Univerzita Palackého
v Olomouci

ZPRAVODAJ

Centra výpočetní techniky

číslo 2 | březen 2016

Úvodní slovo

Vážení čtenáři,

druhé číslo Zpravodaje Centra výpočetní techniky Univerzity Palackého se vedle představení novinek z oblasti IT na UP zaměřuje i na praktické otázky spojené s kybernetickou bezpečností a na problematiku plagiátorství a jeho odhalování. Věříme, že vybraná témata budou pro vás zajímavá a přínosná.

Za tým Centra výpočetní techniky Vám přeji mnoho úspěchů v letním semestru akademického roku 2015/2016.

David Skoupil

ředitel CVT

Obsah

Aplikace Helpdesk

Začátkem letního semestru byla spuštěna nová aplikace Helpdesku, která nahradila stávající Helpdesk v Portálu. Ten byl nedostatečně flexibilní a neodpovídal potřebám současného uživatele.

Helpdesk bude nejprve určen primárně pro zaměstnance univerzity, časem se však plně zpřístupní i studentům. Studenti i zaměstnanci do programu budou moci zadávat své požadavky i „anonymně“. Přihlásit se do aplikace bude možné portálovým ID a heslem.

Helpdesk obsahuje celou řadu nových funkcionalit, jako je například fulltextové vyhledávání nebo funkční přehled řešení problémů. Řešitelé si budou moci mezi sebou snadno úkol předat. Nespornou výhodou této aplikace je responzivní design, díky jemuž je aplikace funkční na mobilních zařízeních. ▪

IDM

IDM, neboli identity management, je systém, který umožňuje automatizovat a zefektivnit správu uživatelů, uživatelských účtů a oprávnění.

Při přijetí zaměstnance do pracovního poměru nebo studenta ke studiu je třeba provést celou řadu nastavení v různých systémech. Uživateli je třeba založit portálový účet, účet v Active Directory, poštovní schránku v systému Exchange nebo Office 365, zpřístupnit síť Eduroam a provést řadu dalších úkonů. To v současném stavu trvá nezřídka i několik dní. Systém managementu identit má za cíl tento postup maximálně automatizovat a zrychlit.

Základním zdrojem dat pro IDM jsou systémy SAP, STAG a databáze externistů. Systém bude zaveden v první polovině roku 2016. ▪

SharePoint

Microsoft SharePoint je komplexní webová platforma umožňující efektivní spolupráci uživatelů. V minulém roce byl SharePoint na UP v testovacím provozu. V roce 2016 je již plně dostupný všem zaměstnancům Univerzity Palackého.

SharePoint nabízí nepřeberné množství funkcí. Základním rysem je možnost ukládat a spravovat dokumenty on-line prostřednictvím nástrojů Word, Excel či PowerPoint. Nad jedním dokumentem přitom může pracovat současně více uživatelů, aniž by docházelo k přepisování verzí a konfliktům. Jednotliví uživatelé si mohou vymezit, na jaké části dokumentu budou pracovat. SharePoint, jak již z názvu vyplývá, je také místem pro sdílení souborů. Soubory je možno sdílet například se skupinou uživatelů, jež náleží k danému projektu či pracovní skupině. Samozřejmostí je možnost nastavení různých uživatelských oprávnění.

Do počítače lze složky se soubory ze SharePointu i synchronizovat a se soubory pak pracovat off-line, po připojení se úpravy automaticky promítnou na server a v dokumentech se zaznačí, kde byly změny provedeny. Výhodou jsou také notifikace, které si lze přiřadit k jednotlivým souborům nebo složkám. Při jakékoli změně dokumentů pak přijde uživateli e-mailové upozornění.

Ve spolupráci s oddělením komunikace jsou na SharePoint přidávány např. normy univerzity a jednotlivých fakult. Při hledání konkrétní normy, je možno využít fulltextové vyhledávání. Vámi hledaný pojem bude hledán nejen v názvech souborů, ale i v obsahu souborů samotných. SharePoint je dostupný pro všechny zaměstnance UP na adrese https://files.upol.cz/. Pro přihlášení je třeba využít stejné údaje jako při přístupu do portálu. ▪

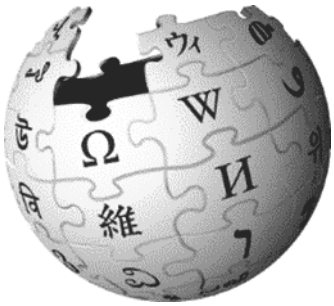
Univerzitní Wiki

V loňském roce přišla studentská skupina Rise UP v čele s Johnem Gealfow, členem akademického senátu Univerzity Palackého, s nápadem vytvořit studentskou wiki encyklopedii, která by obsahovala důležité informace pro stávající, ale i budoucí studenty.

