Metodické doporučení

k řízení rizik v oblasti bezpečnosti výzkumu na institucionální úrovni

Předkládaný soubor dokumentů ke zvyšování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí byl, i na základě požadavků českých vysokoškolských a výzkumných institucí a ve snaze o zamezení roztříštěného přístupu daných institucí k problematice nelegitimního ovlivňování, vypracován v rámci Mezirezortní pracovní skupiny pro potírání nelegitimního ovlivňování ve vysokoškolském a výzkumném prostředí se zásadním přispěním Ministerstva školství mládeže a tělovýchovy, Ministerstva vnitra a Akademie věd ČR a v konzultaci se zástupci a zástupkyněmi dalších českých vysokoškolských a výzkumných institucí.

VÝKLAD POJMŮ

Pro účely této metodiky a souvisejících materiálů *Metodické doporučení, kterým se definuje minimální rozsah due diligence a řízení rizik spolupráce s třetími stranami v rámci posilování odolnosti vysokoškolského a výzkumného prostředí vůči nelegitimnímu ovlivňování*, a *Metodické doporučení k řízení rizik v oblasti bezpečnosti výzkumu na institucionální úrovni* se pojmy uvedené níže vykládají takto:

Akademická instituce

Označení používané jako alternativní pojem pro vysokoškolské a výzkumné instituce, podle kontextu společně i zvlášť.

Bezpečnostní výzkum

Bezpečnostním výzkumem se rozumí výzkumné, vývojové a inovační činnosti, jejichž cílem je identifikace, prevence, příprava a ochrana proti nezákonným jednáním nebo jednáním úmyslně poškozujícím (evropské) společenství, lidské bytosti, organizace nebo struktury, hmotné i nehmotné statky a infrastruktury, včetně zajištění operační kontinuity po takovém jednání a zmírnění jeho důsledků (také aplikovatelné v případě přírodních katastrof a průmyslových havárií).

Bezpečnost výzkumu

Bezpečností výzkumu se rozumí organizační a systémové postupy pro vyhodnocování a zvládání bezpečnostních rizik v oblasti výzkumu a vzdělávání, které snižují rizika spojená s nelegitimním

ovlivňováním ve vysokoškolském a výzkumném prostředí. Primárním cílem bezpečnosti výzkumu je komplexní ochrana výzkumného ekosystému a s ním také spojená ochrana národních a ekonomických zájmů.

Citlivá data/informace

Označení pro data a informace, které akademická instituce chrání jako předmět znalostí v rámci citlivé oblasti výzkumu a vzdělávání, nebo je považuje za důvěrné z vlastního rozhodnutí, nebo jde o data a údaje, které musí chránit na základě regulatorního požadavku státu.

Citlivé oblasti výzkumu a vzdělávání

Jde o označení oblastí výzkumu a vzdělávání, které nesou zvýšená rizika nelegitimního ovlivňování a u nichž se usiluje o jejich zvýšenou ochranu, a to:

- kritické technologie pro ekonomickou bezpečnost EU,
- vybrané obory výzkumu a vzdělávání,
- vybraná spolupráce s třetími stranami,
- zboží a technologie dvojího užití a vojenský materiál,
- to, co se daná akademická instituce sama rozhodne do této oblasti zařadit.

Cizí moc

Rozumí se tím cizí stát nebo jeho orgán anebo nadnárodní nebo mezinárodní organizace nebo její orgán, jakož i jakékoliv další fyzické osoby bez ohledu na jejich státní příslušnost a právnické osoby bez ohledu na jejich sídlo anebo místo působení, pokud se podílí, byť i jen částečně, na prosazování zájmů cizího státu či organizace formou nelegitimního ovlivňování.

Due diligence

Rozumí se tím náležitá péče představující soubor opatření, která mají eliminovat či snížit rizika nelegitimního ovlivňování akademických institucí vyplývající ze spolupráce s třetími stranami.

Identifikační údaje

1. jméno, příjmení, datum narození a státní příslušnost, jde-li o fyzickou osobu,
2. název a sídlo, jde-li o právnickou osobu, nebo
3. označení nebo název v ostatních případech, popřípadě další údaje nezbytné k jednoznačné identifikaci partnera.

Kritické technologie pro ekonomickou bezpečnost EU

Rozumí se tím seznam technologických oblastí definovaných v Doporučení Evropské komise ze dne 3. 10. 2023 o kritických technologických oblastech pro hospodářskou bezpečnost EU pro další posouzení rizik s členskými státy[1] a jeho přílohu[2].

1 COMMISSION RECOMMENDATION of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States; C(2023) 6689 final

2 ANNEX to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, C(2023) 6689 final,

Nelegitimní ovlivňování

Označení pro nežádoucí působení na lidi, rozhodování, či procesy. Zahrnuje jak vlivové působení cizí moci, tak i kriminální (např. korupční) jednání a nežádoucí lobbování. Obvykle jde o aktivity, které jsou skryté, klamavé, vynucující či korupční a které původce či původkyně nelegitimního ovlivňování (cizí moc, korupce, lobbing postupující v rozporu se zákonem, případně obecně uznávanými společenskými etickými pravidly) vykonává sám či sama anebo prostřednictvím třetí strany a které ohrožují či poškozují zájmy vysokoškolských a výzkumných institucí.
Alternativně se používá i pojem nelegitimní působení.

Partner

Rozumí se jím jakákoliv právnická či fyzická osoba, se kterou vstupují, anebo již jsou, vysokoškolské a výzkumné instituce v partnerském vztahu.

Partnerský vztah

Takový vztah či spolupráce, který je založen smlouvou o spolupráci či jiným zpravidla písemným ujednáním (např. memorandum o porozumění, o rozdělení kompetencí v řešitelských týmech) mezi akademickou institucí a třetí stranou. V některých případech se může jednat i o méně formálně či zcela neformálně uzavřený smluvní vztah (včetně konkludentního) mezi zaměstnancem či zaměstnankyní akademické instituce a třetí stranou.

Pracovník či pracovnice vysokoškolské a výzkumné instituce/ akademické instituce

Rozumí se jím student či studentka, stážista či stážistka, vysokoškolský a výzkumný pracovník či pracovnice, další zaměstnanci v pracovněprávním poměru nebo fyzické osoby v jiném smluvním vztahu s akademickou institucí, jakož i další osoby podílející se na činnosti akademické instituce.

Původce nelegitimního ovlivňování

Rozumí se jím vždy osoba, bez ohledu na to, zda jedná sama či ve prospěch nějakého státu, firmy, organizace a bez ohledu na to, jaké formy a metody nelegitimního ovlivňování využívá. Někdy je rovněž používán pojem útočník. Svoje zájmy prosazuje zpravidla v rozporu s demokratickými principy, právním řádem, ale i dobrými mravy. Snaží se najít si co možná nejjednodušší cestu k prosazování svých zájmů, přičemž v absolutní většině případů takové aktivity směřují proti nějaké fyzické osobě (v tomto případě členovi či člence akademické obce nebo zaměstnanci či zaměstnankyni akademické instituce).

Regionální studia

Označení pro vědní obory zabývající se studiem lokálních a regionálních souvislostí vývoje společnosti a životního prostředí, resp. kontextem a reáliemi daného regionu.

