Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

Příloha č. 1 Opatření rektora R 632

Nelegitimní ovlivňování na JU a jeho hlášení

Účel a kontext

Mezinárodní spolupráce, otevřenost a akademické svobody jsou základními elementy excelentního výzkumu, vývoje a inovací. Právě tyto elementy však zároveň mohou činit akademické prostředí (tedy především vysokoškolské a výzkumné instituce) obzvláště zranitelné vůči nelegitimnímu ovlivňování. S rostoucím mezinárodním napětím a zvyšujícím se geopolitickým významem výzkumu, vývoje a inovací musí dnes akademické instituce v rámci své mezinárodní spolupráce stále častěji čelit rizikům spojeným s **nelegitimním ovlivňováním**.

Co je nelegitimní ovlivňování a institucionální odolnost?

Nelegitimní ovlivňování je **nežádoucí působení na lidi, rozhodování nebo procesy**. Zahrnuje vlivové působení cizí moci, ale také kriminální (např. korupční) jednání a nežádoucí nebo nezákonné lobbování. **Obvykle jde o aktivity, které jsou skryté, klamavé, vynucující či korupční.** Tyto aktivity mohou ohrožovat a poškozovat nejen zájmy Jihočeské univerzity, vysokoškolského a výzkumného prostředí, ale i **širší chráněné zájmy ČR** (např. bezpečnostní, obranné, ekonomické nebo politické).

Institucionální odolností proti nelegitimnímu ovlivňování se rozumí schopnost akademické instituce zavést a realizovat **systém opatření k posílení bezpečnosti výzkumu** proti nelegitimnímu ovlivňování a na ochranu jejího dobrého jména. Tento systém spočívá zejména v odpovědné mezinárodní spolupráci, která zahrnuje dodržování závazných sankčních omezení a přiměřené prověřování zahraničních partnerů, dobré 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 či vojenského užití, ale také ve výzkumu s rizikem zneužití osobních údajů nebo znalostí či technologií k porušování lidských práv a svobod.

Nelegitimní ovlivňování může pro JU představovat významná provozní, bezpečnostní, právní, finanční a reputační rizika. Může vést k **narušení rozhodování a interních procesů** nebo **zasažení do duševního vlastnictví, know-how a citlivých informací** (například výsledků výzkumu, neveřejných smluvních informací a osobních údajů). V krajních případech může jeho vlivem dojít k **porušení právních povinností** (např. závazných sankčních režimů), což může mít dopady v podobě vzniku sporů a hrozby finančních ztrát. Nelze také opomenout nemalá **reputační rizika**, včetně ohrožení spolupráce se spolehlivými zahraničními partnery, ohrožení akademické svobody a otevřenosti výzkumu a důvěry ve výsledky a data instituce. Mezi reputačně-rizikové aktivity lze zařadit také záštity či účasti na různých

odborně se tvářících akcích, fakticky se skrytou agendou anebo organizované subjektem představujícím reputační riziko. Nelze také pominout rizika ovlivňování výuky, především v sociálně-vědní oblasti. Je také důležité si uvědomit, že finanční rizika nemusí být nutně svázány jen s porušením sankcí právně závazných v ČR, ale také těch nezávazných, např. prostřednictvím ztráty možnosti podílet se na nějakém prestižním grantu financovaném ze zahraničí kvůli tomu, že zahraniční poskytovatel musí dodržovat pro něj právně závazné sankce, které ale zároveň v ČR právně závazné nejsou.

Posilování institucionální odolnosti znamená **budování této odolnosti a zvyšování obezřetnosti**. Schopnost uvědomit si včas rizika a rozpoznat podezřelé jednání je klíčová. Funkční systém je tak kombinací institucionálního zabezpečení (interní předpisy, procesy, popis rizik a jejich řízení, proškolení zaměstnanců a studentů) a osobní odpovědnosti každého jednotlivce. **Naše informovanost a všímavost je tak fundamentálním předpokladem** k tomu, abychom možným hrozbám dokázali čelit efektivně a včas.

Kdo může být cílem?