Ve spolupráci s CVT a oddělením komunikace se tak spustil projekt oficiální univerzitní wiki.

Cílem wiki Univerzity Palackého je sjednocení informačních materiálů univerzity, od často kladených dotazů po návody pro připojení k internetu.

Zároveň má komplexně popsat aspekty studentského života. Naopak propagace soukromých subjektů, které nejsou součástí univerzity, záměrem wiki není. Obsah je tvořen týmem studentů a Centrem výpočetní techniky.



Články obsahující oficiální informace budou od komunitních vizuálně odděleny. V současnosti je tento informační portál plně funkční a je postupně doplňován informacemi.

Velmi důležitou částí Wiki jsou IT návody a manuály. Nalezneme zde například návody pro připojení k Wi-Fi, VPN nebo pro nastavení e-mailových klientů.

Tyto návody byly původně rozprostřené napříč různými univerzitními weby. Na wiki jsou teď k dispozici studentům i zaměstnancům v aktualizované podobě, a to v češtině i angličtině.

Kromě návodů obsahuje IT část wiki informace o identifikačních kartách ISIC, o přístupu k informačním zdrojům, o bezpečnosti a antivirové ochraně, ale také o možnostech stažení aktuální verze Microsoft Office 365 zdarma.

Do wiki mohou přispívat všichni uživatelé na UP, do redakčního systému se lze se přihlásit pomocí stejných přihlašovacích údajů jako na portál.

Veškeré nové příspěvky však nejprve musí projít kontrolou a schválením administrátorů, aby se zamezilo vkládání nevhodných nebo chybných informací, jež by se na této platformě neměly objevovat.

Vzhledem ke komunitní povaze wiki dejte v případě protichůdných nebo nejasných informací vždy přednost oficiálním materiálům publikovaným na stránkách univerzity.

Potenciálním přispěvatelům je k dispozici manuál jednotného stylu psaní článků na wiki. Uživatelé mají navíc možnost vkládat články týkající se například kultury, turistiky atd. do rozcestníku nazvaného *Volná témata*.

Wiki je dostupná na adrese: https://wiki.upol.cz/ ▪

Digitální podpis

Pokud jste si někdy povzdechli nad tím, že své dokumenty v počítači nebo e-maily nemůžete podepsat, tak pro vás máme řešení, v podobě tzv. digitálního podpisu, který v kybernetickém prostředí nahrazuje vlastnoruční podpis.

Digitální podpis zajistí, že jste dokument podepsali právě vy a že dokument nebyl dodatečně někým změněn. Po technické stránce se jedná o speciálně vytvořená data, která uživatel připojí k jakémukoli dokumentu nebo e-mailu. Pro vytvoření digitálního podpisu je třeba vlastnit tzv. certifikát, ve kterém je uložen speciální podpisový klíč.

Public Key Infrastructure

Digitální podpis je založen na technologii *Public Key Infrastructure*, což je systém digitálních certifikátů a certifikačních autorit. Certifikační autorita vydává nebo odvolává certifikáty, spravuje jejich seznamy a garantuje, že certifikát vydala pouze té osobě nebo tomu subjektu, jehož jméno je v certifikátu uvedeno. V případě zneužití nebo krádeže dat pro tvorbu elektronického podpisu může majitel certifikátu zažádat o jeho zneplatnění.

Proč vlastně digitálně podepisovat e-maily

Vyvstává otázka, proč digitálně podepisovat elektronickou poštu. Počítačová pošta vznikla v dobách, kdy byl internet malým a bezpečným místem. Mechanismy, používané pro přenos e-mailů internetem tak nejsou připraveny na současné bezpečnostní hrozby.