Třetí strana

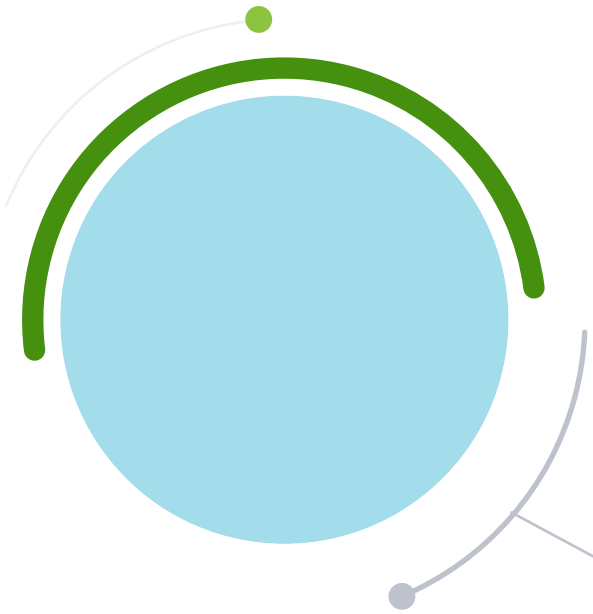
Rozumí se jí jakákoliv právnická či fyzická osoba, orgán veřejné moci nebo jiný subjekt, který zastupuje či jedná ve prospěch státu, který není členským státem Evropské unie (EU)[3], Evropského hospodářského prostoru (EHP)[4] nebo Evropského sdružení volného obchodu (ESVO)[5].

Třetí země

Rozumí se jí jiná země než ČR. Alternativně je též používán termín třetí stát.

VaVaI

Zkratka VaVaI odkazuje na výzkum, vývoj a inovace.
Ostatní použité pojmy jsou vykládány ve smyslu Sdělení Evropské komise o rámci pro státní podporu výzkumu, vývoje a inovací (2022/C 414/01).



3 https://european-union.europa.eu/easy-read_cs

4 https://www.europarl.europa.eu/factsheets/cs/sheet/169/the-european-economic-area-eea-switzerland-and-the-north; Norsko, Island a Lichtenštejnsko

5 https://eur-lex.europa.eu/CS/legal-content/glossary/european-free-trade-association-efta.html; Island, Lichtenštejnsko, Norsko a Švýcarsko

ÚVOD

Tento dokument je metodickým materiálem pro oblast řízení rizik v souvislosti s agendou bezpečnosti výzkumu v akademických institucích v ČR a je zpracován jako prováděcí dokument k obecné metodice **Posilování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí**.

Účelem tohoto dokumentu je poskytnout vedení akademických institucí i odborníkům i odbornicím pro oblast bezpečnosti výzkumu návod, jak realizovat opatření ke zvyšování institucionální odolnosti a představit konkrétní nástroje pro řízení rizik v oblasti ochrany proti hrozbám nelegitimního ovlivňování akademických svobod a narušování institucionální autonomie. Cílem takových opatření a nástrojů je těmto hrozbám předcházet a čelit, resp. zajistit důvěryhodnost výzkumu realizovaného ve vysokoškolských a výzkumných institucích.

Pojmy používané v tomto materiálu mají význam uvedený ve výkladu pojmů v obecné metodice **Posilování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí**.

Jako zdroje pro vypracování tohoto materiálu byly použity politiky a dokumenty EU vydané pro oblast nelegitimního ovlivňování, na které je odkázáno dále v tomto textu, a ISO normy vydané pro agendy informační a kybernetické bezpečnosti ze strany Mezinárodní organizace pro normalizaci (International Organization for Standardization, **ISO – About ISO**) a České agentury pro standardizaci (**Česká agentura pro standardizaci (agentura-cas.cz**), zejména normy z řady ISO/IEC 27000 pro Systém řízení bezpečnosti informací (ISMS), specificky především ČSN EN ISO/IEC 27001 a 27002.

I. INSTITUCIONÁLNÍ ODOLNOST

POLITIKA EU A NÁRODNÍ KROKY

Vývoj politiky EU i přístupu vlády ČR k problematice institucionální odolnosti vysokoškolských a výzkumných institucí a k problematice bezpečnosti výzkumu je popsán v obecné metodice **Posilování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí**. Tato metodika poukazuje na skutečnost, že příprava **Agendy pro Evropský výzkumný prostor na roky 2025–2027**, stejně jako diskuse o nadcházejícím rámcovém programu EU pro výzkum a inovace, zcela jednoznačně kladou důraz na **posílení bezpečnosti výzkumu**. EU opětovně deklaruje zásadní význam oblasti výzkumu, vývoje a inovací na udržitelný rozvoj, prosperitu, konkurenceschopnost, hospodářský a sociální status Evropy a podporuje otevřenost mezinárodní výzkumné spolupráce, avšak zároveň očekává rovné podmínky a reciprocitu partnerských států a institucí založenou na základních akademických hodnotách a respektování duševního vlastnictví. S ohledem na současný politický vývoj ve světě EU zdůrazňuje nutnost tzv. **„vyvážené otevřenosti"**. Tímto termínem označuje rovnováhu mezi rozvíjením otevřené spolupráce s mezinárodními partnery na straně jedné a posílením bezpečnosti výzkumu na druhé.

EK vyzývá, aby se věda mobilizovala a lépe chránila své zájmy, hodnoty a odborné znalosti podle zásady **„as open as possible, as closed as necessary"** a spolu s tím, aby akademické instituce investovaly do specializovaných odborných znalostí v oblasti bezpečnosti výzkumu. Na základě zkušeností je v současné době prokázané, že se výzkumní pracovníci stávají prostředkem, jak mohou autokra-

tické a neliberální vlády získávat nelegitimními cestami nejmodernější znalosti a technologie, a že k tomu používají nekalé praktiky a postupy, často pod záštitou zdánlivě důvěryhodné mezinárodní akademické spolupráce.

Podle **Návrhu Doporučení Rady k posílení bezpečnosti výzkumu** se za nelegitimní ovlivňování v oblasti výzkumu, vývoje a inovací (VaVaI) považuje zejména:

- nežádoucí přenos kritických znalostí, know-how a technologií, které mohou ovlivnit bezpečnost EU a jejich členských států, například pokud by byly použity pro vojenské nebo zpravodajské účely ve třetích zemích,
- zneužití výzkumné činnosti k šíření dezinformací na základě ovlivňování ze třetích zemí/stran,
- podněcování autocenzury mezi studujícími a výzkumnými pracovníky a pracovnicemi vedoucí k narušení institucionální autonomie,
- porušování vědecké etiky nebo integrity výzkumu, jehož důsledkem je zneužívání znalostí a technologií k potlačování nebo podkopávání základních demokratických hodnot.

ODPOVĚDNOST AKADEMICKÝCH INSTITUCÍ

Návrh nového zákona o výzkumu, vývoji, inovacích a transferu znalostí z listopadu 2023 předpokládá v souvislosti s financováním VaVaI zavedení pojmu „institucionální odolnost" a spolu s tím i povinnost „předběžné opatrnosti". Jde o povinnosti k zajištění bezpečnosti výzkumu a ochraně proti nelegitimnímu ovlivňování, přičemž takové povinnosti mají být založeny jak na straně poskytovatelů podpory, tak příjemců.

Pojem **institucionální odolnost** není v této chvíli závazně definován. Měl by být vnímán jako schopnost akademické instituce zavést a realizovat systém opatření k posílení bezpečnosti výzkumu proti nelegitimnímu ovlivňování a na ochranu dobrého jména vysokoškolských a výzkumných institucí, spočívající zejména v bezpečné mezinárodní výzkumné a akademické spolupráci, včetně dodržování závazných sankčních omezení, správě duševního vlastnictví a v řízení rizik zejména v oblastech výzkumu s významným transformačním potenciálem znalostí a technologií, v oblastech vztahujících se k technologiím dvojího užití a vojenského materiálu, ale také výzkumu s rizikem zneužití znalostí či technologií k porušování lidských práv a svobod.

