



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

Výstupy dílčí části projektu:

1. Doporučení pro zabezpečení kolaborativní platformy, včetně doporučení pro její pokročilé nastavení.
2. Popis procesů bezpečného předávání a dlouhodobého uchovávání studijních dokumentů.
3. Model bezpečné správy studijních dokumentů.
4. Soubor doporučení pro ověřování identity a monitoring průběhu ověřování znalostí vysokoškolských studentů v online prostředí, včetně SZZ.



Projekt NPO – komponenta 3.2.1

Specifický cíl C2: Bezpečnost distančních forem výuky

Jihočeská univerzita v Českých Budějovicích
Branišovská 1645/31a
370 05 České Budějovice
IČ: 60076658



Financováno
Evropskou unií
NextGenerationEU

MŠMT
MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



Národní
plán
obnovy

IDENTIFIKAČNÍ ÚDAJE

Název dokumentu:	Název výstupu. Specifický cíl C2: Bezpečnost distančních forem výuky
Vydala:	Jihočeská univerzita v Českých Budějovicích 2023
Adresa:	Branišovská 1645/31a, 370 05 České Budějovice IČ: 60076658 www.jcu.cz
Zpracoval:	Bc. Eduard Krlín, vedoucí Útvaru správy informačních systémů Centra informačních technologií Jihočeské univerzity v Českých Budějovicích
Verze:	1
Přílohy:	č. 1 Doporučení pro zabezpečení kolaborativní platformy č. 2 Studijní dokumenty JU č. 3 Analýza rizik spojená se studijními dokumenty č. 4 Popis procesů bezpečného předávání a dlouhodobého uchování studijních dokumentů č. 5 Distanční formy výuky – data č. 6 Model bezpečné správy studijních dokumentů č. 7 Právní doporučení pro ověřování identity a monitoring průběhu ověřování znalostí vysokoškolských studentů v online prostředí č. 8 Soubor doporučení pro ověřování identity studentů a jejich znalostí Výše zmíněné přílohy nejsou s výstupem doloženy. Jedná se o dokumenty, které není možné zveřejnit zejména z bezpečnostních důvodů. Současně pracovní skupina v čele s koordinující VŠ na výstupech a přílohách i nadále pracuje a nejedná se tedy o finální verzi.
	 EVROPSKÁ UNIE Evropské strukturální a investiční fondy Operační program Výzkum, vývoj a vzdělávání  MŠMT MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY  Národní plán obnovy
Licence:	 Tento výstup lze užit v souladu s licenčními podmínkami Creative Commons BY-SA 4.0 International (http://creativecommons.org/licenses/by-sa/4.0/legalcode).



OBSAH

IDENTIFIKAČNÍ ÚDAJE	1
OBSAH.....	2
1 ÚVOD.....	3
2 BEZPEČNOST DISTANČNÍCH FOREM VÝUKY	3
2.1 DOPORUČENÍ PRO ZABEZPEČENÍ KOLABORATIVNÍ PLATFORMY, VČETNĚ DOPORUČENÍ PRO JEJÍ POKROČILÉ NASTAVENÍ.	3
2.2 POPIS PROCESŮ BEZPEČNÉHO PŘEDÁVÁNÍ A DLOUHODOBÉHO UCHOVÁVÁNÍ STUDIJNÍCH DOKUMENTŮ.....	4
2.3 MODEL BEZPEČNÉ SPRÁVY STUDIJNÍCH DOKUMENTŮ.	4
2.4 SOUBOR DOPORUČENÍ PRO OVĚŘOVÁNÍ IDENTITY A MONITORING PRŮBĚHU OVĚŘOVÁNÍ ZNALOSTÍ VYSOKOŠKOLSKÝCH STUDENTŮ V ONLINE PROSTŘEDÍ, VČETNĚ SZZ.	5



1 ÚVOD

Jihočeská univerzita v Českých Budějovicích (JU) se do projektu NPO ve specifickém cíli C2 s názvem „Bezpečnost distančních forem výuky“ zapojila zejména přebíráním výstupů a jejich implementací na JU. Dále se JU aktivně zapojila do pracovní skupiny 5, která řešila právní aspekty bezpečnosti distančního vzdělávání.

Celý projekt byl zaměřen na komplexní zajištění bezpečnosti distančních forem výuky, včetně přímo návazných činností, a to jak z technického, tak i procesního hlediska, na základě již existujících doporučení, standardů, postupů či metodik.

