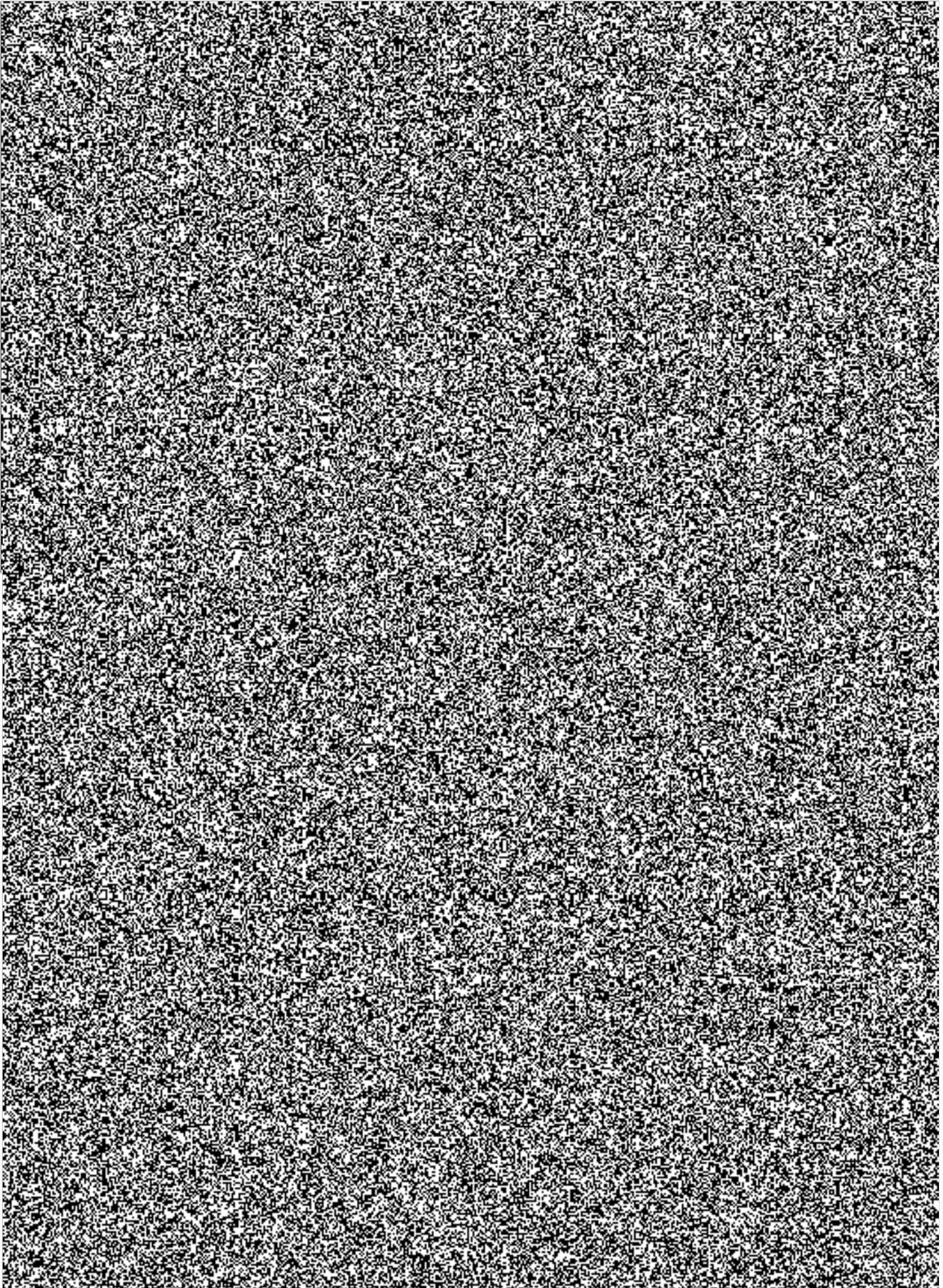


⁴ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)





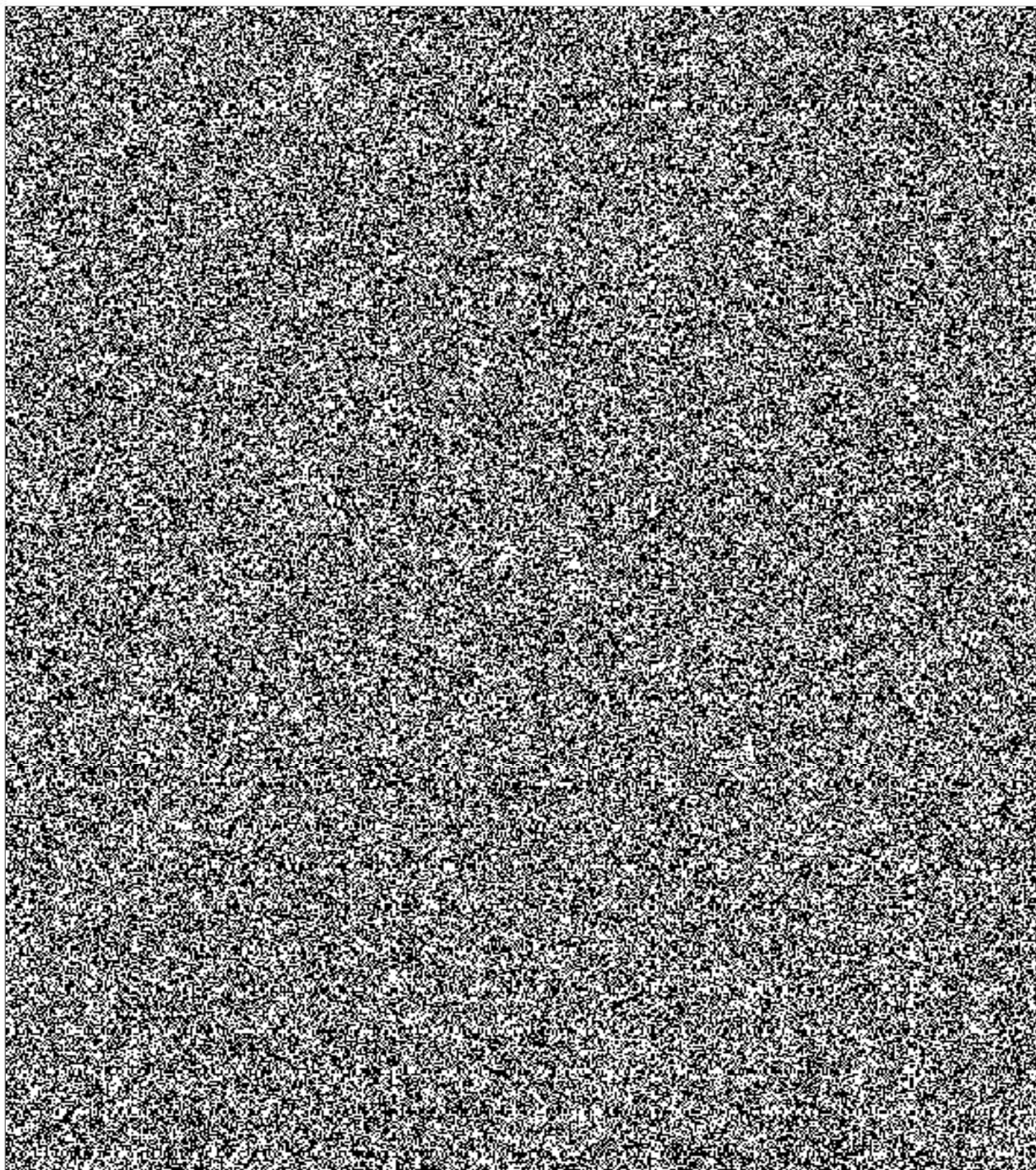
⁵ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)