V souladu s institucionální autonomií a akademickou svobodou jsou akademické instituce pokládány ze strany EU i vlády ČR za **primárně odpovědné** za svou mezinárodní spolupráci a za zavedení opatření k zabezpečení institucionální odolnosti. Velká část práce na posilování odolnosti výzkumných a vysokoškolských institucí proto bude souviset se změnou přístupu jednotlivých pracovišť i jejich pracujících k otevřenosti akademické spolupráce, zejména při přípravě a při provádění výzkumu. Zde bude nezbytné hledat novou rovnováhu mezi otevřeností a bezpečností výzkumu a soustředit se na zajištění ochrany duševního vlastnictví.

II. ZABEZPEČENÍ VÝZKUMU

OCHRANA VÝSTUPŮ Z VAVAI vs. OPEN SCIENCE?

Doporučení Rady k posílení bezpečnosti výzkumu zdůrazňuje podmínku **„otevřenosti podle potřeby"** a vyzývá k rovnováze mezi otevřeným přístupem ve vědě a vzdělávání na straně jedné a ochranou duševního vlastnictví na straně druhé. Otevřenost akademického prostředí by proto měla být ve všech fázích výzkumné spolupráce více vnímána i z pohledu bezpečnosti výzkumu. Již během přípravy a realizace výzkumného projektu by měla být zajišťována ochrana citlivých výzkumných dat a údajů a implementována účelná bezpečnostní opatření na ochranu proti nežádoucímu ovlivňování výzkumu i nelegitimnímu použití výsledků.

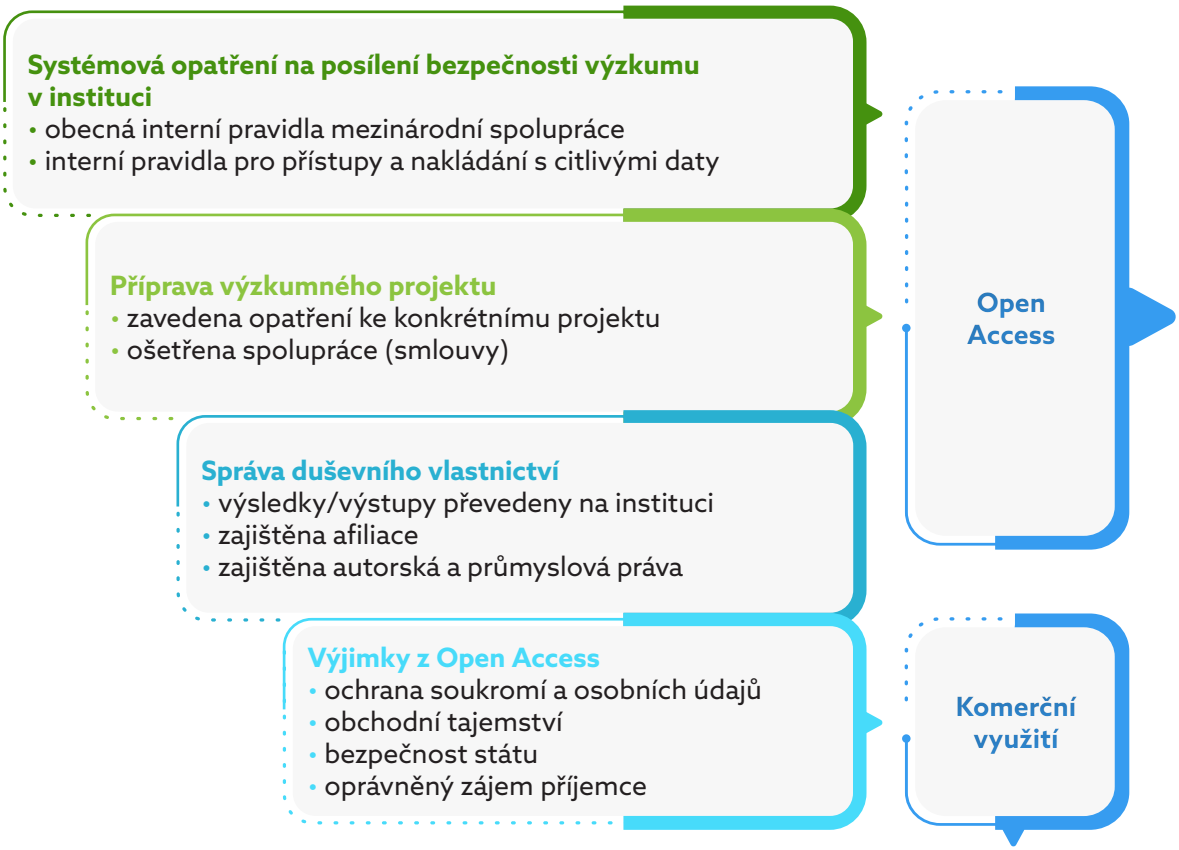
Takový požadavek **rozhodně není v rozporu se zájmy EU na otevřené vědě** (Open Science), která směřuje k reprodukovatelnosti vědeckých poznatků a otevřenému přístupu k publikacím, datům a softwaru pro jejich neomezené použití. Požadavek na otevřený přístup k výzkumným datům (Open Access) je realizován až poté, kdy je výsledků z výzkumného projektu dosaženo a kdy už by měla být zajištěna jak správa duševního vlastnictví, tak aplikovány výjimky z otevřeného přístupu z důvodů ochrany soukromí, civilní bezpečnosti či vojenských nebo obchodních důvodů.

Princip otevřeného přístupu k informacím o výzkumných datech a k výzkumným datům, ve smyslu Směrnice EP a Rady (EU) 2019/1024 o otevřených datech a opakovaném použití informací veřejného sektoru, byl do české legislativy promítnut v ust. §§ 12 a 12a zákona č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovacích, ve znění novely provedené zákonem č. 241/2022 Sb., a to s účinností od 1. září 2022. I v národní právní úpravě jsou tímto založeny možnosti odmítnout poskytnutí výzkumných výstupů/výsledků v případech, kdyby takovým poskytnutím bylo nepřiměřeně zasaženo do práva na ochranu soukromí a osobních údajů, práva na ochranu obchodního tajemství, bezpečnosti státu nebo jiných oprávněných zájmů příjemce. Příjemci mohou odmítnout poskytnutí výzkumných dat také v případě, kdy výzkum nebo vývoj nebyl plně financován z veřejných prostředků. Navíc byl zaveden tzv. časový rámec jednoho roku po ukončení dotační podpory, kdy není nutné výzkumná data zveřejňovat, a to s ohledem na umožnění vědecké výsledky komercializovat.

I podle **Pokynů k pravidlům otevřeného přístupu pro program Horizont Evropa** by mělo rozhodnutí, zda publikovat prostřednictvím otevřeného přístupu přijít až po obecnějším zhodnocení a rozhodnutí, zda publikovat přímo, nebo nejprve usilovat o právní ochranu výsledků projektu.

Obecný výklad k problematice Open Science v kontextu nelegitimního ovlivňování ve vysokoškolském a výzkumném prostředí je k dispozici v obecné metodice Posilování odolnosti vůči nelegitimnímu ovlivňování ve vysokoškolském a výzkumném prostředí.