Na JU bylo implementováno či doporučeno implementovat řešitelským týmem JU mnoho opatření. Řešitelský tým JU se krom výstupů uvedených níže v kapitole 2 zaměřil i na další výstupy vzniklé z projektu a mnoho z nich rovněž implementoval, případně předal odpovědným osobám na JU. A to zejména materiály vzniklé v rámci pracovní skupiny 5, ve které byla JU aktivně zapojena.

2 BEZPEČNOST DISTANČNÍCH FOREM VÝUKY

2.1 Doporučení pro zabezpečení kolaborativní platformy, včetně doporučení pro její pokročilé nastavení.

V rámci realizace výstupu č. 5 projektu SC C2 NPO došlo ve formě dotazníkového šetření k detailní analýze stávajících či pro nasazení vyhovujících component kolaborativní platformy pro podporu distančního vzdělávání na zapojených VVŠ. Primární důraz byl však po celou dobu realizace tohoto výstupu kladen na vytvoření doporučení pro jejich patřičné zabezpečení z pohledu kybernetické a informační bezpečnosti za pomoci implementace ověřených způsobů ochrany. Eliminace nežádoucích vnějších vlivů či systémových rizik plynoucích ze současné praxe bylo dosaženo za pomoci kombinace pokročilého nastavení bezpečnostních mechanismů zvolené kolaborativní platformy a uplatňování bezpečnostních politik splňujících požadavky na realizaci distančního vzdělávání.

V rámci tohoto výstupu a přebírání výsledků se JU zaměřila především na následující oblasti:

Komunikační platforma – cloudové prostředí M365 od společnosti Microsoft

JU využívá v případě online a hybridní výuky v drtivé většině případů prostředí M365 a to zejména aplikaci MS Teams, která je dostupná pro různé operační systémy jak pro počítače, tak pro mobilní zařízení či jako webová aplikace. MS Teams umožňuje komunikaci pomocí chatů, audio či videohovorů, a to i s více účastníky. Dále disponuje úložištěm v MS Sharepoint a dalším velkým množstvím komponent (OneNote, Booking, atd.)

V prostředí JU jsou týmy v MS Teams sloužící pro výuku zakládány výhradně pomocí API přes studijní informační systém IS/STAG. Čímž je zajištěna integrita zejména v přístupu vyučujících a studentů, kteří jsou do týmu zapisováni automaticky a dochází k pravidelné synchronizaci.

V rámci výstupu pracovní skupiny byla připravena sada doporučení, jak prostředí M365 zabezpečit. Jelikož je prostředí M365 velice živé, tak jsou doporučení dostupná on-line a jsou neustále aktualizována. Tato doporučení byla rovněž představována na několika seminářích.

Veškerá doporučení byla předána správcům prostředí M365 na JU, kteří daná doporučení průběžně implementují. Správci na JU se rovněž pravidelně účastnili uvedených seminářů.

Dále v rámci této části projektu došlo k úpravě zabezpečení elektronické pošty na JU, která je provozována rovněž v prostředí M365, a to pomocí autentizace pošty - SPF, DKIM, DMARC a ARC, jenž napomáhá při rozlišování zpráv od legitimních a nelegitimních odesílatelů. Uvedená opatření jsou navíc v případě systému spadajících pod zákon o kybernetické bezpečnosti povinná.



Learning Management System (LMS)

JU využívá jako LMS open source software Moodle. V průběhu roku 2023 došlo k upgradu na long-term support verze 4.1, pro kterou trvá podpora až do prosince 2025. JU v rámci projektu implementovala doporučení vydaná v metodice pracovní skupiny PS5.

Primárně jsou pro přihlašování používány IdM účty a je využívána autentizační metoda Shibboleth. Manuální účty jsou využívány jen v nezbytně nutných případech. Požadavky na hesla u ručně vytvořených účtů byly nastaveny dle doporučené metodiky.

Dále bylo upraveno nastavení rolí a fotografií, rovněž dle metodiky PS5.

Příloha č. 1 – Výstup číslo 5 - Doporučení pro zabezpečení kolaborativní platformy, včetně doporučení pro její pokročilé nastavení.