Kdo všechno může být cílem vlivových aktivit? Jsme to potenciálně my všichni z řad členů akademické obce i mimo ni. **Každá osoba přicházející do kontaktu s akademickou institucí** je potenciálně zajímavá – student či studentka, stážista či stážistka, vysokoškolský a výzkumný pracovník či pracovnice, další zaměstnanci či zaměstnankyně, ale i ostatní osoby podílející se na činnosti akademické instituce. Je to proto, že **jako pracovníci akademické instituce máme přístup k celé škále citlivých informací, které mohou být zneužity proti chráněným zájmům instituce, akademického prostředí nebo celé ČR**. Kromě toho **někteří z nás mohou ovlivnit důležité procesy či osoby, na čemž může mít cizí moc zájem**. V některých případech se můžete se stát „jen“ **nástrojem** útočníka **k ovlivňování někoho jiného**.

Je to **náš přístup k citlivým informacím, výzkumným či jiným interním procesům, nebo dalším osobám, co nás činí pro útočníky zajímavými**.

Rozpoznávání podezřelých situací

Jak poznám, že jsem se stal cílem nelegitimního ovlivňování? V absolutní většině existujících případů bylo těm, kteří se stali cílem nelegitimního ovlivňování či jejich nejbližšímu okolí, zřejmé, že dochází k nějaké anomálii – že **je „něco špatně“, případně „jinak“, než je v obdobných situacích běžné**. Dostali například **nabídky, které vypadaly příliš dobře na to, aby byly opravdové** a za kterými se často opravdu skrýval nekalý úmysl. Nebo dostali **nabídky, které museli promyslet v časové tísni**. Taková strategie útočníka sází na vyvolání tlaku na rychlé rozhodování, a tudíž nižší ostražitost a promyšlení celé věci. Úplný popis technik nelegitimního ovlivňování lze najít v kapitole 6 dokumentu Protivlivový manuál pro

sektor vysokých škol. Některé specifické scénáře nelegitimního ovlivňování demonstruje také série videí na stránce Trusted Research – Implementation Scenario Videos.

Je také třeba poznamenat, že bezpečnostní incident se nemusí stát jen na půdě JU, můžete být kontaktováni také na služební cestě nebo soukromých cestách, na společenských akcích, při nahodilých setkáních či v jiných situacích mimo pracovní prostředí. Mezi typické situace, které následně vedou či mohou vést k oslovení za účelem získání pro spolupráci, patří např. přímé oslovení ke spolupráci, zinscenovaný incident, neformální jednání za zvláštních okolností, dárky či další výhodná pozvání. Nejen odborné či zdvořilostní zahraniční návštěvy na půdě JU, ale také výměnné programy, konference a další mezinárodní setkání jsou často využívaným vstupním bodem jak pro oslovení jednotlivých akademiků, tak pro umožnění nebo usnadnění zahraničních cest a pobytů cizích státních příslušníků v ČR, kteří se vydávají za akademiky či členy jejich doprovodného personálu.

Hlášení incidentů

A co mám dělat, **pokud se mi něco takového stane** nebo to zpozoruji u někoho jiného?

Pokud:

- máte pocit, že se Vás snaží někdo **ovlivnit nebo na Vás vyvíjí nátlak** (v nějaké situaci se vůči Vám chová nebo jedná neodpovídajícím způsobem, například se nadměrně vyptává na Váš výzkum, interní procesy apod.),
- **jste dostali nápadně výhodné nabídky spolupráce** (pozvání na akce, nepřiměřené dary, hrazené zahraniční cesty a školení),
- se někdo skrze Vás nebo Vaše kolegy snažil získat nebo získal **neoprávněný přístup k důvěrným informacím**,
- **si nejste jistí, zda určitá nestandardní situace**, která se stala Vám nebo Vašim kolegům, a která může neoprávněně zasahovat do interních procesů nebo rozhodování na fakultě nebo JU, je **pokusem o nelegitimní ovlivnění** a působení cizí moci,

informujte Bezpečnostního manažera JU.

Kontaktní adresa: protivliv@jcu.cz

Stručně popište, o jakou situaci šlo, kdy a kde se stala a kdo byl jejím účastníkem (kdo byl přítomen, kdo Vás kontaktoval).

Bezpečnostní manažer JU Vás pak požádá o schůzku a vyplní s Vámi **formulář Hlášení bezpečnostního incidentu, který je k dispozici v samostatné příloze opatření.** Případně můžete tento formulář vyplnit rovnou a poslat na uvedenou adresu (i tak se s Vámi Bezpečnostní manažer JU zkontaktuje a celou situaci s Vámi osobně probere).

