# Zpráva o stavu a rozvoji IT na 1. LF UK

2021

[Zpráva o stavu a rozvoji IT na 1. LF UK 1](#_Toc86256697)

[1 Fakultní weby 1](#_Toc86256698)

[2 Software a aplikace 2](#_Toc86256699)

[3 Studijní informační systém 4](#_Toc86256707)

[4 Mobilní aplikace pro studenty 6](#_Toc86256714)

[5 Bezpečnost 6](#_Toc86256715)

[6 Správa hardware 10](#_Toc86256720)

[7 Počítačová síť LAN 12](#_Toc86256730)

[8 Bezdrátové sítě 14](#_Toc86256735)

[9 Elektronické přístupové systémy 15](#_Toc86256737)

[10 Kamerový systém 16](#_Toc86256739)

[11 Telefonie 16](#_Toc86256740)

[12 Podpora 3D tisku 17](#_Toc86256742)

[13 Podpora testování 18](#_Toc86256743)

# Fakultní weby

Fakulta provozuje 174 webů, z toho 95 na portálu WebBlast. Pro jeho administraci používá redakční systém, k němuž poskytuje uživatelům školení a monitoring návštěvnosti.

Všechna pracoviště fakulty mají webové stránky v češtině, vyjma BIOCEVu, který má stránky pouze v angličtině. Deseti pracovištím chybí anglická verze webu (většinou jde o společná pracoviště fakulty a nemocnic).

|  |  |
| --- | --- |
| Fakultních webů celkem  | 174 |
| Webů ústavů a klinik | 73 |
| Počet ústavů a klinik s vlastním CZ webem (%): | 99 % |
| Počet ústavů a klinik s vlastním EN webem (%): | 86 % |

Detailní a aktuální přehled webů pracovišť je na stránce: <https://www2.lf1.cuni.cz/weby>

Poslední změny:

* Klinika adiktologie přešla pod WebBlast
* Sexuologický ústav splynul s Psychiatrickou klinikou
* Int1 má nový web, pod redakčním systémem WebBlast
* Int4 má nový web na WebBlastu
* Int3 má nový web na RUK, Document Globe
* Klinika paliativní medicíny – nový web mimo fakultu

Většina webů ústavů a klinik je aktualizována. Podrobnost a obsah webů klesá s jejich „vzdáleností“ od centra. Nejproblematičtější jsou weby společných pracovišť (mimo fakultu).

Fakultní web je plně responzivní, včetně verze mobilní verze a to v obou jazykových mutacích.

# Software a aplikace

## Poštovní služby

Fakulta spravuje přibližně 3700 adres uživatelů s jednotným formátem adresy krestni.prijmeni@lf1.cuni.cz. Z toho je 1900 plnohodnotných schránek a 1800 adres je realizovaných jako automatické přesměrování na jiné účty.

Celkový objem schránek, který se pravidelně zálohuje, je 900 GB. Data uživatelů jsou fyzicky uložená na vlastním diskovém poli fakulty a zálohují se každou noc. Denně systémem projde 20 tis. e-mailů.

V souladu s GDPR je přesměrování omezené jen na jiné univerzitní adresy a na adresy fakultních nemocnic.

Jako spamový a virový filtr používáme službu Antispam-gw. Filtr se automaticky učí podle toho, co uživatelé sami označí jako nevyžádanou poštu – stačí jednoduše došlý mail přesunout do složky SPAM. Druhou úroveň filtrování spamu poskytuje fakultě (resp. univerzitě) sdružení CESNET jakožto svému členu.

Uživatelé mají k dispozici webmail s moderním responzivním rozhraním a server spolupracuje se všemi e-mailovými klienty používajícími standardní protokoly IMAP a SMTP, samozřejmě se šifrovaným TLS přenosem dat. Počáteční nastavení a reset hesla se řeší s využitím centrální autentikační služby UK CAS a stránky asistent.lf1.cuni.cz.

Systém běží ve virtuálním prostředí VMware.

## Přihlašování na sportovní kurzy

<https://sport.lf1.cuni.cz>

Přesun výuky do elektronického prostředí ovlivnil i prostředí sportovní aktivit. V minulých letech bylo obvyklé, že studenti přicházeli na Ústav tělesné výchovy osobně a po diskusi s vyučujícími se písemně zapsali na určitý tělovýchovný předmět či sportovní kurz. Již před pandemií byly snahy přesunout přihlašování na kurzy do elektronické formy a pandemie tuto potřebu ještě zvýraznila.

Vytvořili jsme proto řadu webových aplikací, které umožňují kompletní on-line řešení přihlašování ke sportovním aktivitám a kurzům. Od ověření stavu studenta v SISu, po přihlášení (závazné či jako náhradník), úpravu odeslaných přihlášek a odesílání e-mailových notifikací. Vyučujícím pak webová aplikace umožňuje obvykle přesun studentů z náhradníků mezi závazně zapsané a zpět, označení přihlášky jako neaktivní (smazané), správu variabilních symbolů jednotlivých přihlášek pro účely plateb za kurzy, sledování stavu plateb od studentů a také případnou další editaci přihlášek.