soukromoprávních organizací i veřejnosti, zpřístupňovat systematicky zařazené a prezentované informace ke kvalifikacím v kyberbezpečnosti, o nabídce vzdělávání v dané oblasti.

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

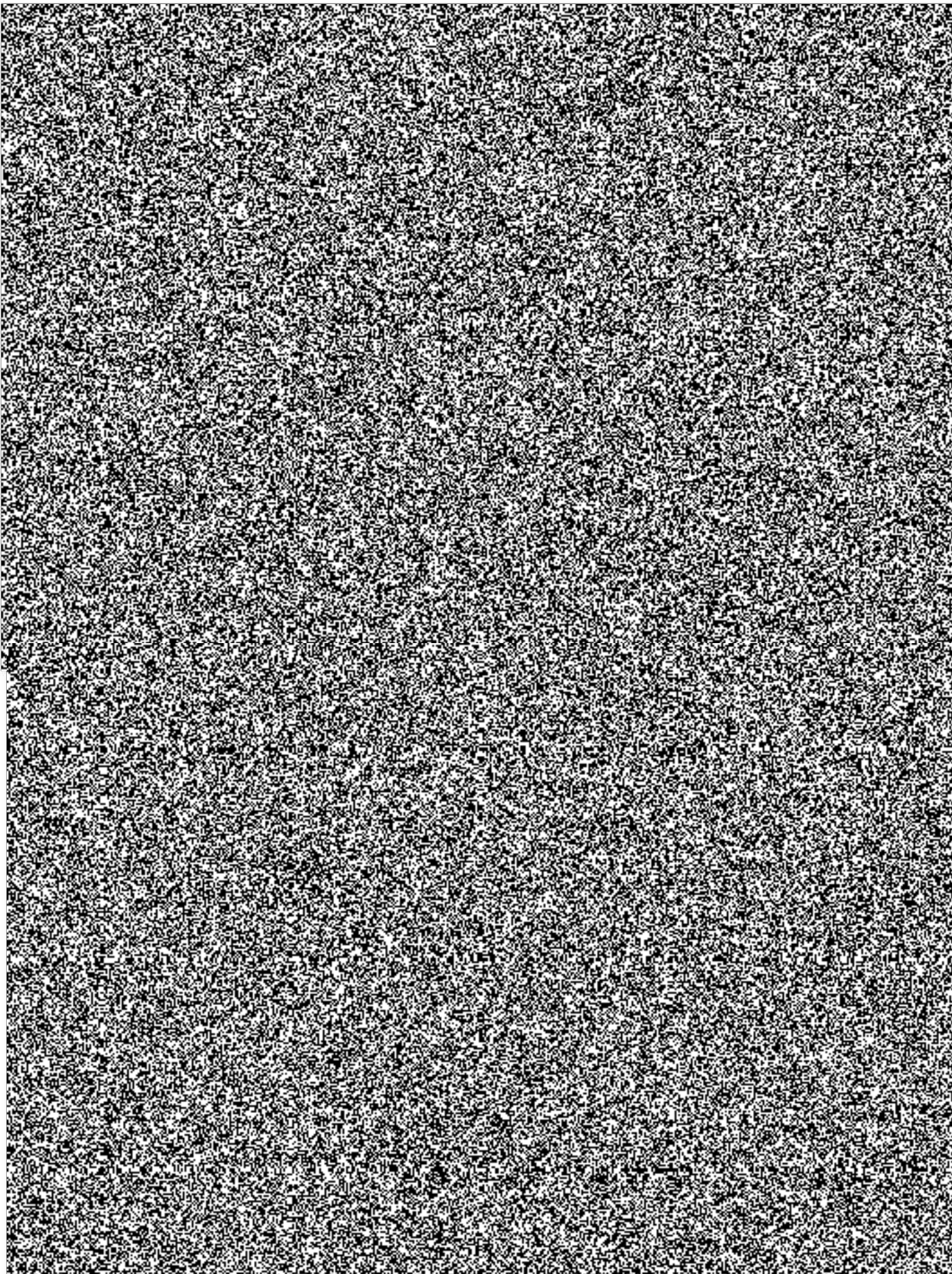
Metodika 2013 (zadávací dokumentace + elektronická přihláška)		Metodika 2017+	
název výsledku	kód výsledku	název výsledku	kód výsledku
patent	P	patent	P
software	R	software	R
výsledky s právní ochranou - užítý vzor, průmyslový vzor	F	speciálovaná veřejná databáze	S
poloprovoz, ověřená technologie	Z	užitý vzor	F _{uzi}
technicky realizované výsledky - prototyp, funkční vzorek	G	průmyslový vzor	F _{prum}
metodika	N	poloprovoz	Z _{polip}
		ověřená technologie	Z _{tech}
		prototyp	G _{prot}
		funkční vzorek	G _{funk}
metodiky schválené příslušným orgánem státní správy, do jehož kompetence daná problematika spadá	N _{neis}	metodiky certifikované oprávněným orgánem	N _{neic}
		metodiky a postupy akreditované oprávněným orgánem	N _{meia}
		specializovaná mapa s odborným obsahem	N _{map}
		výsledky promítnuté do právních předpisů a norem	H _{leg}
poskytovatelem realizované výsledky - výsledky promítnuté do právních předpisů, norem, směrnic a výsledky promítnuté do předpisů nelegislativní povahy	H	výsledky promítnuté do směrnic a předpisů nelegislativní povahy zazazných 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