Uživatelé si mnohdy neuvědomují, že je například velmi snadné odeslat email s podvrženou adresou odesílatele. Může se snadno stát, že někdo bude posílat e-maily vaším jménem. Teprve digitální podpis zaručí, že e-mail opravdu odeslal ten, jehož e-mailová adresa je uvedena v záhlaví.

Certifikát na Univerzitě Palackého

Studenti a zaměstnanci Univerzity Palackého si mohou vygenerovat *osobní certifikát TSL*, a to na stránkách *CESNETu*. Certifikační autoritou pro vydávání tohoto certifikátu je americká společnost *DigiCert*.

Certifikáty TSL jsou dostupné všem organizacím zařazeným v národní akademické federaci identit eduID.cz. Svou identitu při vydání certifikátu uživatel prokáže přihlášením svým uživatelským jménem (doplněným o příponu @upol.cz) a heslem stejným jako pro přístup do portálu UP. Návod pro získání certifikátu je k dispozici na univerzitní wiki.

V České republice poskytují široké veřejnosti kvalifikované digitální podpisy celkem tři certifikační autority: První certifikační autorita, Česká pošta a eIdentity. Jsou zákonem uznávané a plně nahrazují písemný podpis. Certifikáty vydávané CESNETem písemný podpis z pohledu zákona nenahrazují.

Jak e-mail digitálně podepsat

Využíváte-li poštovní klient Microsoft Outlook, je vložení digitálního podpisu snadné. V *Možnostech* vyberete *Centrum zabezpečení*, poté kliknete na *Nastavení centra zabezpečení*, kde přejdete do nabídky *Zabezpečení e-mailu*. Zde si nejprve svůj certifikát importujete a poté nastavíte, zda chcete šifrovat všechny odchozí e-maily či nikoliv.

V Mozille Thunderbird si digitální podpis nastavíte v *Nástrojích*, předete do *Nastavení účtů*, odkud si vyberete možnost *Zabezpečení* a v sekci *Digitální podpis* a vyberete svůj certifikát, který do vašeho e-mailového klienta chcete vložit. ▪

Kybernetická kriminalita

Počet internetových trestných činů se od roku 2011 výrazně zvýšil. Za kybernetickou kriminalitu se považuje využití počítačového hardwaru nebo softwaru k nelegální, trestné činnosti.

K této trestné činnosti patří všeobecně známé pirátství, stalking, šíření pomluv, DDoS útoky, ale také kyberšikana, krádeže dat platebních karet, hospodářská kriminalita, šíření dětské pornografie nebo šíření rasové nesnášenlivosti. Pachateli jsou obvykle organizované skupiny, jednotlivci zneužívající citlivá data společností k vlastnímu obohacení, teroristé či státy vedoucí takzvanou informační válku.

Nové formy kyberkriminality

V posledních letech se objevují nové druhy podvodů, např. phishing nebo pharming. Nezkušení uživatelé internetu mohou byt těmito podvody poměrně snadno oklamáni.

Fenoménem se staly útoky prostřednictvím sociálních sítí. Uživatelské účty mohou být napadeny takřka okamžitě po kliknutí na podvodný odkaz. Malware poté např. sleduje, co uživatel na klávesnici píše a poté odesílá jeho uživatelské údaje dál. Podvodníci dále využívají Facebook k vylákání peněz, vydávají za se přítele své oběti a vylákají od ní finanční obnos.

Kyberkriminalita však necílí pouze na jednotlivé uživatele, ale také na firmy či státní instituce.

> Malware je počítačový program, jehož cílem je poškození a vniknutí do systému počítače. Jedná se o souhrnné označení pro počítačové viry, trojské koně či spyware, atd.

Prokazatelnost zločinů na počítačové síti je malá, jelikož se jedná o prostředí, které se neustále mění. Metody pro zajišťování stop kyberkriminality navíc nejsou v současnosti dostatečné.

Stalking

Stalking nebo kyberstalking je dlouhodobé, cílené obtěžování a pronásledování člověka za pomoci technologie, zvláště internetu. Pronásledování obvykle provází křivá obvinění, sledování, krádeže identity či manipulace s daty oběti. Ve většině případů se kyberstalkingu dopouštějí osoby, které svou oběť znají, ne někdo cizí.