Aplikace je vždy nakonfigurovaná pro aktuální účel a po skončení přihlašování je opět znepřístupněna. Je velmi pravděpodobné, že elektronická forma přihlašování a správy sportovních kurzů na Ústavu tělesné výchovy přetrvá coby nový standard.

## Redcap a TAO

Stále větší zájem je o aplikaci **RedCap** (<https://redcap.lf1.cuni.cz/>) pro online průzkumy a sběry dat od pacientů na klinických pracovištích. Aplikace byla aktualizována na nejnovější verzi. Aktuální počet běžících projektů je 80, počet uživatelů 152. Hlavními uživateli jsou:

* Gynekologicko-porodnická klinika
* Neurologická klinika
* Ústav patologie
* Ústav všeobecného lékařství
* Ústav nukleární medicíny

Zrušili jsme podporu open source projektu TAO of testing: <https://tao.lf1.cuni.cz>.
Systém není dostatečně dokumentován, upgrade obsahuje neplatné odkazy a nebyl výrobcem (v bezplatné verzi) udržován.

## Příležitostné aplikace

### Web pro losování otázek při online zkoušení

Pro online zkoušení bylo třeba zajistit ekvivalent prezenčního losování otázek.
K tomu účelu byl vytvořen systém Losování otázek pro online zkoušení:

<https://los.lf1.cuni.cz/>

Zkoušející i student vidí vylosovaná čísla otázek každý na svém počítači. Zkouška pak může probíhat pomocí některého z videokonferenčních nástrojů.

### Rezervace na testy COVID-19 na Stomatologické klinice

Pro rezervaci zaměstnanců k antigennímu testování na Stomatologické klinice jsme vytvořili rezervační systém:

<https://rezervace.lf1.cuni.cz/covid-stoma>

Může se přihlásit kdokoliv, stačí zadat jméno, email a vybrat si termín. Aplikace potvrzuje rezervaci emailovou zprávou. Odběrové pracoviště má k dispozici seznam rezervovaných.

### Dotazníky studijního oddělení

Na žádost Studijního oddělení jsme připravili dotazníky, umožňující sběr informací: <https://dotazniky.lf1.cuni.cz/zastupci-pro-vyuku>

Uživatel, vyplňující data za pracoviště, se může přihlásit takto: login = heslo = nákladové středisko (např. pro Anatomický ústav je to 110).

Administrace umožňuje aktivaci/deaktivaci formuláře a stažení dat ve formátu CSV.

Pokud pro dané pracoviště ještě neexistuje řádek v databázi, bude vložen. Jinak dojde k editaci stávajícího záznamu.

<https://dotazniky.lf1.cuni.cz/dotaznik2>

Sběr dat pro studijní oddělení. Každé pracoviště může vložit (a následně i editovat) řádky, kterými se přihlašují zaměstnanci na vypsané termíny.

Uživatel, vyplňující data za pracoviště, se může přihlásit takto login = heslo = číslo pracoviště (např. pro Anatomický ústav je to 110).

Administrace umožňuje aktivaci/deaktivaci formuláře a stažení dat ve formátu CSV.

### Formuláře v Office 365

Potřebujeme-li získat nějaká data od studentů či zaměstnanců, první volbou je pokusit se využít existující řešení Microsoftu. Pro tyto účely jsou vhodné formuláře Office 365, kam mají přístup všichni zaměstnanci a studenti

<https://forms.office.com/>.

Respondenti mohou odpovídat anonymně nebo po přihlášení podle toho, zda u konkrétního formuláře potřebujeme znát identitu účastníků.

Využití je velmi široké, řešili jsme takto např.:

* Průzkum proočkovanosti studentů 1. LF proti COVID-19
* Zapojení vědeckých skupin do programu Cooperatio
* Registrace na školení Amboss
* Registraci na Slavnostní udělení čestné vědecké hodnosti doktora honoris causa lékařských věd

# Studijní informační systém

## Integrace SIS a MS Teams

V důsledku zavedení distančních a hybridních forem výuky byl v SIS vytvořen nástroj, který umožní na základě dat o předmětech a rozvrhových lístcích, jejich učitelích a zapsaných studentech vytvářet jedním kliknutím týmy pro předměty a kanály pro studijní skupiny v MS Teams. Žluté tlačítko „Vytvořit tým“ najde v popisu předmětu.

## SIS4

Na rektorátu a v Erudiu pokračuje příprava nového uživatelského rozhraní Studentského informačního systému SIS4. V první etapě jde o moduly pro studenty. Nové rozhraní je Erudiem postupně předáváno k testování studentům. V souvislosti s virtuální mobilitou se v současné době pracuje na převodu přihlášky pro stážisty do SIS4 a na jejím zásadním přepracování.