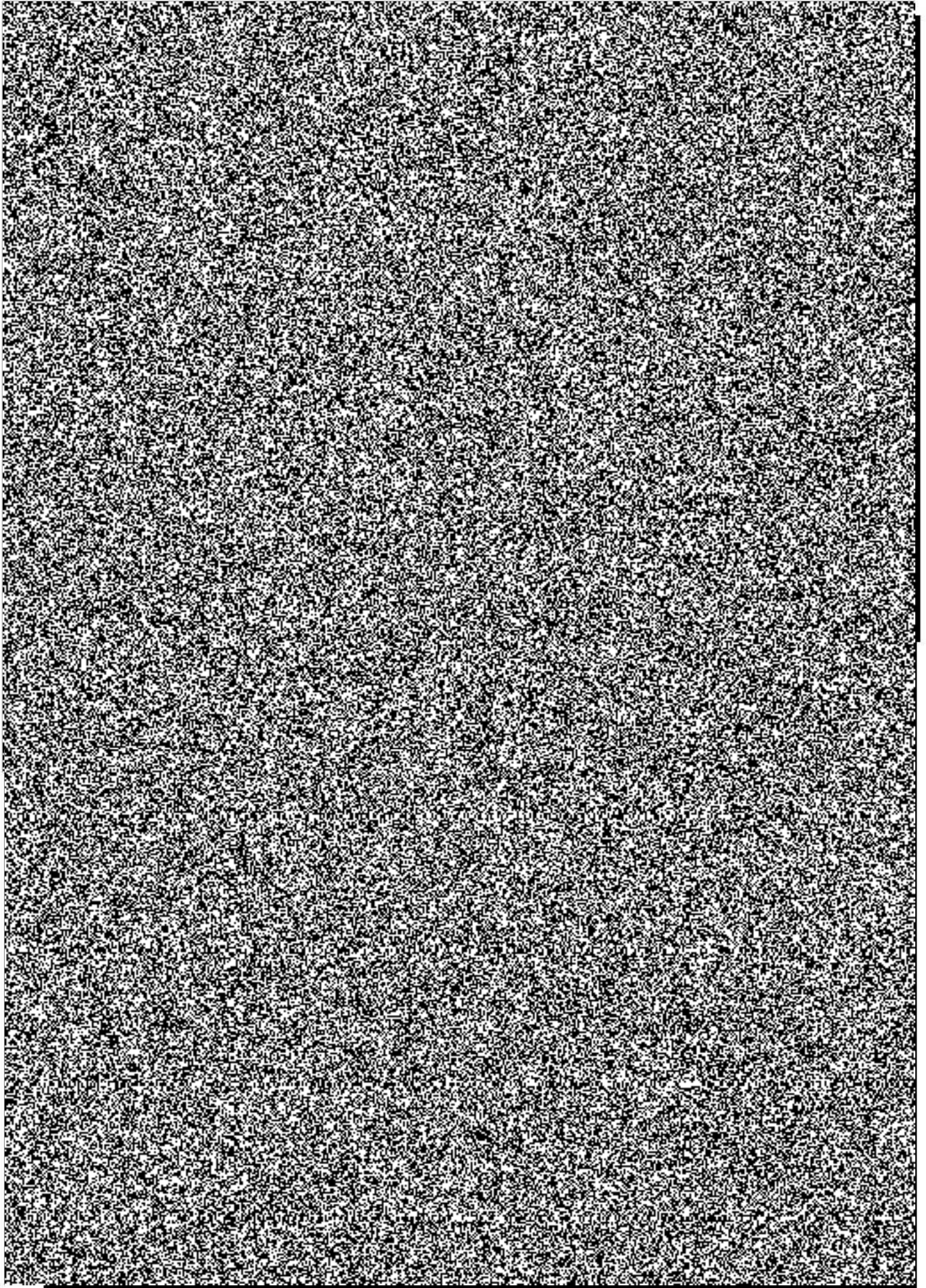


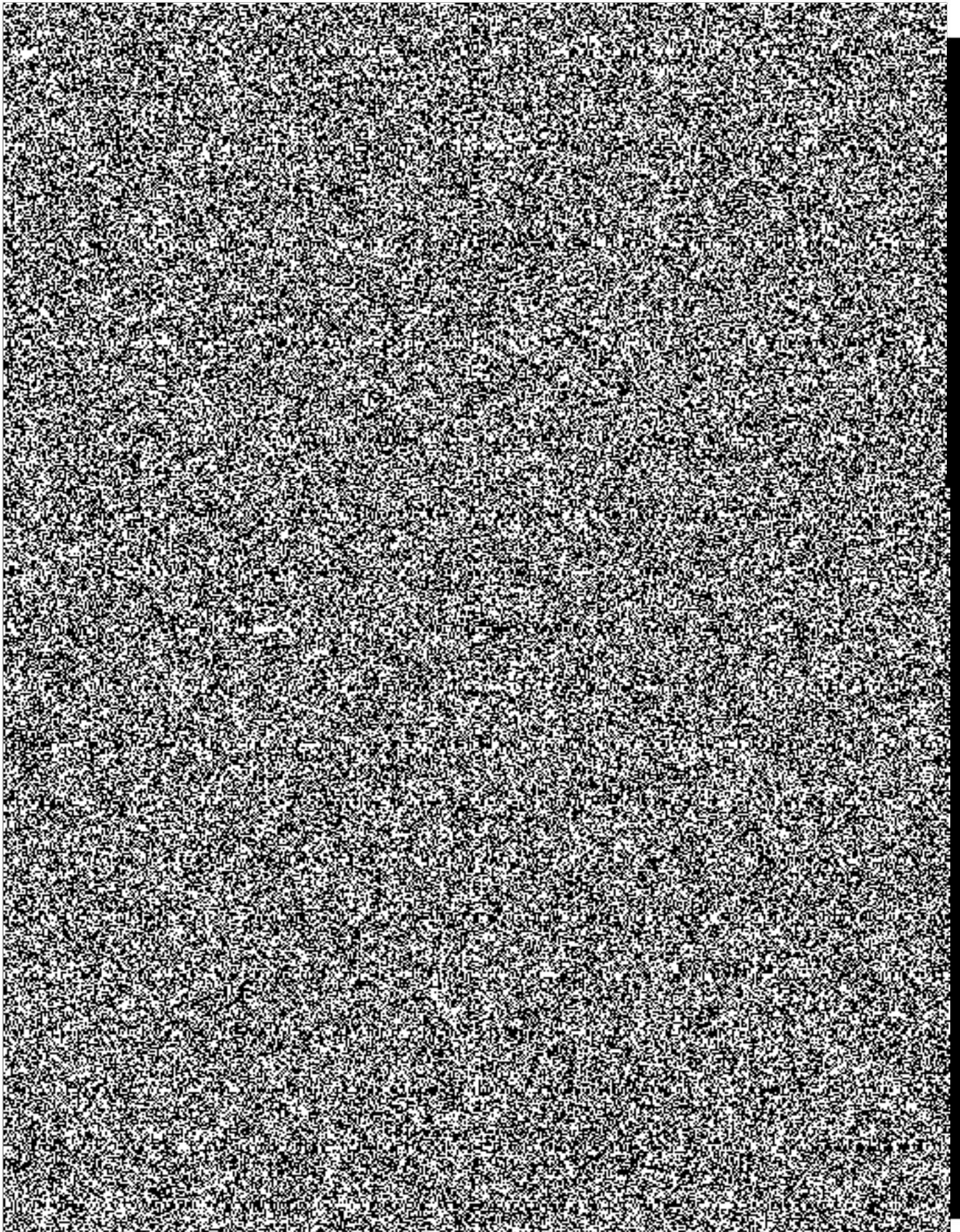
*) Uchazeč záhlaví vyplní, nehodící se škrtněte

¹ Uchazeč list vyplní, aktualizuje Počet listů