Důležité je **nenechat si informaci o možném probíhajícím pokusu o nelegitimní ovlivňování pro sebe** a incident opravdu nahlásit. Podobně se na Bezpečnostního manažera JU lze obracet v situacích, kdy existenci rizik předvídáte, např. před pracovní či soukromou cestou do nějaké rizikové země (viz také následující příloha), před podpisem smlouvy, v níž se Vám nezdají nějaké pasáže, při přípravě společných výzkumných projektů s rizikovými partnery nebo také v průběhu přijímacího řízení osoby ke studiu či zaměstnání, u níž se můžou vyskytovat rizika. Jedním z hlavních cílů budování institucionální odolnosti totiž není jen řešit již nastalé ať již skutečné či domnělé incidenty/anomálie, ale také dobrat se stavu, kdy větší část akademické obce JU bude o rizicích přemýšlet již dopředu a bude je chodit konzultovat. Ultimátním cílem pak je to, aby i rizikové spolupráce mohly probíhat, jen bezpečněji jak pro JU, tak i pro členy její akademické obce.

Shrnutí základních principů

Základem zvýšení odolnosti akademické instituce vůči nelegitimnímu ovlivňování je uvědomění si, že cílem nelegitimního ovlivňování či ohrožení bezpečnosti výzkumu se může stát každý. Klíčové rovněž je, že každý musí v takové situaci za své jednání přijmout odpovědnost. Stručně lze shrnout, že:

- **Každý je zajímavý.** Každý může disponovat přístupem k určitému množství citlivých informací (nebo rozhodovacích pravomocí).
- **Každý je zranitelný.** Každý, kdo má přístup k citlivým informacím (nebo má rozhodovací pravomoci), se může stát cílem nelegitimního ovlivňování a zda se tak stane, nezáleží na něm.
- **Každý může požádat o pomoc.** Pokud se již někdo stane cílem nelegitimního ovlivňování, má možnost situaci řešit s pomocí dalších osob. Včasné oznámení může být nejúčinnější prevencí vzniku škod.

JU se díky Vašemu odpovědnému přístupu stane odolnější vůči nelegitimnímu ovlivňování a celkově bezpečnějším prostředím nejen pro výzkum. Taková odolnost umožní lépe reagovat na rizikové situace, předcházet jim a minimalizovat případné následky. Vaše chování může být **dobrým příkladem a inspirací** pro Vaše kolegy a další instituce.

Příloha č. 2 Opatření rektora R 632

Pravidla chování na zahraničních cestách

Účast na zahraničních konferencích, stejně jako návštěva zahraničních kolegů na jejich pracovištích, je pro akademické a výzkumné pracovníky integrální součástí jejich profesionálních aktivit. S rostoucím mezinárodním napětím a zvyšujícím se geopolitickým významem výzkumu a inovací tak roste potřeba důkladně posoudit rizika příslušných cest, zejména pokud se týkají zemí, jejichž demokratické a etické hodnoty se liší od našich, a to nejen před jejich uskutečněním, ale i po návratu.

Tento text má za cíl krátce představit možná rizika a hrozby na zahraničních cestách, a poskytnout základní rady a doporučení, jak takovým možným výzvám čelit. Týká se zejména:

- Účasti na konferencích a jiných vědeckých setkáních.
- Výuky.
- Návštěv akademických a výzkumných pracovišť.
- Návštěv neakademických partnerů, jako jsou byznysoví nebo průmysloví partneři.

Tato pravidla se týkají zejména **krátkodobých pobytů (pracovních cest) plně financovaných JU**. Netýkají se primárně dlouhodobějších pobytů spojených s výzkumem, jako jsou terénní práce či stáž, nebo pobytů (částečně) financovaných třetí stranou – ty budou řešeny samostatně (i když řada doporučení popsaných níže se může hodit i na dlouhodobější pobyty).

Co zvážit před cestou?

Před každou zahraniční cestou je třeba si uvědomit, že různé země mohou mít rozdílné/ý:

- Chápání demokracie a etických principů.
- Chápání akademické svobody (stupeň ochrany akademických svobod v dané zemi se pokouší kvantifikovat tzv. Index akademické svobody).
- Pravidla omezující spolupráci stanovená sankčními opatřeními ČR, EU, OSN apod. nebo i plynoucí z pravidel dané země.
- Kulturní a právní prostředí.