Postup v souvislosti s implementací opatření na ochranu výzkumných dat při přípravě a provádění projektů a jejich zpřístupněním lze schematicky vyjádřit takto:



CÍL

Organizační a systémové postupy pro vyhodnocování a zvládání rizik mezinárodní spolupráce v podobě nelegitimního ovlivňování mají za cíl docílit statusu **důvěryhodného výzkumu**. V obecné rovině je to takový výzkum, ve kterém jsou otevřenost akademického prostředí a bezpečnost výzkumu v rovnováze, protože akademická instituce:

- **má systém ochrany proti ohrožení duševního vlastnictví a citlivého výzkumu, proti ovlivnění rozhodovacích procesů a proti poškození dobrého jména instituce a jejich pracujících,**
- **chrání citlivá data a informace (o výzkumu, svých pracujících, organizaci) a umí zajistit důvěrnost, integritu a dostupnost informací z VaVaI,**
- **pomáhá co nejlépe využívat mezinárodní spolupráci a zároveň chránit duševní vlastnictví, citlivý výzkum i osobní údaje,**
- **zná potenciální rizika spolupráce v akademickém prostředí v současném světě,**
- **realizuje informovaná rozhodnutí,**
- **chrání svou instituci a své pracující proti zneužití,**
- **a konečně napomáhá integraci a mezinárodní spolupráci ve VaVaI tím, že dává jistotu partnerům, že rizika jsou přiměřeně řízena.**

OBLASTI OPATŘENÍ

Konkrétní opatření na ochranu proti nelegitimnímu ovlivňování, jejichž přijetí by měly akademické instituce zvážit, lze rozdělit do následujících kategorií; podrobnější rozvedení těchto opatření obsahuje tento **materiál v části III.**:

- **Ochrana proti nelegitimním zásahům do činnosti vysokoškolských a výzkumných institucí**

  Součástí bude provedení klasifikace citlivých oblastí výzkumu a citlivých dat a informací podle konkrétního předmětu činnosti instituce, aktuálních projektů a probíhající mezinárodní spolupráce v dané instituci. Doporučuje se předchozí kvalitní popis interních procesů a oběhu dat a informací v instituci. Instituce by měly analyzovat bezpečnostní rizika mezinárodní spolupráce v souladu s **Metodickým doporučením pro spolupráci s třetími stranami**. Instituce by měla také vyhodnotit potřebu provedení auditu stávajících vědeckých a partnerských spoluprací za účelem odhalení rizik nelegitimního ovlivňování a provedení opatření ke snížení těchto rizik.

- **Zavedení důsledného systému ochrany duševního vlastnictví**

  Instituce musí vyhodnotit, zda výstupy/výsledky výzkumu mají či mohou mít komerční hodnotu, a pokud ano, zajistit, aby takové výstupy/výsledky byly chráněny. Současná právní úprava vyžaduje, aby práva k projektovým výsledkům/výstupům byla primárně převedena z výzkumníků a výzkumnic (a jiných stran, které byly nápomocny při dosažení výsledků/výstupů) na instituci, ve které jsou tyto osoby zaměstnány. Instituce musí zvážit, zda mohou být výsledky/výstupy využity v praxi. Pokud se u daného výsledku/výstupu komerční či jiné využití nepředpokládá, či se v rozumné době nepodaří realizovat, měl by být výsledek/výstup společně se souvisejícími daty zveřejněn (i s časovým odstupem), a to s umožněním otevřeného přístupu (Open Access).

- **Zajištění informační a kybernetické bezpečnosti**

  Instituce by měly přijmout účinná opatření pro zajištění své informační a kybernetické bezpečnosti za účelem zabezpečení důvěrnosti, dostupnosti a integrity dat a informací, se kterými

nakládají ať již ve formě ústní, tištěné nebo elektronické. Instituce by měly nastavit systém autorizací a přístupů ke zdrojům tak, aby jejich data byla chráněna, zároveň mohla být sdílena, je-li to účelné či vyžadováno, a současně aby byla zachována jejich platnost a aktuálnost.

- **Dodržování závazných předpisů a pravidel**

  Instituce musí přijmout opatření nezbytná pro zajištění obecně závazných předpisů, včetně závazných pravidel na ochranu proti bezpečnostním hrozbám a rizikům. Vedle standardně plněných postupů ve věci zadávání veřejných zakázek, GDPR, ke kterým přistupuje také ochrana oznamujících (whistleblowing), je podle oboru hlavní činnosti a aktuálních projektů nezbytné vyhodnocovat i omezení daná z důvodu mezinárodních sankcí, kontrolních režimů, povinnosti prověřování zahraničních investic.

III. OPATŘENÍ NA ÚROVNI AKADEMICKÝCH INSTITUCÍ

KROKY AKADEMICKÝCH INSTITUCÍ

Úkolem akademických institucí bude, aby agendu institucionální odolnosti implementovaly podle své potřeby na svých pracovištích, resp. aby jednotlivá opatření **přizpůsobily svému oboru činnosti a specifickým potřebám aktuálních výzkumných projektů**. Vnitřní procesy a mechanismy podporující odolnost instituce by měly zahrnovat:

- systémové ukotvení agendy související s posílením odolnosti a ochranou proti nelegitimnímu působení,
- nastavení kompetencí, zajištění zdrojů a podpory,
- metodiky pro jednotlivé činnosti v rámci agendy institucionální odolnosti,
- komunikační, vzdělávací a osvětové aktivity.

Účinným nástrojem k posouzení potřeby implementace opatření na ochranu bezpečnosti výzkumu budou na jednotlivých pracovištích **interní postupy pro řízení rizik**. S ohledem na shodné základní poslání vysokoškolských institucí i obdobnou hlavní činnost výzkumných institucí, přinejmenším v rámci vědních oblastí, budou takové interní postupy na jednotlivých pracovištích do značné míry podobné, protože budou zahrnovat obecně platné návody pro identifikaci rizik, pravidla hodnocení potenciálních partnerů i postupy pro rozhodování o mezinárodní spolupráci se zvýšeným rizikem apod.

Akademické instituce by proto měly zároveň vytvořit prostor pro budování komunity na národní i mezinárodní úrovni k řešení otázek bezpečnosti vzdělávací a výzkumné činnosti a pro sdílení zkušeností i výměnu informací mezi sebou navzájem, a to zejména s cílem **sdružování zdrojů a odborných znalostí**. Vedení by měla podporovat setkání na úrovni zřizovatelů, poskytovatelů, národních úřadů i EU za účelem předávání a zlepšování znalostí o osvědčených postupech v oblasti institucionální odolnosti, nových technologiích i službách, ale i hrozbách nebo zranitelnostech akademických pracovišť. Stejně tak bude vhodné nastavit a udržovat kontakt s příslušnými autoritami pro řešení konkrétních bezpečnostních incidentů.

Implementace opatření institucionální odolnosti na konkrétních pracovištích nebude možná bez podpory nejvyššího vedení akademických institucí a na základě přijetí odpovědnosti za tuto agendu ze strany pracovníků a pracovnic ve všech řídících úrovních.

Zároveň bude zcela zásadní, **aby přijímaná opatření byla přiměřená**, s plným respektem k zásadě „rizika snížit, nikoli oddělit", a aby zavedená řešení znamenala pro instituce **minimální administrativní, organizační a finanční zátěž**.

ŘÍZENÍ RIZIK

Následující text je **určen zejména pro odborné pracovníky a pracovnice**, kteří budou mít agendu řízení rizik bezpečnosti výzkumu na akademických pracovištích na starosti. Rozsah a podoba dále uvedených doporučení není komplexním a detailním popisem dílčích postupů a návodů, avšak může podat přehled o účinných nástrojích řízení rizik, o dopadech problematiky do jiných agend, jejich vzájemném propojení, jakož i posloužit pro tvorbu hlubšího a uceleného prováděcího materiálu pro potřeby dané instituce.