Kyberšikana

Kyberšikana je druh šikany, k němuž násilník využívá internetu či mobilního telefonu. Nejčastěji dochází k vytváření dehonestujících webových stránek nebo k rozesílání útočných, urážlivých a pomluvných zpráv.

Phishing

Jedná se o typ podvodu, který využívá e-mailové komunikace k získání citlivých dat uživatele. E-mail vypadá, jako by pocházel ze sociální sítě či platebního portálu. Tyto zprávy obvykle po uživateli vyžadují jak uživatelské jméno a heslo. Phishingu se dá zabránit pomocí digitálně podepsaných mailů, u kterých je jistota, že víme, od koho přicházejí.

Pharming

Tato technika je podobná phishingu. Pachatelé získávají citlivá data od obětí napadením DNS serverů a přepsáním IP adres, čímž přesměrují oběť na falešné stránky internetového bankovnictví, které nejsou rozpoznatelné od originálu. Pokud se stránky nechovají standardně a budou po vás vyžadovat informace, které obvykle nevyžadují, kontrolujte adresní řádek a případně sledujte i certifikáty zabezpečení vaší banky. ▪

Kybernetická bezpečnost

Kybernetických hrozeb, které se netýkají jen jednotlivých uživatelů internetové sítě, ale také státních systémů a kritické infrastruktury, neustále přibývá.

Z tohoto důvodu bylo otevřeno Národní centrum kybernetické bezpečnosti, které zajišťuje prevenci před kybernetickými hrozbami a před útoky namířenými proti subjektům kritické infrastruktury nebo orgánům veřejné správy.

Dále shromažďuje data o počítačových útocích a zastřešuje řešení případných incidentů. Spolupracuje navíc s podobnými pracovišti na národní i mezinárodní úrovni. Jeho pravomoc vychází z mediálně propíraného zákona o kybernetické bezpečnosti.

Budova Národního centra kybernetické bezpečnosti v Brně

Co je to zákon o kybernetické bezpečnosti?

V reakci na aktuální hrozby v kybernetickém prostoru vešel 1. 1. 2015 v platnost zákon o kybernetické bezpečnosti. Do té doby chyběla v České republice systematická organizace přístupu k internetové bezpečnosti, což by mohlo mít za následek ohrožení citlivých dat občanů.

Zákon byl provázen obavami veřejnosti týkajících se omezení soukromí na internetu, ale i protesty proti schválení zákona. Mezi občany České republiky panoval strach ze státem řízené cenzury internetu. Nicméně jednou ze zásad zákona je minimální zásah do práv soukromých subjektů, což znamená, že stát do soukromí soukromých subjektů nebo jednotlivců zkrátka nezasahuje.

Zákon naopak zvyšuje standard bezpečnosti pohybu v kybernetickém prostoru. Vytváří systém opatření, jež mají předcházet výskytu kybernetických bezpečnostních incidentů. Tato opatření mají zajistit, že nedojde k ohrožení fungování informačních a komunikačních systémů.

Bezpečnostní opatření

Zákon má za cíl vybudování systému preventivních bezpečnostních opatření. Dále stanovuje minimální požadavky na zabezpečení systémů kritické informační infrastruktury a významných informačních systémů.

Bezpečné heslo

Dle Vyhlášky o kybernetické bezpečnosti by bezpečné heslo mělo mít minimální délku osmi znaků a obsahovat alespoň tři z následujících prvků: alespoň jedno velké písmeno, alespoň jedno malé písmeno, nejméně jednu číslici a speciální znak. Uživatel by měl heslo měnit po zhruba sto dnech, aby zajistil bezpečnost svého účtu.

Kybernetická bezpečnost

Bezpečnostní hlášení sděluje zodpovědná osoba Národnímu bezpečnostnímu úřadu, který je dále zpracovává. Hlášení dělíme na kybernetické bezpečnostní incidenty a kybernetické bezpečnostní události.

Kybernetická bezpečnostní událost může způsobit narušení bezpečnosti informací, bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací.

Kybernetickým bezpečnostním incidentem se rozumí narušení bezpečnosti informací,

bezpečnosti služeb nebo integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. Dojde-li k takovému incidentu, je nutné jej nahlásit.