2.2 Popis procesů bezpečného předávání a dlouhodobého uchování studijních dokumentů.

Studijní dokumenty lze pro účely tohoto výstupu chápat jako záznamy událostí souvisejících s jednotlivými studenty a jejich studiem na VVŠ. Tyto dokumenty byly v tradičním pojetí uchovávány v listinné podobě v tzv. „složce studenta“. Pojem studijní dokumenty může být v současnosti poněkud matoucí, neboť mimo tradiční písemnosti zahrnuje také data, která jednotlivé události zaznamenávají ve studijních informačních systémech (SIS), obvykle ve formě databázových záznamů (typickým případem jsou záznamy o absolvovaných zkouškách studenta). Z těchto dat často vznikají dokumenty (listiny) pouze v reakci na konkrétní žádosti studentů (např. potvrzení o studiu, výpis studijních výsledků) nebo v případě, kdy univerzita vystupuje vůči studentovi jako orgán veřejné moci, a forma dokumentu je tedy při komunikaci vyžadována (např. rozhodnutí o ukončení studia).

V rámci tohoto výstupu proběhla identifikace základních dokumentů, které vznikají v rámci studijní agendy během studia na JU. Pro každý dokument jsou evidovány rámcové informace o původu dokumentu, způsobu vytvoření, zajištění původu, integrity a doba archivace. Uvedené identifikace jsou v Příloze č. 2 - Studijní dokumenty JU.

Dále proběhla analýza rizik v souvislosti se zpracováním studijních dokumentů na JU. Analýza je dostupná v příloze č 3 - Analýza rizik spojená se studijními dokumenty JU. Součástí analýzy je i návrh cílového stavu a doporučených opatření. Tato analýza byla konzultována a ve finální verzi předána manažerovi kybernetické bezpečnosti JU pro další zpracování do směrnic a postupů na JU.

Příloha č. 4 – Výstup číslo 13 - Popis procesů bezpečného předávání a dlouhodobého uchování studijních dokumentů.

2.3 Model bezpečné správy studijních dokumentů.

V rámci tohoto výstupu nejprve proběhla analýza využívaných řešení na JU, a to v rámci dotazníku, který sloužil pro zmapování potřeb v rámci celého projektu NPO SC C2 na JU. Výsledky šetření jsou detailně zpracovány v příloze číslo 5 – Distanční formy výuky.

Tento výstup navazoval plynule na výstup předcházející, a tak byl zaměřen především na záznamy událostí souvisejících s jednotlivými studenty a jejich studiem na VVŠ. Výstup byl zaměřen na řízení přístupů, doporučení k verzování dokumentů a evidenci změn, včetně auditních záznamů v systému studijní agendy, jímž je na JU informační systém IS/STAG. V rámci pracovní skupiny PS 3 vznikl soubor doporučení, který je v příloze číslo 6 - Model bezpečné správy studijních dokumentů. Na JU byla na základě těchto doporučení provedena revize spisového řádu, viz příloha číslo 2 a analýza rizik, viz příloha číslo 3. Dále byl soubor doporučení týkající se identifikace, autentizace, autorizace, auditování, verzování a přidělování přístupů



předán kompetentním osobám na JU. Na JU byla také zahájena příprava na zavedení více faktorové autentizace do studijního informačního systému. Rovněž proběhla kontrola a ověření správného auditování a logování událostí ve studijním informačním systému dle doporučení PS3.

2.4 Soubor doporučení pro ověřování identity a monitoring průběhu ověřování znalostí vysokoškolských studentů v online prostředí, včetně SZZ.

V rámci tohoto výstupu došlo nejprve k průzkumu výchozího stavu ověřování identity a monitoringu průběhu ověřování znalostí vysokoškolských studentů v online prostředí pomocí dotazníkového šetření. Dotazníkové šetření proběhlo na JU individuálním způsobem a následně byl odevzdán jeden vyplněný dotazník pracovní skupině 4, která následně dotazníky zpracovala napříč VVŠ a provedla jejich vyhodnocení. Výsledky šetření jsou v příloze č. 8.

Dále v rámci pracovní skupiny 5 vznikl soubor právních doporučení k online examinaci. Na podobě dokumentu se JU aktivně podílela. Ve finální verzi byl dokument předán pověřeným osobám na JU. Uvedený dokument je v příloze č. 7 - Právní doporučení pro ověřování identity a monitoring průběhu ověřování znalostí vysokoškolských studentů v online prostředí.