## Kvalifikované elektronické pečeti, časová razítka

CESNET poskytuje službu pro vzdálené elektronické pečetění kvalifikovanou elektronickou pečetí, vzdálený elektronický podpis a kvalifikované časové razítkování dokumentů. Rozhraní pro tyto služby je tzv. systém RemSig realizovaný Masarykovou univerzitou.
Připravuje se napojení SIS na rozhraní RemSig, dokumenty, které jsou dosud pečetěny elektronickou pečetí uloženou v SIS budou pečetěny přes rozhraní RemSig a orazítkovány kvalifikovaným časovým razítkem.

## Nový způsob přípravy studijních plánů v SISu

Probíhá vývoj programu pro přípravu studijních plánů v SIS. Cílem je zjednodušit přípravu studijních plánů. V polovině roku proběhl distanční seminář o principech vytváření plánů a kontrol studia. Pro některé fakulty, např. MFF, je současný stav vývoje vyhovující, splňuje jejich potřeby a nový program plně využívají. Pro lékařské obory zatím použitelný není. Neumožňuje kontrolovat splnění povinných předmětů po ročnících, ročník je jen doporučený, skupiny povinných předmětů v ročníku nejsou definovány, kontroluje se jen počet kreditů. Program neumí udělat kontrolu před poslední částí státní zkoušky v případě, že je poslední část státní zkoušky pro každého studenta jiná a může se měnit. Vývoj modulu bude pokračovat, připomínky lékařských fakult budou řešeny v další etapě.

## Přechod na novou spisovou službu ESSS

Připravuje se přechod na spisovou službu ESSS k 1.1.2022. V nejbližší době je nutné připravit verzi aplikace Uchazeč pro 1. LF tak, aby mohla být nasazena v okamžiku zahájení příjmu přihlášek a nebylo nutné dodatečné přečíslování přihlášek a zakládání spisů uchazečů.

## Převod agendy Erasmu do SISu

Agenda programu Erasmus+, kterou provozuje UK, bude celá převedená do SISu. Půjde o tři webové moduly, pro přijíždějící studenty, pro vyjíždějící studenty, pro fakultní a univerzitní koordinátory. Součástí řešení bude evidence bilaterálních smluv uzavřených mezi UK a zahraničními VŠ, evidence fakultních koordinátorů Erasmus + a realizace přenosu dat na zahraniční univerzity rozhraním na bázi webových služeb. Proběhly schůzky se všemi fakultami, s 1. LF 23.4.2021, aby se zmapoval současný stav, zkušenosti a připomínky referentů zahraničních oddělení. Pokračuje analýza a úprava datových tabulek.

# Mobilní aplikace pro studenty

Aplikace inteligentního kalendáře (4E Centre).
Hlavním záměrem projektu je:

* Zobrazovat individuální rozvrh každého studenta
* Informovat o místech a časech výuky
* Informovat o změnách v těchto údajích
* Usnadnit studentské hodnocení výuky

Ve spolupráci s externím projektovým inženýrem (ing. Davidem Hybešem) připravujeme zadávací dokumentaci pro výběrové řízení. Proběhla řada konzultací se správci SIS na RUK a řada schůzek s odborníky na mobilní aplikace. Ukázalo se, že má-li mít systém rozumnou životnost, musí být sestaven za použití moderních protokolů a rozhraní a být modulární. Podobně jako řešení na 3. LF bude aplikace ze SISu čerpat data, ale do SISu nebude zapisovat. Správně navržená architektura by mohla být pilotním projektem pro návrh nového SISu.



Obr. 1 Modulární datové schéma připravované mobilní aplikace

# Bezpečnost

Ačkoliv to nemusí být na první pohled patrné, v poslední době prudce narůstá počet online bezpečnostních útoků a hrozeb. Současně se i zvyšují dopady na provoz zasažených institucí.
Útoky využívají zejména nejslabšího článku – koncových uživatelů. Metodami sociálního inženýrství získávají od uživatelů jejich přístupové údaje, které pak zneužívají k přístupům do interních agend.

Zcela novou formu ohrožení představují útoky využívající k sociálnímu inženýrství nátlaku po telefonu. Tyto útoky jsou mimořádně věrohodné a vystavují oběť velkému stresu, ve kterém může přijmout špatné rozhodnutí. Tyto vishing (voice phishing) útoky byly donedávna známé jen ze zahraničí.

Citace ze zprávy NUKIB o bezpečnostní situaci na Českých vysokých školách:
„Vysoká škola ekonomická v Praze se potýkala s ransomwarovým útokem, Masarykova univerzita v Brně zachytila nový malware zaměřený na své uživatele prostřednictvím zacílené phishingové kampaně a Univerzita Palackého v Olomouci detekovala do té doby nezjištěnou formu ransomwaru, která po restartu počítače zašifrovala všechna data.