Kybernetické nebezpečí

Kybernetické nebezpečí je stav ohrožující ve velkém rozsahu bezpečnost informací, integritu služeb nebo sítí elektronických komunikací, což by mohlo mít za následek ohrožení zájmů České republiky. Stav kybernetického nebezpečí vyhlašuje ředitel Úřadu pro kybernetickou bezpečnost v případě, kdy ohrožení nelze odvrátit.

Kam se řadí Univerzita Palackého?

Univerzita Palackého se v tomto zákoně řadí mezi poskytovatele služeb a provozovatele služeb elektronických komunikací a subjekt zajišťující síť elektronických komunikací (§ 3, písm. a). Na univerzitu se tedy nevztahuje povinnost hlásit incidenty či události.

Zabezpečení připojení na UP

Bezpečnost počítačové sítě UP je mimo jiné zabezpečována připojením k velké infrastruktuře CESNET, která je dále napojena na mezinárodní infrastruktury. CESNET neustále monitoruje své sítě Zaznamená-li CESNET bezpečnostní incident, informuje správce sítě, kteří sjednají nápravu problému.

CESNET rovněž provozuje takzvanou forenzní laboratoř, jež provádí analýzy bezpečnostních incidentů, penetrační a zátěžové testy, bezpečnostní školení, konzultace a analýzy technologií. ▪

CESNET je sdružení vysokých škol a Akademie věd, které provozuje a rozvíjí národní e-infrastrukturu pro vědu, výzkum a vzdělávání. Mimo jiné poskytuje i další služby, například ukládání a zálohu dat, bezpečnost, správu identit, monitoring a měření provozu sítě a konzultace či školení.

Plagiátorství

Co to je plagiátorství?

Plagiátorství je v době internetu rozšířeným fenoménem. Všechny informace se nacházejí na dosah ruky každého uživatele internetu a okopírovat text je velice snadné.

Plagiátorství je vydávání cizího díla za vlastní, popř. převzetí části cizí práce bez uvedení zdrojů. Za plagiát se považuje odevzdání stejné nebo jen částečně pozměněné práce ve dvou a více různých předmětech za účelem splnění studijních povinností.

Odhalení plagiátu se neobejde bez disciplinárního řízení, které může skončit vyloučením ze studia na vysoké škole. Plagiátorstvím porušujete nejen pravidla vědecké etiky, ale také autorský zákon.

Jak se mu vyhnout?

Pokud se chcete vyhnout vytvoření plagiátu, je nutné uvádět zdroje názorů, myšlenek, teorií,

statistik, grafů, ale i přímých citací či parafrázovaného textu, jež ve své práci použijete. Neuvedete-li, že na danou myšlenku přišel někdo jiný, vytvoříte tak plagiát. Jednou z častých příčin plagiátorství je neznalost citačních pravidel.

Citace

Doslovné přepsání textu či myšlenky autora, označené adekvátním citačním odkazem na původní text, musí být v textu graficky odlišeno (např. uvozovkami, kurzívou). Citovat je vhodné, když chcete vyjádřit přímý názor, chcete podpořit vlastní tvrzení nebo v případě, že byste myšlenku nevyjádřili lépe. Citace na půdě Univerzity Palackého podléhají citační normě ČSN ISO 690.

Parafráze

Parafráze je přeformulování textu jiného autora do jiné podoby. Autor původního textu je však buď uveden v poznámkách pod čarou, nebo může být součástí textu, např. Nietzsche ve své knize tvrdí, že […].

Typy plagiátorství

Plagiátorství můžeme rozlišit na několik typů:

Vědomé plagiátorství

Jak již napovídá označení samotné, jedná se o vědomé doslovné opsání nebo zkopírování textu jiného autora s cílem označit text za vlastní. Motivem je často snaha ulehčit si práci.

Nevědomé plagiátorství

Dochází k němu nedostatečným uváděním zdrojů k citovaných a parafrázovaných textů. Texty nejsou utvářeny za účelem podvodu, dochází k tomu často omylem nebo z nedbalosti.

Autoplagiátorství

Jedná se o využití svých vlastních myšlenek z vaší přechozí publikované práce bez správného citačního odkazu. Citace pocházející z vašeho autorského textu by se v práci měly objevit maximálně z 20%. ▪

Odhalování plagiátů

Masarykova univerzita v Brně již několik let vyvíjí systémy, které mají za úkol utvořit jednotné uložiště vysokoškolských závěrečných prací. Toto uložiště zároveň slouží k odhalování plagiátů.