Podle **Návrhu Doporučení Rady k posílení bezpečnosti výzkumu** je cílem opatření zajistit hospodářskou bezpečnost a ekonomickou odolnost EU. S ohledem na to se má řízení rizik týkat zejména opatření proti:

- nežádoucímu přenosu kritických znalostí, know-how a technologií, které by mohly být použity například pro vojenské nebo zpravodajské účely ve třetích zemích,
- nežádoucímu vlivu na výzkum prostřednictvím ovlivňování studujících a pracujících s cílem šíření dezinformací nebo dosažení autocenzury ve prospěch nelegitimních zájmů třetí strany uvnitř akademické instituce,
- porušování etiky nebo integrity výzkumu, kdy by znalosti a technologie byly využívány k potlačování akademické svobody i základních demokratických hodnot.

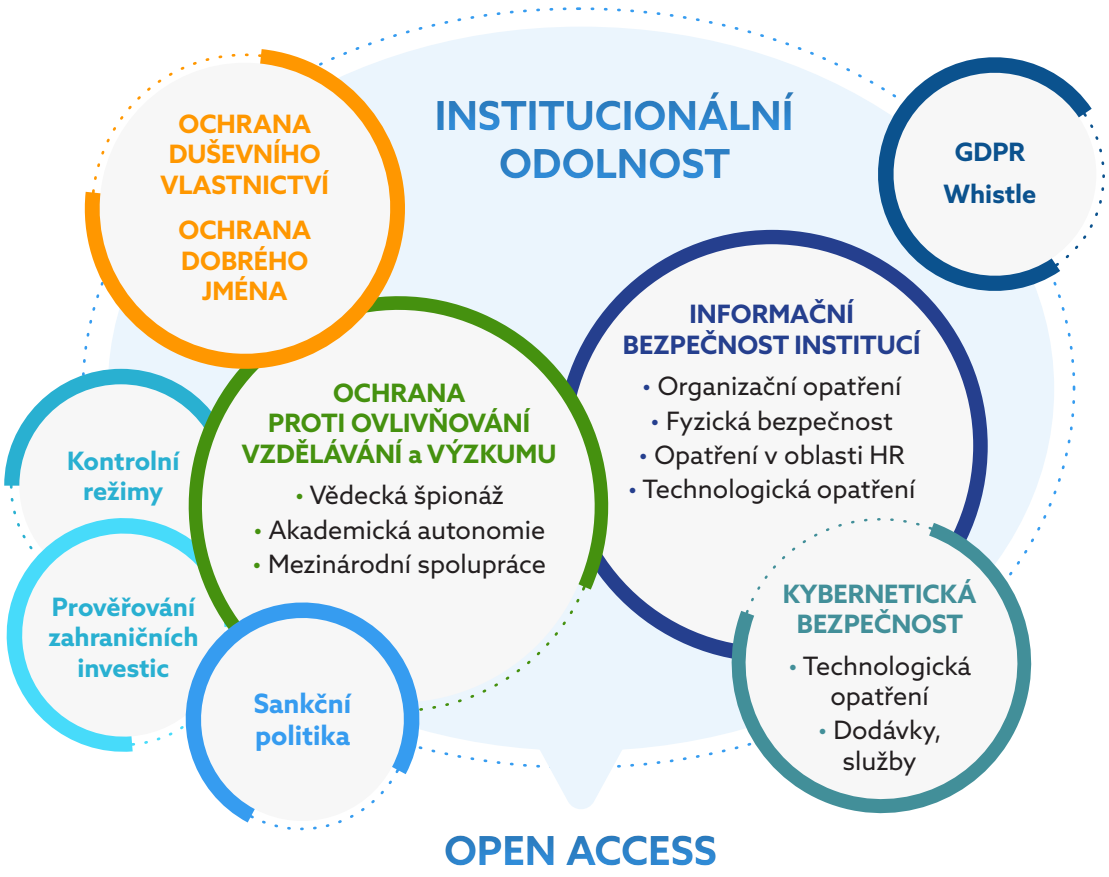
Pro nastavení postupů řízení rizik v souvislosti s bezpečností výzkumu bude účelné vycházet i z **mezinárodních standardů** používaných v organizacích, bez ohledu na jejich právní formu a předmět činnosti, pro zajištění ochrany informací, např. ČSN EN ISO/IEC 27001 „Informační bezpečnost, kybernetická bezpečnost a ochrany soukromí – Systém managementu informační bezpečnosti – Požadavky" a ČSN EN ISO/IEC 27001 27002 „Informační bezpečnost, kybernetická bezpečnost a ochrany soukromí – Opatření informační bezpečnosti".

Jde o standardy tzv. „informační bezpečnosti", v rámci kterých organizace řeší ochranu citlivých dat a informací buď na základě svého autonomního rozhodnutí (informace považuje za významné a důvěrné), nebo je musí chránit ve smyslu regulatorních požadavků státu (např. osobní údaje). **Ochranná opatření informační bezpečnosti** se standardně dělí následovně:

- organizační opatření = opatření na úrovni vnitřních předpisů a pokynů,
- opatření v oblasti lidských zdrojů = opatření na úrovni HR,
- opatření fyzické bezpečnosti = opatření na úrovni fyzického zabezpečení prostor, vybavení a fyzických přístupů k nim,
- technologická opatření = opatření na úrovni HW a SW a kyberprostoru.

Potřeba přijetí jednotlivých opatření v konkrétní akademické instituci by měla být posouzena s ohledem na její hlavní a vedlejší činnosti a aktuální výzkumné projekty na základě interního vyhodnocení potřeby ošetřit konkrétní reputační a finanční rizika či zvýšená rizika ovlivnění vnitřních samosprávných procesů. Rozhodnutí o přijetí bezpečnostních opatření bude zcela v kompetenci akademické instituce a měla být zaváděna vždy důsledně účelně a pouze **přiměřeně k pojmenovaným a vyhodnoceným rizikům a jejich dopadům**.

Opatření institucionální odolnosti v akademických institucích a nastavení systému řízení rizik pro zvýšení bezpečnosti výzkumu budou mít dopady do kompetencí různých útvarů instituce. **Průnik jednotlivých agend**, kterých se zabezpečení důvěryhodného výzkumu bude dotýkat, lze vyjádřit schematicky takto:



IV. PŘÍKLADY OPATŘENÍ NA POSÍLENÍ BEZPEČNOSTI VÝZKUMU

ORGANIZAČNÍ OPATŘENÍ

Organizační opatření budou spočívat zejména ve zpracovávání interních směrnic a pravidel.