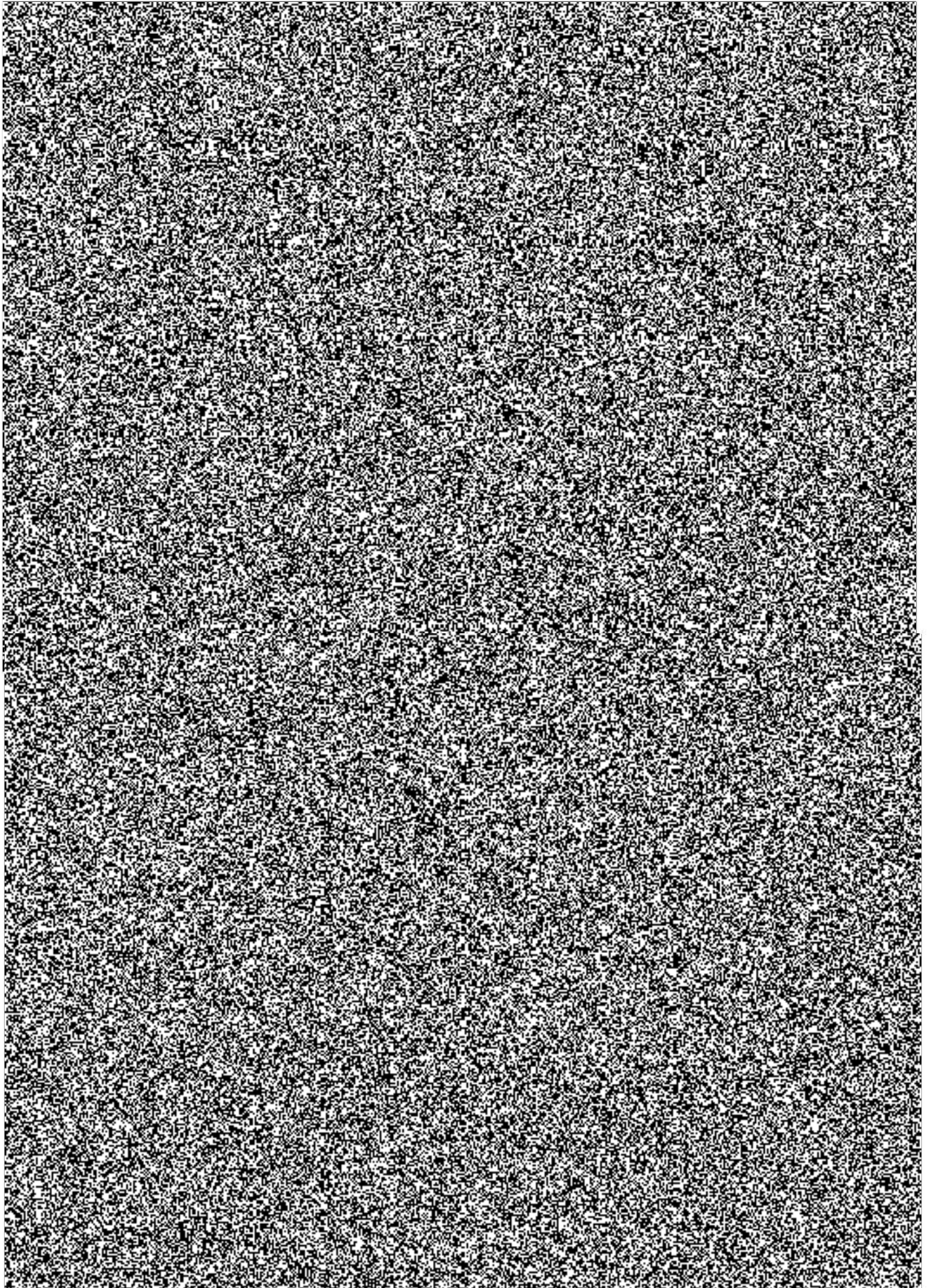
² Povinná příloha pro všechny uchazeče, v případě, že projekt podává více uchazečů, předkládá koordinátor