Před každou zahraniční cestou spojenou s vědou a výzkumem (ale i výukou) bychom toto měli zvážit ve spojení s důvodem naší cesty. Měli bychom se tedy ptát:

- Jaká je v dané zemi ochrana akademických svobod?
- Podléhá země závazným relevantním sankcím?
- Může být náš výzkum vzhledem k dané zemi citlivý?

- Mohou být naše odborné zaměření či aktivity v dané zemi pro nás samotné rizikem? Např. pokud by mohly být vnímány v rozporu s tradicí, pravidly nebo dokonce právem dané země.

Na každou zahraniční cestu je tedy nutné se pečlivě připravit. Kromě standardních záležitostí jako mít schválený cestovní příkaz, správný typ víza (je-li potřeba) a adekvátní pojištění, je potřeba uvážit řadu dalších aspektů:

- Musíte si s sebou brát veškerý svůj výzkum, který máte ve svém notebooku nebo je z Vašeho notebooku nechráněně přístupný? V některých zemích mají úřady právo přístupu do Vašeho notebooku a zkopírování veškerého jeho obsahu, někdy to však mohou udělat, aniž o tom víte (viz také další doporučení níže).
- Není téma, o kterém chcete mluvit, a to i neformálně, nějak omezeno nařízeními JU (např. citlivý výzkum či chráněné duševní vlastnictví) nebo smlouvami JU s třetími stranami (např. smluvní výzkum, kdy dané téma můžete prezentovat pouze s výslovným souhlasem třetí strany)?

Elektronika a data

Všichni si (nejen) na zahraniční cesty bereme notebook a mobilní telefon. To je v pořádku a bez toho to nakonec ani nejde. Je třeba ale zvážit, jaké pracovní a osobní informace obsahují a jaké by to mělo pro nás a pro JU důsledky, kdybychom něco z toho ztratili, bylo nám ukradeno, nebo bylo „jen“ zkopírováno. Před každou cestou do vysoce rizikové země (seznam těchto zemí uvádíme níže v Příloze č. 4) proto požadujeme konzultovat Vaši cestu a elektroniku, kterou si zamýšlíte brát, s Manažerem kyberbezpečnosti JU. To vám objasní a doporučí, jaká Vás mohou čekat rizika, jak Vaše data zabezpečit, jak se ze zahraničí bezpečně připojit na JU, zda Vaše technika bude na místě vůbec fungovat, ale také Vám nabídne vzít si na cestu pouze čistá zařízení s nejnutnějším obsahem pro Vaši cestu. Mezi hlavní doporučení patří:

- Někdy se vyplatí pořídit si místní telefon a tarif.
- Mějte vaše zařízení zaheslované, ideálně každé jiným heslem.
- Umožňuje-li některá vaše aplikace dvou-faktorové ověřování, zapněte si jej.
- Budete-li si brát vlastní notebook, uvažte ještě před cestou zálohování a odstranění (tedy přesun na jiné médium) dat a informací, které nebudete potřebovat nebo jsou vysoce citlivé.
- Zálohujte si před odjezdem obsah svého mobilního telefonu.
- Na JU se připojujte primárně přes VPN.
- Ujistěte se, že všechny vaše aplikace jsou aktualizované, antivirus je zapnutý, automatické spuštění USB při jeho vložení do notebooku je vypnuté, a notebook se automaticky nepřipojuje k Wi-Fi (IT oddělení v tomto jistě rádo poradí).
- Nikdy nestahujte aplikace od neoficiálních poskytovatelů.

- Po návratu kontaktuje IT oddělení, zkonzultujte s nimi průběh cesty a předejte jim veškerou techniku k prověření.

Pokud už jste v dané zemi a nikdo se na Vás hned na letišti nebo v hotelu očividně nepřilepí, můžete snadno získat pocit, že nikoho nezajímáte a nic Vám nehrozí. Stále však pečlivě vážte všechny Vaše aktivity, ať už spojené s cílem Vaší návštěvy (věda, výzkum, výuka) nebo s volným časem (kouření nebo pití alkoholu na veřejnosti, nevhodné oblékání, zejména (ale nejen) u žen, prohlížení si nějaké demonstrace nebo policejní či vojenské techniky stojící v ulici apod.). Nemohou Vás vystavit nějakému nebezpečí, vnějšímu tlaku, poškození reputace Vás, JU nebo dokonce ČR?