Interní směrnice by měly řešit zejména následující:

- **nastavení základních politik a cílů** bezpečnostní agendy v instituci, zajištění personálních a finančních zdrojů a nastavení kompetencí, což bude úkolem vrcholového vedení institucí – půjde o deklaratorní dokument nejvyššího vedení s vyslovením závazku k zavádění a zlepšování ochranných opatření pro zvýšení bezpečnosti výzkumu v dané instituci,
- **identifikaci vlastních potřeb a rizik**, která bude spočívat zejména v následujícím:
  - provedení důsledné klasifikace citlivých dat, informací a výstupů, tedy takových údajů, které akademická instituce chrání jako předmět znalostí v rámci citlivé oblasti výzkumu a vzdělávání, nebo z vlastního rozhodnutí, případně na základě regulatorního požadavku státu,
  - identifikace citlivých oblastí výzkumu a vzdělávání ve smyslu **Metodického doporučení pro spolupráci s třetími stranami**, tj. zhodnocení zvýšeného rizika při provádění výzkumu v projektech týkajících se:
    - kritických technologií významných pro ekonomickou bezpečnost EU,

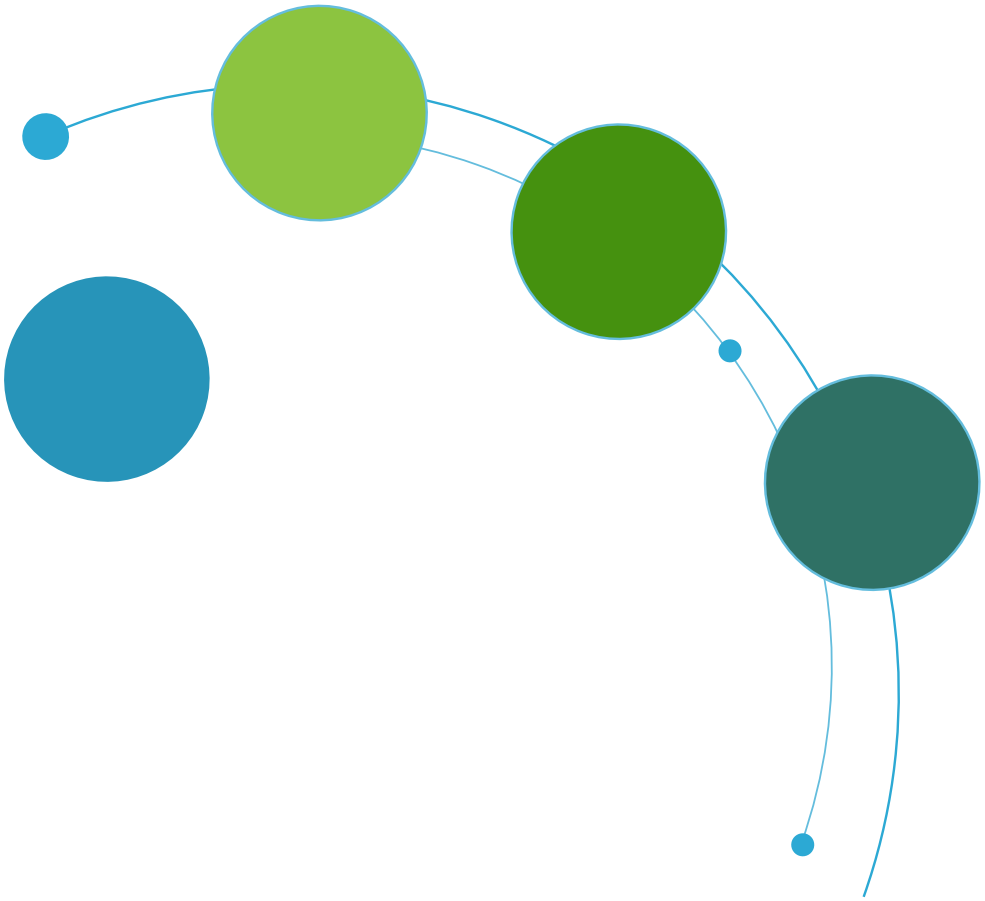
  - kontrolovaných položek dvojího užití ve smyslu evropské a národní legislativy, tj. zboží, SW a technologií, které lze použít jak pro civilní, tak i/samostatně vojenské účely,
  - civilního bezpečnostního výzkumu, regionálních studií a aplikovaného výzkumu,
  - spolupráce s třetími stranami s vysoce rizikovými zeměmi,
  - dalších oblastí dle rozhodnutí akademické instituce,
- identifikace činností, které instituce realizuje v rámci svých aktivit, včetně administrativních, při nichž je nakládáno s citlivými daty/informacemi a/nebo se týkají citlivých oblastí výzkumu a vzdělávání, včetně rizikové mezinárodní spolupráce na daném pracovišti,
- popis oběhu citlivých dat a informací na pracovištích, v laboratořích a systémech instituce,
- monitoring regulatorních omezení plynoucích z mezinárodních sankcí a případných povinností s prověřováním příchozích zahraničních investic, např. při vstupu zahraničního investora do spin-off, resp. právních předpisů v oblasti ochrany proti bezpečnostním hrozbám a rizikům,

- **řízení mezinárodní spolupráce**, které bude spočívat v následujícím:
  - nastavení interních pravidel pro hodnocení rizikovosti mezinárodní spolupráce z pohledu nelegitimního ovlivňování, které by mělo vycházet z hodnocení kombinace hlavních rizikových faktorů, kterými jsou:
    - konkrétní oblast výzkumu a inovací, v níž se má konkrétní mezinárodní spolupráce uskutečnit,
    - rizikový profil konkrétního partnera – organizace se sídlem v/mimo EU,
    - rizikový profil země, v níž má partner sídlo, nebo odkud je kontrolován či vlastněn, přičemž bližší doporučení k nástrojům pro hodnocení rizikovosti konkrétního projektu mezinárodní spolupráce je rozpracováno v **Metodickém doporučení pro spolupráci s třetími stranami**,
  - přenesení rozhodování o rizikové spolupráci na vyšší úroveň,
  - posouzení potřeby a provedení auditu stávajících mezinárodních spoluprací v rámci konkrétních projektů, pokud se realizují v citlivých oblastech výzkumu a vzdělávání,
  - hodnotit rizika spojená s nelegitimním ovlivňováním u projektů pro začínající vysokoškolské a výzkumné pracovníky a pracovnice, zejména v rámci zahraničních stáží,

- **ošetření rizik**, které bude spočívat v nastavení opatření na posílení bezpečnosti výzkumu zejména pro citlivé oblasti výzkumu a vzdělávání, a to:
  - nastavení systému autorizací a přístupů k jednotlivým citlivým datům a informacím podle jejich povahy, umístění a míry rizikovosti, s přihlédnutím k zásadě „potřebuji vědět" a za účelem zajištění důvěrnosti, dostupnosti a integrity takových dat,
  - nastavení či revize interních pravidel realizace mezinárodní spolupráce, a to jak ve vztahu k aktivitám instituce, tak jednotlivých vědeckých pracovníků a pracovnic,