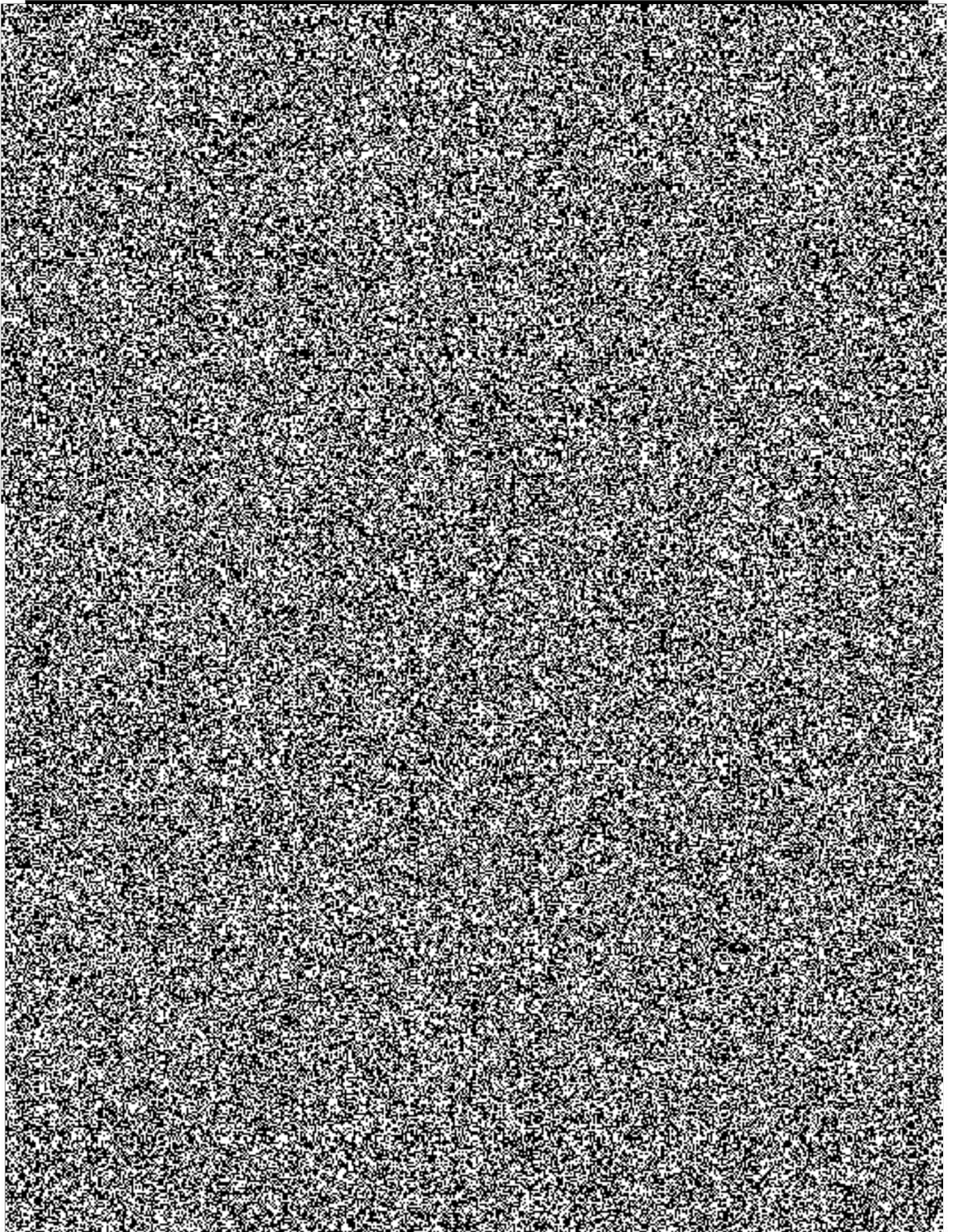




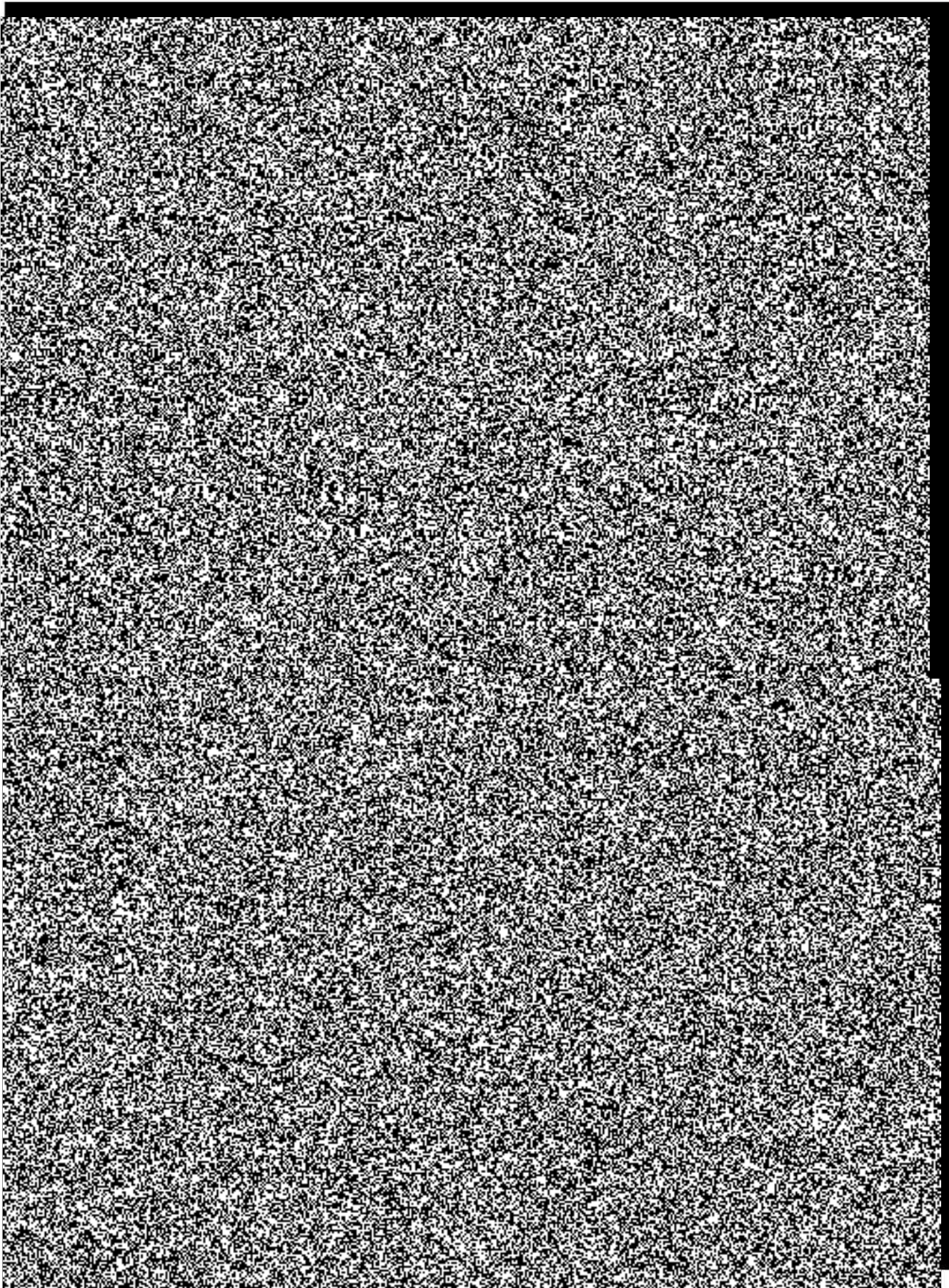