Nárůst útoků proti českým vzdělávacím institucím odpovídá celosvětovému trendu.

Útoky měly podobu phishingové kampaně v různorodých podobách od jednoduchých, plošně rozesílaných vyděračských e-mailů až po sofistikované a specificky cílené podvodné

e-maily, v nichž se útočníci vydávali za zaměstnance univerzity. Sektor vzdělávání byl přitom nejvíce ze všech sektorů postižen snížením bezpečnostních rozpočtů, ke kterému došlo u 65 % respondentů.“

Pro data instituce jsou nebezpečné zejména ransomwarové útoky, které pomocí podvržených mailů uvedou v omyl nepozorného uživatele a jeho prostřednictvím napadnou i další počítače, jejichž data zašifrují.

Čelit se tomu dá důslednou antivirovou ochranou, segmentací sítě, školením uživatelů, a především nasazováním nových technologií, které aktivně sledují dění v síti. Přesto není otázkou, zda dojde k úspěšnému útoku, ale kdy. Důležitá je proto celá paleta zmíněných opatření včetně zálohování do bezpečných úložišť. Naléháme na uživatele, aby stejně obezřetně zacházeli i se svými daty.

## Bezpečnostní incidenty

Za poslední rok evidujeme devět bezpečnostních incidentů (tj. situací, kdy skutečně došlo ke zneužití prostředků výpočetní techniky útočníkem) a dále celou řadu bezpečností událostí (kdy ke zneužití nedošlo).

Incidenty:

* 6 pracovních stanic napadených malwarem
* 3 e-mailové účty zaměstnanců zneužité k rozesílání nevyžádané pošty

Nejčastější události:

* phishing nebo malware v příloze e-mailů, které prošly spamovým filtrem a nedetekoval je ani antivir na pracovních stanicích
* zranitelnosti pracovních stanic, které jsme sami aktivně detekovali scanováním vnitřní sítě

Přístupové údaje k e-mailu útočníci získali v jednom případě phishingem, ve zbylých případech použili přístupové údaje z prolomené databáze hesel externí webové služby. Uspěli u dvou zaměstnanců, kteří používali jedno **stejné heslo** u všech svých účtů (pracovních i soukromých).

Nejsilnějším vektorem útoků je e-mail. Útočníci jsou schopni překonat spamový filtr a antivirový program na pracovních stanicích tím, že použijí malware tak nový, že ho antivirový program ještě nezná, resp. dokáže ho detekovat až za několik hodin. Pokud během toho intervalu neopatrný uživatel přílohu e-mailu otevře, útočník získá přístup do jeho počítače a odtud i do sdílených úložišť, které jsou k němu připojené (síťové disky apod.).

## Detekce a reakce na ohrožení koncových bodů

**Endpoint Detection and Response** (EDR systém) je kybernetická technologie, která nepřetržitě monitoruje bezpečnostní hrozby u koncových uživatelů a reaguje na ně. Zatímco antivirová řešení pomohou proti známému malwaru, nemohou chránit před zero-day útoky (neznámým malware). Obranu proti tomuto druhu útoku řeší systémy EDR (**Endpoint Detection and Response**).

Pokud dosud neznámý malware projde např. v příloze e-mailu a uživatel přílohu otevře, EDR systém dokáže upozornit na podezřelou aktivitu otevřené přílohy. Správce sítě pak může napadený počítač odpojit od sítě, aby se vir nebo ransomware nešířil, ale současně sám na počítač má po síti přístup a může provést forenzní analýzu. Z EDR systému také získá informaci, na kterých dalších počítačích v síti podezřelý soubor je, a EDR systém na nich otevření souboru blokuje.



Testovali jsme EDR systém **ReaQta** a ukázal se jako velmi přínosný. Testování probíhalo ve spolupráci s Ústavem výpočetní techniky, který EDR systém testoval v síti rektorátu a správy kolejí a menz.

Cena za ochranu 270 PC v síti děkanátu 1. LF UK by byla 400 tis. Kč ročně. Společným postupem s UK se snažíme o optimalizaci výběrového řízení a dosažení nejlepší ceny.

## Projekt CRP-KYBER21

Univerzita Karlova se účastní CRP projektu „**Zvýšení úrovně kybernetické bezpečnosti v prostředí veřejných vysokých škol**“. Z 1. lékařské fakulty jsou dva pracovníci OVT členy realizačního týmu v oblasti osvěty uživatelů a bezpečnosti (Horák, Kajzar). Plánovaným výstupem projektu jsou výukové materiály a kurzy pro školení zaměstnanců v oblasti kyberbezpečnosti.

## Bezpečnostní školení zaměstnanců

Postupující elektronizace a digitalizace procesů a komunikace s sebou nesou rychle narůstající rizika na poli kyberbezpečnosti. Zahájili jsme proto pravidelná školení zaměstnanců na téma bezpečnosti. Proběhla bezpečnostní školení zaměstnanců děkanátu poukazující na nejpalčivější problémy bezpečnosti, zejména chování koncových uživatelů. Školení proběhla prezenčně i online, záznamy a prezentace jsme umístili na stránky fakulty, kde si je mohou pustit ti, kdo školení nestihli.