Theses.cz

Theses.cz je národním registrem závěrečných prací, který od roku 2008 slouží pro odhalování plagiátů mezi závěrečnými pracemi. Využívá jej čtyřicet čtyři vysokých škol v ČR.

Veřejnost má přístup buď k záznamům o pracích, nebo k plným textům. Každá škola stanovuje přístupová práva pro zobrazení plných textů závěrečných prací svých studentů nezávisle na sobě. Univerzita Palackého práce svých studentů zveřejňuje.

Program srovnává texty a vyhledává podobnosti ve své databázi. Dále porovnává seminární a jiné práce v systému Odevzdej.cz či vědecké publikace v systému Repozitar.cz. Rovněž vyhledává a zkoumá možné podobnosti i vůči zdrojům z celého internetu.

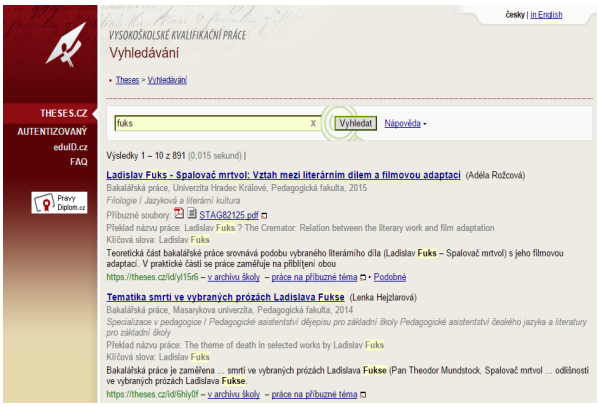
Kromě vyhledávání plagiátů umožňuje Theses.cz

vyhledávání v záznamech o pracích (metadatech) a v textech prací. Nabízí také volitelné zpřístupňování metadat a plných textů prací, kontrolu souborů antivirovým programem, zálohování a převod prací do PDF nebo do *.txt dokumentů.

Propojení se STAGem

Studenti svou kvalifikační práci nahrají do STAGu. U práce je vyplněno datum odevzdání, které do STAGu zadá buď sekretářka katedry, nebo studijní referentka.

Práce se automaticky posílají ke kontrole, obvykle jedenkrát denně, vždy v noci. Theses.cz najde a ukáže podobnost s jinými dokumenty. Výsledky této kontroly jsou staženy do STAGu, nejpozději do dvou dní od nahrání práce do systému. Posuzovatel na základě výsledku vyhodnotí, zda se jedná o plagiát či nikoliv.



Odevzdej.cz

Systém Odevzdej.cz od roku 2009 provozuje Masarykova univerzita a je do něj zapojeno třicet pět vysokých škol a tři střední školy a další instituce. Odevzdej.cz navazuje na Theses.cz a nabízí nejen školám, ale i institucím systém pro odhalování plagiátů. Systém umožňuje odevzdávání prací učiteli, kontrolu podobnosti v textech a vyhledávání textů podobných.

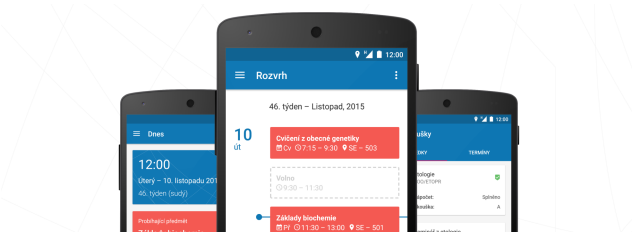
Odevzdej.cz je přístupný takřka komukoliv, můžete do systému vložit váš text a nechat si jej zkontrolovat. Výsledek vám pak bude odeslán na e-mail.

Repozitar.cz

Univerzita Palackého je jednou z dvaceti šesti vysokých škol zapojených do projektu Repozitar.cz. Ten slouží jako meziuniverzitní uložiště děl, ale také jako systém pro porovnávání odborných článků a jiných děl akademiků.