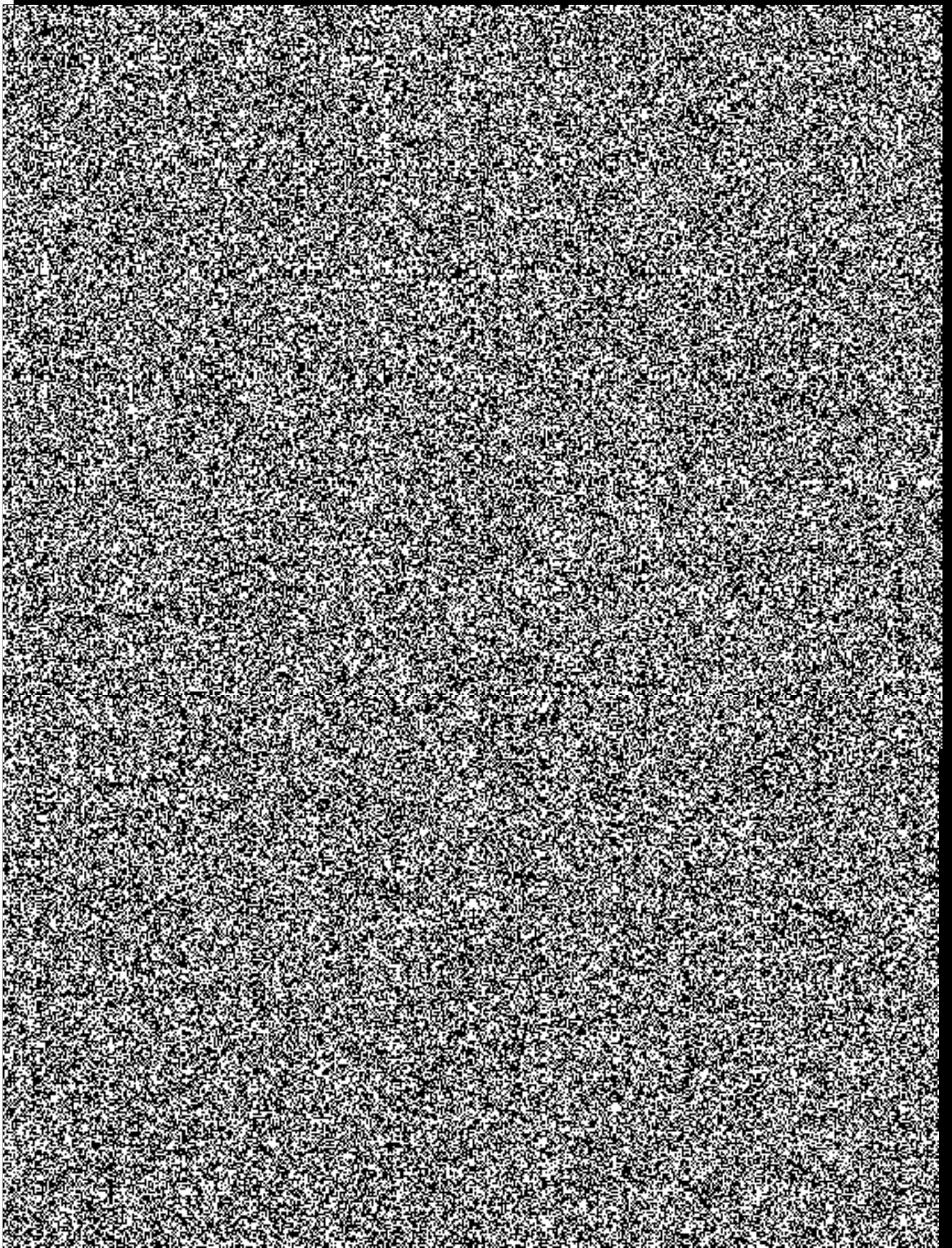
³ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)