- přijetí pravidel pro **omezení či zákaz tzv. technické pomoci a nehmotného přenosu technologií** v oblasti kontrolovaných položek dvojího užití; technickou pomocí ve smyslu evropské legislativy může být i poskytování vysokoškolského vzdělávání a provádění aplikovaného výzkumu,
- vypracování či revize interních předpisů pro **zajištění správy a ochrany duševního vlastnictví instituce**; ošetření autorských práv, převedení majetkových práv na akademickou instituci, zajištění licenční smluv před publikováním, patentová a další ochrana průmyslových práv apod.,
- přijetí pravidel pro **uzavírání memorand a smluv pro realizaci mezinárodní výzkumné a akademické spolupráce** se zeměmi se zvýšeným bezpečnostním rizikem, či jejich institucemi:
  - uzavírání rámcových dokumentů pro zakotvení záruk vyváženosti a reciprocity spolupráce, jako např. vzájemné sdílení a využívání dat,
  - závazná ujednání ve smlouvách o spolupráci na projektu – zejména ohledně způsobu využití výsledků dané spolupráce, ošetření autorství a majetkových práv, zajištění finančních smluvních závazků, včetně podmínek ukončení spolupráce,
- **řešení informační bezpečnosti ve vztazích s dodavateli** zařízení, zdrojů a služeb souvisejících s prováděním výzkumu, ale i zboží a služeb pro provozní potřeby akademických institucí,
- řízení rizik spočívajících v **ohrožení dobrého jména** akademické instituce i reputace jejích pracujících, a to:
  - zhodnocení rizika ohrožení dobrého jména instituce, týmů a pracujících z důvodu výzkumné i diplomatické spolupráce se zeměmi se zvýšeným bezpečnostním rizikem a nastavení pravidel pro vedení takové spolupráce či přenesení rozhodování o takové spolupráci na vyšší úroveň,
  - zhodnocení rizika ohrožení dobrého jména instituce, týmů a pracujících z důvodu vědecké i nevědecké spolupráce se soukromou sférou, tj. v rámci zakládání spin-off, převodu nehmotného majetku, vstupů či účastní v právnických osobách, včetně spolků, a nastavení pravidel pro vedení takové spolupráce či přenesení rozhodování o takové spolupráci na vyšší úroveň,
  - řízení poskytování záštit nad vědeckými a společenskými projekty, konferencemi a dalšími akcemi, včetně pronajímání prostor instituce,
- nastavení pravidel pro **pořádání vědeckých konferencí, vzdělávacích akcí i diplomatických a společenských setkání** a návštěv, kde se předpokládá účast neakreditované veřejnosti či přítomnost osob ze zemí se zvýšeným bezpečnostním rizikem, nebo jde o jednání ve věcech týkajících se citlivé oblasti výzkumu a vzdělávání, např. podle pravidel v **Metodickém doporučení pro spolupráci s třetími stranami**,
- **plnění postupů stanovených závaznými právními předpisy** ve věci zadávání veřejných zakázek, GDPR, ochrany oznamujících (whistleblowing), a podle oboru hlavní činnosti a aktuálních projektů i z důvodu mezinárodních sankcí, kontrolních režimů, povinnosti prověřování zahraničních investic a dalších závazných pravidel na ochranu proti bezpečnostním hrozbám a rizikům,

- nastavení postupů pro **řešení konkrétních bezpečnostních incidentů**, zejména pro podávání zpráv o pozorovaných či podezřelých událostech, pro přijímání nápravných opatření potřebných k odstranění příčin a zavedení systému hodnocení účinnosti bezpečnostních opatření a realizace jejich změn,
- **řízení dokumentovaných dat** a informací souvisejících s citlivými oblastmi výzkumu a vzdělávání, spočívající v systému vytváření a aktualizací dokumentů (identifikace, formát a nosič dokumentu) a zajištění jejich ukládání, dostupnosti pro oprávněné přístupy i likvidaci,
- vedení vhodné **interní komunikace** za účelem podpory agendy institucionální odolnosti v instituci i nastavení ochranných opatření v souvislosti s **mediální komunikací**, založených zejména na přístupech k citlivým datům a rozhodování o jejich použití.



OPATŘENÍ V OBLASTI LIDSKÝCH ZDROJŮ

Opatření v oblasti lidských zdrojů se budou týkat zejména HR pracovníků a pracovnic, avšak jejich implementace bude dopadat na všechny vedoucí pracovníky, protože bezpečnostní pohled by se měl promítat do řídících činností ve všech úrovních řízení.

Půjde zejména o následující opatření:

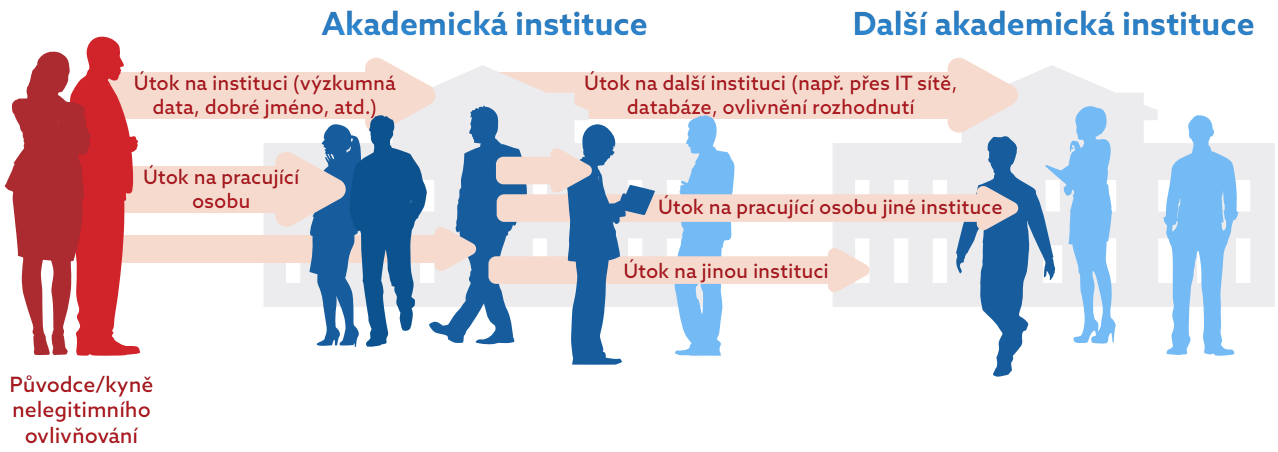
- při náboru **nových zaměstnanců a zaměstnankyň/spolupracovníků a spolupracovnic, při změnách a ukončování** pracovního poměru hodnotit hledisko ochrany odolnosti instituce; promítnutí postupů do interních pravidel v oblasti HR,
- promítnutí odpovědnosti pracujících za informační bezpečnost do **pracovních smluv**, využívat dohody o mlčenlivosti,
- nastavení bezpečnostních opatření na ochranu informací při zpracování a ukládání dat **při práci na dálku**,
- vyhodnocení potřeby a možností právní regulace jednání pracovníků a pracovnic **ve veřejném prostoru včetně kyberprostoru**, např. zpřístupňování údajů o práci pro akademické pracoviště na sociálních sítích či aktivity v online příspěvcích; doporučuje se využívat doložky o mlčenlivosti,
- nastavení **pravidel pro zahraniční cesty** zaměstnanců a zaměstnankyň do rizikových destinací podle **Metodického doporučení pro spolupráci s třetími stranami**,

- promítnutí požadavků na ochranu výzkumu proti bezpečnostním hrozbám do **etických kodexů** akademických institucí, zejména v souvislosti s respektováním základních lidských práv, ochranou principů nestrannosti a nezávislosti na ideologických a politických tlacích či zájmech a podporou důvěryhodného výzkumu,
- **zpracování školicích programů** pro bezpečnostní manažery, manažerky, náborové pracovníky a pracovnice, resp. realizovat vzdělávání v oblasti institucionální odolnosti pro nové zaměstnance a zaměstnankyně s ohledem na jejich pracovní pozice a náplně,

- zvyšování povědomí o problematice bezpečnosti výzkumu a vlivu nelegitimního ovlivňování na dobré jméno instituce i reputaci výzkumných pracovníků a pracovnic za účelem pochopení **osobní odpovědnosti každého pracovníka a pracovnice akademické instituce**, neboť platí, že:
  - **každá osoba má přístup k citlivým informacím**, které mohou být cílem nelegitimního zájmu třetí strany, protože informace, které jsou pro někoho bezcenné, mohou mít velkou cenu pro někoho jiného,
  - **každá osoba se může stát předmětem zájmu** (nelegitimního ovlivňování), protože rozhodnutí, zda se třetí strana zaměří přímo na konkrétního zaměstnance či zaměstnankyni, nemůže zaměstnanec ani zaměstnankyně nijak ovlivnit,
  - **každá osoba se může bránit**, protože jsou k dispozici nástroje, jak nelegitimní ovlivňování rozeznat, jak se zachovat a na koho se obrátit.