Chování při zahraničních cestách

Doporučujeme:

- Připravte se na to, že můžete čelit neobvyklým požadavkům, např. můžete být dotazováni až tlačeni ke sdílení informací o citlivějších oblastech Vaší práce. To Vás jistě postaví do velmi nekomfortní pozice. Vždy reagujte zdvořilým, avšak pevným odmítnutím.
- Zvažte pečlivě, co uděláte s případnými dary, zda případné hodnotné dary musíte někde deklarovat.
- Zvažte pečlivě, co případně podepisujete (zda se například nezbavujete nějakých práv nebo někomu něco tímto nedáváte), a v případě nejistoty kontaktujte Útvar právní Rektorátu JU.
- Uvědomte si, že veřejné a hotelové Wi-Fi připojení nemusí být bezpečné a zvažujte, jaké informace budete přes tato připojení sdílet. Zejména se vyhněte zadávání přihlašování svým JU účtem nebo např. používání svého internetového/mobilního bankovnictví. Používání veřejných Wi-Fi je rizikové obecně, nejen ve vztahu k pracovním aktivitám, protože může dojít ke kompromitaci zařízení jako takového bez ohledu na to, zda je používáno k pracovní nebo soukromé činnosti. Minimálně je tedy vždy vhodné použití VPN.
- Všímejte si neobvyklého chování Vašich zařízení a s nikým Váš notebook, telefon ani USB disk nesdílejte.
- Buďte opatrní se všemi IT dárky jako například USB disky. Je bezpečnější je přijmout, poděkovat a nenápadně se jich zbavit.
- Svoje USB nikdy nepřipojujte do jiného zařízení, ani cizí USB do Vašeho.
- Vždy mějte elektroniku a citlivé materiály u sebe. Ani hotelový trezor nezaručuje zcela bezpečné uložení.
- Přemýšlejte, komu a jaké informace o sobě a o své práci sdělujete.
- Buďte ostražití, pokud Vás někdo zve na akci, která je zadarmo, nebo se objeví nabídka, která vypadá příliš dobře na to, aby byla reálná.

Vždy platí, že pokud se stane něco neobvyklého nebo podezřelého, **informujte** (už během nebo až po návratu podle Vašeho posouzení závažnosti) **Vaše nadřízené a Bezpečnostního manažera JU** (**viz Nelegitimní ovlivňování na JU a jeho hlášení – hlášení incidentů**) a zvažte předčasný návrat.

Konference či jiná vědecká setkání jsou mimořádnou příležitostí k výměně zkušeností a informací, ale také k navázání nové spolupráce. Vždy je však třeba, zvláště pak v dnešní době, mít na paměti bezpečnostní rizika s takovými cestami spojená. Na každou zahraniční cestu je tak i po této stránce více než žádoucí se dobře připravit.

Můžete se podívat také na stránku Trusted Research Countries and Conferences Guidance

Příloha č. 3 Opatření rektora R 632

Seznam vysoce rizikových zemí

Následující seznam obsahuje země:

- s indexem akademické svobody vyšším než 0,1, které jsou na sankčním seznamu – modře,
- s indexem akademické svobody menším než 0,1, které jsou na sankčním seznamu – červeně,
- s indexem akademické svobody menším než 0,1, které nejsou na sankčním seznamu – černě.

Index akademické svobody i sankční seznam se může v čase měnit. Bezpečnostní manažer JU může zejména s ohledem na zahraničně-bezpečnostní situaci po schválení kolegiem rektora rozhodnout o úpravě tohoto seznamu. O tomto rozhodnutí musí informovat jednotlivé součásti JU.

Haiti
Somálsko
Demokratická republika Kongo
Středoafrická republika
Libye
Ukrajina (okupovaná území, vč. Krymu)
Súdán
Jemen
Zimbabwe
Rusko
Venezuela
Sýrie
Írán
Jižní Súdán
---------- 0,1 (hodnota indexu akademické svobody)
Kuba
Egypt
Afghánistán
Tádžikistán
Rovníková Guinea
Saudská Arábie
Čína
Turkmenistán
Rwanda
Bělorusko
Eritrea
Myanmar/Barma
KLDR
Nikaragua