Průběžně informujeme zaměstnance i studenty o aktuálních rizicích online světa na stránkách e-learning.lf1.cuni.cz, pomocí vyskakovacích bannerů na stránkách WikiSkript, e-mailových zpráv a prostřednictvím fakultních stránek.

V současné době (podzim 2021) připravujeme ve spolupráci s rektorátem na téma kyberbezpečnosti interaktivní online kurz.

Aby byla všechna důležitá bezpečnostní varování na jednom místě a uživatel při pochybnostech nemusel procházet mnoho různých zdrojů, připravujeme rovněž ve spolupráci s rektorátem jednotný web **security.cuni.cz**. Zaměstnanci i studenti zde najdou aktuální doporučení a informace z oblasti kyberbezpečnosti na jednom místě. Sem budou odkazovat i e-maily varující před aktuálními hrozbami nebo odkazy ze školení. Cílem je účinně a rychle distribuovat novinky a znalosti z oblasti kyberbezpečnosti nejen mezi zaměstnance, ale také mezi studenty.

Počet úspěšných útoků pomocí sociálního inženýrství převyšuje jiné, "techničtější" způsoby útoků. Takové útoky jsou levné a při neproškolených uživatelích velmi účinné. Na cíleně napsaný podvodný e-mail může naletět až 70 % nepoučených uživatelů! Opakovaná školení mohou toto riziko významně snížit.

# Správa hardware

## Dokončen přechod na operační systém Windows 10 Education

Dokončili jsme kompletní konverzi všech počítačů v doménové správě (250+ ks) na aktuální verzi operačního systému Windows 10 Education. Společně s tím došlo v minulém období k transformaci operačního systému i na všech počítačích v učebnách (300+ ks) včetně aktualizací instalovaného aplikačního software.

## Centralizace služeb UK

**Plánované zavedení jednotných e-mailových adres na UK**

Probíhá jednání s UVT UK o připravované centralizaci IT služeb (e-maily, active directory). V současné době UVT připravuje technické řešení propojení systémů s cloudem Microsoftu a centrální autentifikační službou UK, které bude nabídnuto fakultám. Přechod a integrace ze stávajících řešení bude techniky i časově náročná záležitost. Výsledkem by měla být jednotná identita uživatelů pro přihlašování do systémů fakulty, univerzity, cloudu a navazujících služeb Microsoftu.

Kolegium rektora UK schválilo na svém zasedání dne 28. 6. 2021 záměr zavedení jednotného

systému e-mailových schránek na UK.

**Cíl úprav**

Cílem navrhované úpravy je sjednocení e-mailových adres, a to jak u studentů, tak u zaměstnanců. Počítá se s využitím účtů Office 365. Primárně bude užívána pro zaměstnance mailová adresa ve tvaru **jméno.příjmení@fakulta.cuni.cz** a pro studenty jméno.příjmení@student.fakulta.cuni.cz, adresa ve tvaru osobníčíslo@o365.cuni.cz bude interní (skrytá).

Výhodou navrhovaného řešení je využití jednotného prostředí Office 365, především sdílené kalendáře, Onedrive a SharePoint pro sdílení dokumentů a MS Teams pro distanční setkávání a výuku.

**Postup a harmonogram realizace**

Přechod do cílového stavu potrvá zhruba dva roky, do pololetí roku 2023.

**Pozice 1. LF UK**

Navrhujeme spojit zavádění jednotných e-mailových adres s přechodem pod centrální active directory (LDAP). To by vyřešilo sjednoceni uživatelských účtů (každý uživatel by měl jeden účet, z CASu) a tím by se přihlašoval do všeho, tj. SSO včetně připojení do cloudu.

## Nové rámcové výběrové řízení na dodávku PC, NB, LCD, tiskáren

V polovině příštího roku uplyne období platnosti stávající rámcové smlouvy na dodávky IT techniky. V první polovině roku bude nutné připravit nové technické zadání pro VZ v režimu otevřeného nadlimitního řízení.

## Plánovaná investice pro rok 2022: Počítačové rotundy v Purkyňově ústavu

Purkyňův ústav – horní a dolní rotunda (mikroskopické sály), Ústav histologie a embryologie a Ústav biologie a lékařské genetiky. V obou patrech je celkově provozováno 120 počítačů z roku 2009. Ústav histologie požaduje zdvojnásobení počtu počítačů, pokud to bude v horní rotundě technicky možné, ze současného počtu 43 ks na 86 ks. Požadovaný stav nových celkem 160 ks. Současné počítače nelze upgradovat a jsou na hraně použitelnosti s OS Windows 10.