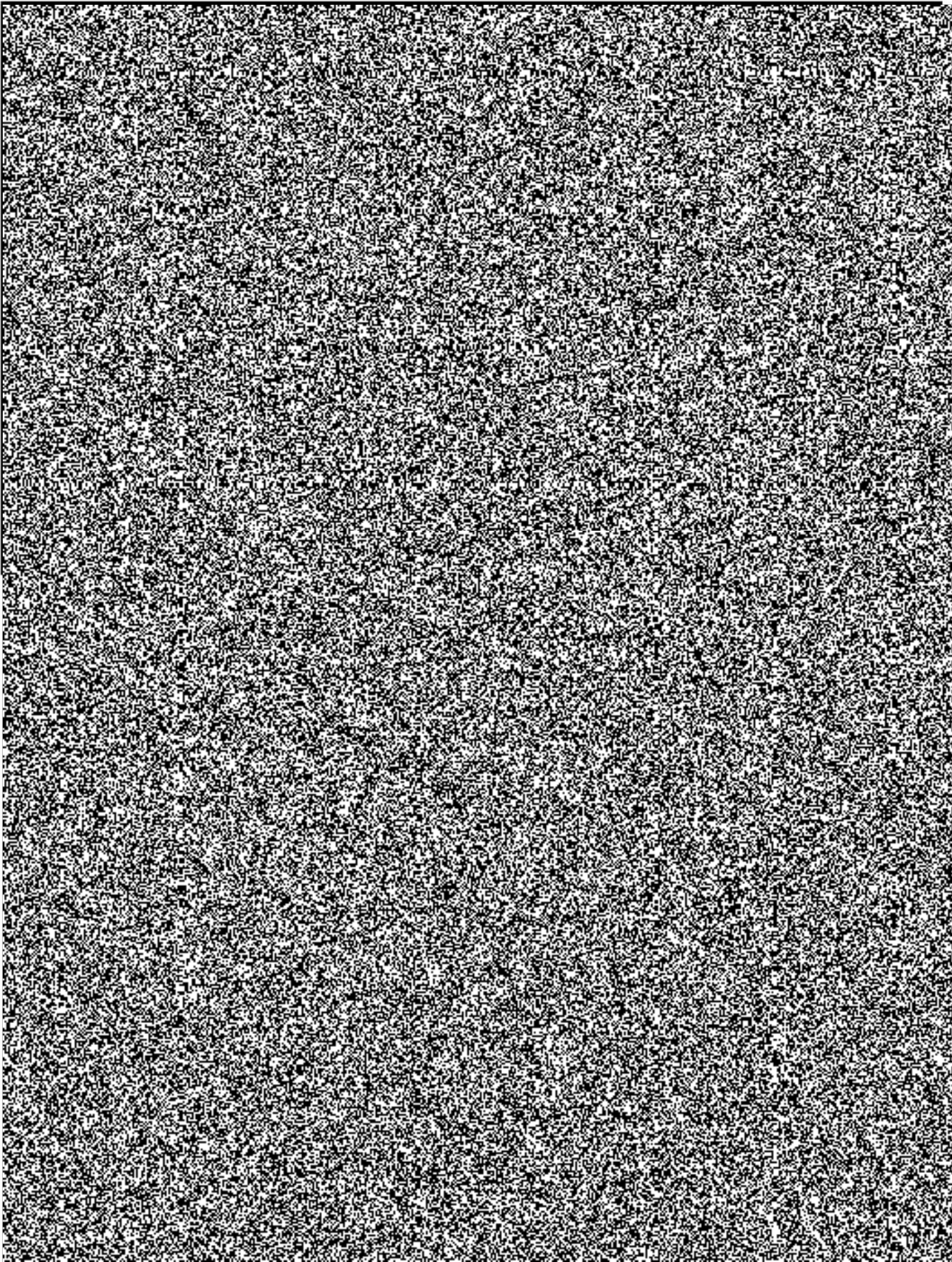


⁴ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)



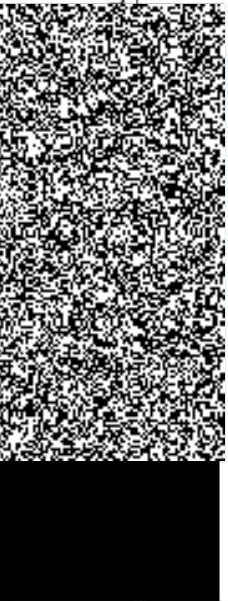


⁵ Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)



Zákon č. 112/2009 Sb., o ochraně údajových informací a o bezpečnosti zprávnosti nebo Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

soukromoprávních organizací i veřejnosti, zpřístupňovat systematicky zařazené a prezentované informace ke kvalifikacím v kyberbezpečnosti, o nabídce vzdělávání v dané oblasti.