Nesprávným rozhodnutím může pracující poškodit nejen svoji reputaci, ale i dobré jméno domovské instituce nebo poškodit jinou akademickou instituci a/nebo další osoby.

Povědomí o rizicích nelegitimního ovlivňování se týká všech!



OPATŘENÍ V OBLASTI FYZICKÉ BEZPEČNOSTI

Opatření v oblasti fyzické bezpečnosti budou znamenat taková opatření, která již mohou být zavedena v rámci agendy správy budov a požární bezpečnosti, avšak bude třeba je přehodnotit i z pohledu agendy institucionální odolnosti, a to zejména pro zajištění ochrany citlivých dat a informací.

V rámci fyzické bezpečnosti lze zavádět například:

- opatření pro **fyzické vstupy do zabezpečených oblastí** (oddělení, laboratoří apod.) a práci v nich,
- opatření pro přístupy k zařízení a vybavení, které jsou využívány při činnostech v citlivých oblastech výzkumu a vzdělávání,
- opatření pro zajištění **fyzického zabezpečení kanceláří a vybavení**, včetně ochrany proti fyzickým hrozbám vůči infrastruktuře,
- opatření na **ochranu měkkých cílů**, včetně využití technologických opatření pro **systémy varování** a předávání informací,
- stanovení pravidel pro **nakládání s nosiči informací**,
- opatření na ochranu vybavení instituce mimo pracoviště ve smyslu pravidel pro používání a ukládání svěřeného majetku,
- další, i podle doporučení odborníků a odbornic na ochranu budov a bezpečnost měkkých cílů.

TECHNOLOGICKÁ OPATŘENÍ

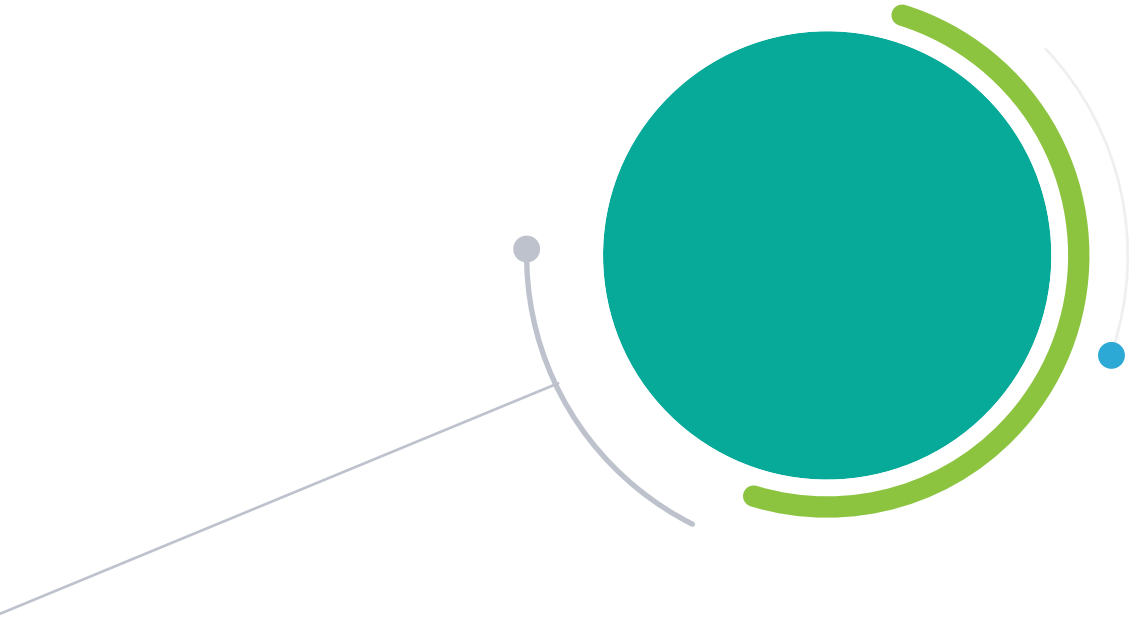
Technologická opatření jsou nebo budou realizována v rámci kompetencí IT útvarů akademických institucí nebo na základě dodávek a služeb IT v souvislosti s řešením kybernetické bezpečnosti.

Podle mezinárodních standardů pro systémy bezpečnosti informací je kybernetická bezpečnost užší podskupinou informační bezpečnosti, protože se týká ochrany informací v kyberprostoru. Implementace nových opatření pro zajištění kybernetické bezpečnosti proto neznamená vždy či pouze implementaci nových ICT zařízení a systémů, ale nese zároveň či samostatně potřebu opatření v oblasti organizační, HR a/nebo fyzické ochrany budov a zařízení.

Opatření kybernetické bezpečnosti bude potřeba přehodnotit a doplnit i z pohledu ochrany institucí proti nelegitimnímu ovlivňování a za účelem posílení bezpečnosti výzkumu, a to zejména zavedením:

- **řízení autorizací a přístupů** k citlivým a chráněným datům v elektronické formě v souladu s organizačními opatřeními, řízení přidělování a používání přístupových práv a jejich bezpečná autentizace,
- **zabezpečení integrity dat** (uchování a dosažitelnosti), včetně maskování dat, v souladu s organizačními opatřeními týkajícími se přístupů k informacím,

- zabezpečení **důvěryhodných služeb a dodávek** ICT,
- **zabezpečení koncových zařízení** uživatelů a uživatelek, řízení používání výměnných médií,
- **zvyšování opatření kybernetické bezpečnosti** a řešení technických zranitelností, ať již na základě povinné implementace evropské legislativy NIS2, zejména:
  - přístupy ke zdrojovým kódům,
  - ochrana před škodlivým softwarem, řízení instalací SW,
  - bezpečnost síťových služeb,
  - řízení technických zranitelností,
  - bezpečné programování a vývoj,
  - používání kryptografie,
  - provádění auditů kybernetické bezpečnosti,
- průběžné hodnocení účelnosti příslušných opatření pro konkrétní instituci či výzkumný projekt,
- a další podle odborníků a odbornic na kybernetickou bezpečnost.



ZÁVĚR

Má-li systém opatření na posílení bezpečnosti výzkumu dosáhnout zamýšleného výsledku a napomoci upevnění důvěryhodnosti výzkumu a vysokoškolských a výzkumných institucí v ČR, bude implementace účinných opatření vyžadovat adekvátní finanční a kapacitní zdroje.

EK v **Návrhu Doporučení Rady k posílení bezpečnosti výzkumu** vyzývá členské státy, národní orgány i jednotlivé akademické instituce, aby pro posílení bezpečnosti svého výzkumu mobilizovali stávající finanční zdroje. Zároveň je třeba očekávat, že kritérium bezpečnosti výzkumu se v budoucnu stane nedílnou součástí schémat podporujících mezinárodní výzkumnou spolupráci.

S ohledem na uvedené se agenda institucionální odolnosti bude muset do činnosti vysokoškolských a výzkumných institucí promítnout. Zpočátku si implementace této agendy vyžádá zvýšenou pozornost, avšak následně se stane běžnou součástí práce výzkumných i administrativních pracovníků a pracovnic a nebude představovat vyšší zatížení ani z pohledu personálního ani finančního. Naopak by měla poskytnout záruky pro stabilní rozvoj a prostor pro důvěryhodnou spolupráci.