Články jsou systémem poté zpřístupněny širší veřejnosti. Tento projekt má za úkol řešit plagiátorství na úrovni vysokého školství. ▪

UPlikace



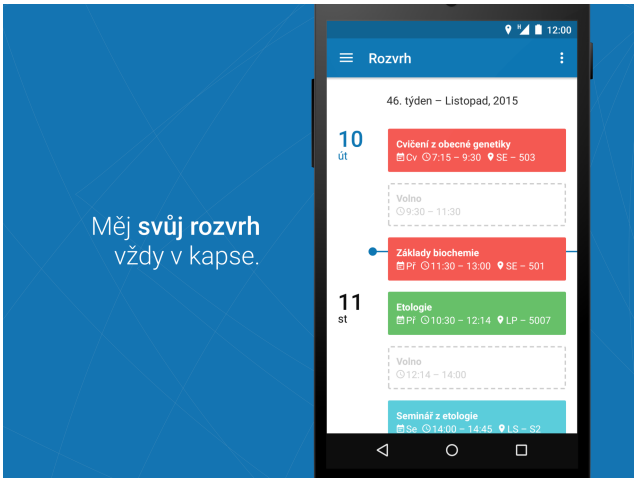
Studenti Univerzity Palackého se začátkem letního semestru dočkají možnosti mít přístup do STAGu prostřednictvím aplikace ve svém mobilním telefonu. Autorem aplikace UPlikace je absolvent Univerzity Palackého Lukáš Novák, který stojí i za projektem mobilní aplikace pro objednávání jídel v menze.

UPlikace bude fungovat na telefonech a tabletech se systémem Android verze 4 a vyšším. Studenti se do aplikace budou přihlašovat stejnými uživatelskými údaji jako na Portálu.

Funkce UPlikace

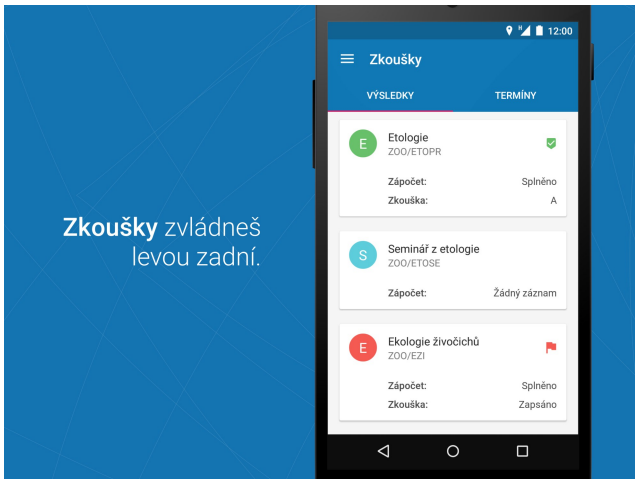
Studenti se mohou prostřednictvím UPlikace dozvědět vše, co souvisí s jejich studiem. Každý uživatel si bude moci zobrazit aktuálně platný seznam zapsaných předmětů v daném

akademickém roce, rozvrh pro daný semestr či seznam aktuálně platných vypsaných zkušebních termínů, včetně data, času, místnosti, zkoušejícího a kapacity volných míst na zkušebním termínu. Zkoušky si budou studenti moci zapisovat i odepisovat pomocí této aplikace.



Součástí aplikace bude rovněž možnost zjištění podrobností o zapsaném předmětu nebo rozvrhové akce jako například popis předmětu, jméno přednášejícího a zkoušejícího, způsob ukončení, počet kreditů atd.

Studenti se například pomocí push-notifikací dozvědí, že jim byla zapsána známka, že se na zkušebním termínu uvolnilo místo nebo že vyučující vypsal termín na zkoušku. Všechna upozornění je možné vypnout a zapnout pro každý předmět zvlášť.



Budoucnost aplikace?

V současnosti aplikace bude sloužit pouze studentům. Vzhledem k velkému zájmu se v budoucnu uvažuje o jejím zpřístupnění i pro zaměstnance univerzity. UPlikace bude samozřejmě dostupná i zahraničním studentům, jelikož bude jak v českém, ale i v anglickém jazyce

Plánuje se také zpřístupnění této aplikace i pro další školy, které využívají STAG, a to pod názvem UniZone. ▪