Předpokládaná cena cca 6 000 000 Kč s DPH

## Nákup SW podpory v roce 2022 na rok 2023

Na letošní a celý příští rok jsou podpory (support + práva na aktualizace) software zajištěny. Na konci příštího roku bude pořídit podpory pro rok 2023.

Předpokládaná cena 750 000 Kč s DPH

## Plánovaná investice pro rok 2023: Nový server pro virtualizaci

Fakulta používá virtualizační platformu VMware. Na této platformě provozujeme více než 60 virtuálních serverů, na kterých běží prakticky vše, co je na fakultě digitalizováno. V současné době provozujeme hlavní cluster na třech serverech. Na začátku loňského roku byly nahrazeny dva kusy virtualizačních serverů. Třetí server bude nutné nahradit nejpozději do konce roku 2023, kdy končí jeho podpora.

Předpokládaný hrubý odhad ceny je 500 000 Kč s DPH.

## Plánovaná investice pro rok 2023: Primární SAN pole

V polovině roku 2023 skončí platnost podpory stávajícího diskového SAN úložiště. Úložiště uchovává veškerá uložená data virtualizačních serverů. Výrobce umožňuje prodloužení podpory maximálně o další dva roky, avšak za nevýhodného poměru ceny v porovnání s nákupem pole nové generace. Hlavní diskové úložiště je kritická součást infrastruktury, bude nutné naplánovat pořízení nového.

Investice cca. 5 000 000 Kč s DPH.

## Plánovaná investice pro rok 2023: Primární SAN pole

Diskové úložiště SAN je propojeno speciálními aktivními prvky typu NEXUS. Nejpozději v roce 2023 (kdy po 7 letech provozu skončí podpora těchto zařízení) bude potřeba pořídit nové SAN aktivní přepínače (datovou propustností 40/100 GB/s na port) včetně nových výkonnějších trancsieverů.

Odhadovaná cena je 13 mil. Kč

## Plánovaná investice pro rok 2025: Počítačové učebny

V učebnách je celkově provozováno 200 počítačů z roku 2008, kterým v roce 2015 byla rozšířena operační paměť. Předpokládáme udržitelný provoz do konce cyklu OS Windows 10, tj. do roku 2025. S novějším OS již nejsou kompatibilní.

Předpokládaná cena cca 6 000 000 Kč s DPH

## Proběhlo prodloužení licencí antivirového řešení na další dvouleté období

Proběhlo prodloužení licence antivirového prostředí Kaspersky na další dvouleté období.

Antivirové řešení je k dispozici pro všechny osobní počítače, notebooky, servery a chytrá mobilní zařízení v majetku 1. LF UK. Více než 1000 zařízení.

Umožňuje centrální správu, vzdálené aktualizace i nastavení a u mobilních telefonů blokaci, vymazání obsahu a lokalizaci odcizených zařízení.

# Počítačová síť LAN

Datová síť 1. LF UK má topologii dvojité hvězdy, která umožňuje další rozvoj v odlehlých oblastech a současně je odolnější proti lokálním výpadkům než topologie kruhová. Síť prochází rozvojem reagujícím na nové požadavky pracovišť postupnou obměnou, která řeší náhrady zastaralých prvků sítě. Z důvodu ekonomie provozu jsou starší aktivní prvky přesouvány na méně významné uzly sítě a vyřazovány jsou až tehdy, když přestanou sloužit nebo začnou tvořit bezpečnostní riziko.

## Výměna centrálních switchů

Střed topologie „hvězdy“ tvoří dvojice výkonných identických přepínačů v serverovnách DR01 a DR81 (v lokalitách Kateřinská 32 a U Nemocnice 5). Síťová architektura typu „hvězda“ poskytuje vyšší bezpečnost a spolehlivost jádra sítě, ale vyžaduje větší počet optických portů pro propojení. S postupným rozvojem sítě se vyčerpal počet optických portů stávajících přepínačů řady 4500 a museli jsme je nahradit výkonnějšími přepínači Cisco 9500.

Nové switche mají větší propustnost (40/100 GB/s), více optických portů a větší výkon procesorů. Dosáhli jsme tak čtyřnásobné zvýšení datové propustnosti z 20 G na 80 G mezi aktivními prvky v DR01 a DR81. Dále došlo k více než 2,5násobnému zvýšení počtu 10 G přípojných míst (z 18 na 48). Nové prvky řady C9500 nám umožnily zapojit více zařízení do 10 GB/s optických portů, a tím i připojit vice objektů a datových serverů na tuto rychlost.



Obr. č. Schéma datové architektury páteřní sítě 1. LF UK.

Vyřazenou dvojici prvků řady 4500 jsme přesunuli a slouží jako klasické core access switche pro připojení uživatelů.

## Přechod v zabezpečení metalické sítě na autentikační protokol 802.1x

V některých budovách jsou pracoviště VFN s počítači připojenými do nemocniční sítě přes fakultní infrastrukturu. Rostoucí bezpečnostní požadavky na zabezpečení vedly VFN k požadavku na zabezpečení připojení těchto počítačů bezpečnějším autentikačním protokolem 802.1x.