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

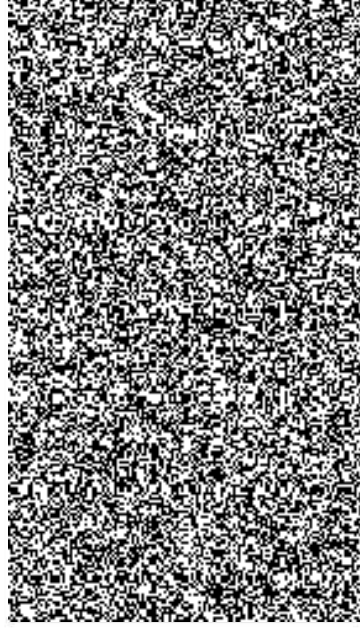
Metodika 2013 (zadávací dokumentace + elektronická přihláška)		Metodika 2017+	
název výsledku	kód výsledku	název výsledku	kód výsledku
patent	P	patent	P
software	R	software	R
výsledky s právní ochranou - užítý vzor, průmyslový vzor	F	speciálovaná veřejná databáze	S
poloprovoz, ověřená technologie	Z	užitý vzor	F _{uzi}
		průmyslový vzor	F _{prum}
		poloprovoz	Z _{polop}
technicky realizované výsledky - prototyp, funkční vzorek	G	ověřená technologie	Z _{tech}
		prototyp	G _{prot}
		funkční vzorek	G _{funk}
metodika	N	metodicky schválené příslušným orgánem státní správy, do jehož kompetence daná problematika spadá	N _{stns}
		metodicky certifikované oprávněným orgánem	N _{meic}
		metodicky a postupy akreditované oprávněným orgánem	N _{meia}
		speciálovaná mapa s odborným obsahem	N _{map}
		výsledky promítnuté do právních předpisů a norem	H _{lep}
poskytovatelem realizované výsledky - výsledky promítnuté do právních předpisů, norem, směrnic a výsledky promítnuté do předpisů nelegislativní povahy	H	výsledky promítnuté do směrnic a předpisů nelegislativní povahy zazazných v rámci kompetence příslušného poskytovatele	H _{leing}
		výsledky promítnuté do schválených strategických a koncepčních dokumentů orgánů státní nebo veřejné správy	H _{honic}
výzkumná zpráva obsahující utajované informace	V	výzkumná zpráva	V

Upravený rozpočet projektu: Národní kvalifikační rámec v kyberbezpečnosti

6. Financování a náklady projektu

6.1 Výše státní podpory projektu podle jednotlivých uchazečů

Uchazeč	Rok	Původní způsobilé náklady projektu (tis. Kč)	Způsobilé náklady projektu (tis. Kč)	Z toho vlastní zdroje (tis. Kč)	Požadovaná státní podpora (tis. Kč)	Intenzita podpory (%)	% původního rozpočtu
Masarykova univerzita / Fakulta informatiky	Celkem	8 748,95	7 436,60	0,00	7 436,60	100,00	85,00%
	2019	1 382,92	1 175,48	0	1 175,48	100,00	85,00%
	2020	3 065,03	2 605,28	0	2 605,28	100,00	85,00%
	2021	2 966,99	2 521,94	0	2 521,94	100,00	85,00%
	2021	1 334,01	1 133,90	0	1 133,90	100,00	85,00%



MASARYKOVA UNIVERZITA
Žerotínovo nám. 5
601 77 BRNO



10-06-2019

6.2 Rozpočet projektu

6.2.1 Výpočet maximální míry podpory uchazeče Masarykova univerzita / Fakulta informatiky

Kategorie uchazeče	výzkumná organizace
Kategorie výzkumu	průmyslový výzkum
Způsobilé náklady uchazeče (tis. Kč)	7 436,60
Účastní se projektu alespoň dva nezávislé podniky?	NE
Hradí každý podnik maximálně 70% nákladů projektu?	NE
Účastní se projektu malý, střední nebo zahraniční podnik?	NE
Účastní se projektu výzkumná organizace?	ANO
Je podíl výzkumné organizace na celkovém rozpočtu projektu vyšší než 10 %?	ANO
Může výzkumná organizace zveřejnit své výsledky?	ANO
Budou výsledky projektu obecně šířeny?	ANO
Základní intenzita podpory (%)	25,00
Bonus (%)	75,00
Maximální intenzita podpory (%)	100,00
Maximální výše podpory uchazeče (tis. Kč)	7 436,60

6.2.2 Náklady na mzdy uchazeče Masarykova univerzita / Fakulta informatiky

Jméno	Pozice v projektu	Druh pracovní smlouvy	Hodinová mzdová sazba (Kč)	Průměrný počet odprac. hodin měsíčně	Náklady na mzdy v jednotlivých letech trvání projektu (tis. Kč)	Náklady celkem (tis. Kč)
4 551,750						

6.2.4 Rozpočet nákladů uchazeče Masarykova univerzita / Fakulta informatiky

Náklady/výdaje uchazeče (tis. Kč)	2019	2020	2021	2022	Celkem
Osobní náklady/výdaje - mezisoučet					
a) mzdy/platy na základě pracovního poměru	959,18	2 125,90	2 057,90	840,27	5 983,26
b) esební mzdové náklady/výdaje na základě dohody o pracovní činnosti	660,14	1 524,37	1 524,37	622,42	4 331,30
c) esební mzdové náklady/výdaje na základě dohody o provedení práce	0,00	0,00	0,00	0,00	0,00
d) povinné pojistné na sociální zabezpečení	0,00	0,00	0,00	0,00	0,00
e) povinné pojistné na zdravotní pojištění	165,03	381,09	381,09	155,61	1 082,83
f) odvody do FKSP nebo sociálního fondu	59,41	137,19	137,19	56,02	389,82
g) cestovné	6,60	15,24	15,24	6,22	43,31
	68,00	68,00	0,00	0,00	136,00
Náklady/výdaje na pořízení hmotného a nehmotného majetku - mezisoučet					
a) dlouhodobý hmotný majetek	0,00	0,00	0,00	0,00	0,00
b) dlouhodobý nehmotný majetek	0,00	0,00	0,00	0,00	0,00
c) drobný hmotný majetek	0,00	0,00	0,00	0,00	0,00
d) drobný nehmotný majetek	0,00	0,00	0,00	0,00	0,00
Další provozní náklady/výdaje - mezisoučet					
Náklady/výdaje na služby - mezisoučet					
a) subdodávky	0,00	0,00	0,00	85,00	85,00
b) ostatní služby - mezisoučet	0,00	0,00	0,00	0,00	0,00
Audit projektu					
výjezdní zasedání					
konferenční poplatky					
	0,00	0,00	0,00	85,00	85,00
Doplňkové náklady/výdaje - mezisoučet					
Režie příjemce	216,29	479,37	464,04	208,64	1 368,33
	216,29	479,37	464,04	208,64	1 368,33
Celkové způsobilé náklady - mezisoučet					
	1 175,48	2 605,28	2 521,94	1 133,90	7 436,60
Celková státní podpora - mezisoučet					
	1 175,48	2 605,28	2 521,94	1 133,90	7 436,60