Připravujeme proto technické řešení, které umožní nasazení 802.1x v celé fakultní síti.

Mezi výhody patří možnost blokovat přístup neautorizovaných osob (např. kvůli šíření virů). Tento mechanismus umožňuje např. umístění klienta do karanténní VLAN, kde má přístup pouze k minimu služeb a kde je izolován do vyřešení problémů.

V objektech, kde neproběhla celková stavební rekonstrukce, je pro toto řešení nedostatek metalických kabelů pro připojení každého koncového uživatele samostatně, což je výchozí předpoklad pro nasazení nového bezpečnostního standardu.

V síti máme přes 40 ks starých pasivních rozbočovačů (hubů), které bychom museli nahradit aktivními prvky. Vzhledem k rostoucím požadavkům na bezpečnost a potřeby VFN nás toto opatření nemine. Odhad nákladů (včetně plošné strukturované kabeláže v prostorách jednotlivých ústavů), odhadujeme na 10 mil. Kč.

## Dokončení výměny zastaralých aktivních prvků

V celé síti LAN zbývá cca 20 posledních starých aktivních přepínačů řady 2950, které běží již více než 15 let a jsou mimo veškerou podporu. Odhad nákladů na výměnu je 1,2 mil. Kč.

## Změny sítě na úrovni pracovišť

**Studničkova 7** (mikrobiologie) – v budově byl nainstalován druhý switch s přenosovou rychlostí 10 Gb/s. Přepínače jsou umístěny v datových centrech DR45 a DR48 v objektu mikrobiologie. Zároveň byla změněna i vnitřní architektura sítě v budově. Spolupracujeme s projektantem SLA systémů a uživateli na projektu rekonstrukce budovy. Projekt je ve stádiu podkladů pro výběr zhotovitele. Rekonstrukce bude etapizována. Začátek stavební rekonstrukce je plánován na rok 2022 dle návrhu MŠMT.

V lokalitě je plánována výstavba nové automatizované vstupní brány. K bráně Studničkova 7 je natažena příprava pro kabeláž včetně pokládky HDPE trubky a nového silového napájecího kabelu. O kompletní rekonstrukci bude rozhodnuto po stavební přestavbě objektu, neboť se v místě ještě předpokládá provoz stavební techniky včetně výstavby jeřábu.

**Purkyňův ústav** - v rámci postupných rekonstrukcí sítě LAN jsme v objektu nainstalovali řadu nových datových rozvaděčů (DR 163, 164, DR165, DR166 a DR167) včetně metalické kabeláže kategorie 6 (1GB/s) a tyto rozvaděče jsme napojili optickými kabely na páteřní síť.

Na Purkyňově ústavu proběhlo úpravou místnosti telefonní ústředny zřízení nové klimatizované serverovny.

**U Nemocnice 3 a 5** – v objektu byly rekonstruovány rozvaděče DR12 a DR15. Součástí nově vybavených rozvaděčů jsou i nové aktivní prvky řady C9200 či C2660S.

**Albertov 7** (Fyziologie) – byla dokončena rekonstrukce budovy včetně kompletní výměny kabeláže na přenosovou rychlost 1 GB/s novými přepínači typu C9200 s 10 GB/s uplinky a PoE+ architekturou pro napájení kamer a čteček.

V lokalitě proběhla výstavba nových automatizovaných vstupů a systémů vjezdových vrat.

Realizovány byly brány Albertov 5 a Albertov 7.

**Anatomický ústav**

Započala rekonstrukce počítačové sítě v objektu Anatomického ústavu. Jedná se o rozsáhlou rekonstrukci kabeláže, kdy budou položeny metalické kabely kategorie 6, systém optických a telefonních kabelů a vybudovány 3 nové datové rozvaděče. Projekt zahrnuje také nákup 4 nových aktivních prvků se 48 porty řady C9500 s PoE a 5 bezdrátových pojítek WiFi.

**Kampus Albertov – zokruhování optické kruhové trasy**

Pro stabilní připojení nově budovaného areálu Kampus Albertov je třeba zajistit zokruhování optické sítě. Z důvodu prodlužujícího se archeologického průzkumu v lokalitě zahrady U Apolináře dochází ke zpoždění celé akce. Předpokládáme realizaci v roce 2022 za spolufinancování RUK a VFN. Odhadovaná spoluúčast nákladů ze strany 1. LF je cca 300 tis. Kč.

# Bezdrátové sítě

## Rozvoj bezdrátové sítě WiFi

Fakultní síť WiFi obsahuje v současné době 218 AP (WiFi přístupových bodů) a je postupně rozšiřována, jak přicházejí požadavky od uživatelů.

Bezdrátová síť 1. LF UK se skládá z dvojice WLC kontrolérů řídících prvků (Cisco řada 5508) a 218 přístupových bodů (AP) různých typů výrobce Cisco. Majoritní typ AP je řada C1850.

Dvojice WLC kontrolérů je 12 let stará a výrobce již končí s další hardwarovou i softwarovou podporou tohoto typu.

Z tohoto důvodu jsme porovnávali technické a následné i finanční řešení vynucené obměny řídících prvků bezdrátové sítě. Technicky jsme srovnali řešení od výrobců Cisco a Aruba. Obě řešení jsou s výhledem na cca 7 let, tedy do ukončení podpory těchto zařízení výrobci.

Technicky a technologicky jsou si tato řešení podobná, včetně cen jednotlivých komponentů i cen podpory a licencování jednotlivých zařízení. Jelikož by se pro řešení od výrobce Aruba musela kupovat všechna AP nová a následně namontovat a nainstalovat, vycházela by tato cesta finančně i časově náročnější než stávající řešení založené na technologiích výrobce Cisco.

Protože v květnu 2022 přestanou být definitivně podporovány naše stávající řídící kontroléry bezdrátové sítě WLC, a je potřeba do té doby pořídit dvojici nových WLC kontrolérů, které budou podporovat nové standardy bezdrátové sítě.

Souběžně probíhá výměna 30 nejstarších přípojných bodů z důvodu končící kompatibility s novými kontroléry. Nové přípojné body WiFi již mají implementovány všechny nové standardy a vysílají na obou pásmech 2,4 a 5 GHz.

V příštím roce budeme muset vyměnit posledních 12 ks starých WiFi přípojných bodů, které nejsou kompatibilní s novými WLC kontroléry. Model WiFi pojítek tak bude sjednocen na řadu C1852. Denní využití bezdrátové sítě v pracovní den se pohybuje mezi 2000 až 4000 připojených uživatelských zařízení.

# Elektronické přístupové systémy

## Kartové vstupy

Elektronické zabezpečení vstupů do budov se osvědčilo a přináší vyšší úroveň bezpečnosti objektů a větší flexibilitu řízení vstupů. V současnosti spravujeme systémem Aktion.NEXT 198 čteček (adresových bodů).

Nově byly nainstalovány kartové vstupy v těchto lokalitách:

* Vstup do nově budované posilovny a šaten Anatomického ústavu (5x čtečka)
* Vchod a branka UTV (2x čtečka, 2x komunikátor 2N)
* Serverovna Purkyňova ústavu (čtečka)
* Vstup chodbou na nukleární medicínu (PATF - čtečka)
* Vstup na ústav Imunologie a vstup do suterénu (2x čtečka)
* Čtečka pro UTPO na sledování docházky studentů
* Ve druhé etapě rekonstrukce Fyziologického ústavu a následných instalací bylo k dnešnímu dni zprovozněno dalších 50 vstupů. Celkově je na Fyziologii 89 čteček
* Děkanát – kolárna a vstup ze dvora (tzv. pod sochou) do budovy (2x čtečka)

Pro Fyziologický ústav byla vytvořena grafická nástavba systému Alvis (EPS/EZS) a Aktion.NEXT pro sledování zamykání a zavírání dveří. Vznikl tak jednoduchý přehled, které dveře zůstaly otevřeny nebo odemčeny.

Pro následující roky má OTP pro děkanát soutěžit dodávku výměny stávajících poruchových vložek Abloy za vložky opatřené čtečkou karet. Ty budou následně zapojeny do našeho přístupového systému. Zaměstnanci už nebudou nosit klíče, ale budou si otevírat dveře od kanceláře zaměstnaneckou kartou.

#  Kamerový systém

Kamerový systém 1. LF UK obsahuje 341 kamer, 5 serverů nového kamerového systému Ateas, 2 servery staršího kamerového systému Go1984. Záběry z našeho kamerového systému svou kvalitou a pokrytím pomáhají Policii České republiky řešit případy týkající se kriminální činnosti uvnitř i vně našich objektů, a tak zvyšovat bezpečnost na fakultě a v jejím okolí.

Za rok 2020 došlo k 16 a za rok 2021 zatím k 11 žádostem o vydání kamerového záznamu.

Fakultní kamerový systém byl rozšířen o 38 nových kamer:

* + 4 kamery – Anatomický ústav
	+ 2 kamery + 1 komunikátor 2N Helios IP Verso s IP kamerou – Děkanát
	+ 1 kamera UVI
	+ 2 komunikátory 2N Helios IP Verso s IP kamerou - UTV
	+ 27 FYZI (12x 2N 15x AXIS)
	+ 1x streamovací kamera se zvukem pro online přenos na youtube

Z důvodu kompatibility s GDPR a s dohledovými systémy byl instalován nový kamerový systém Ateas Security, který umožňuje propojení s přístupovým systémem AKTION.NEXT a systémem ALVIS (EPS/EZS).

Nasazením nového kamerového systému se výrazně snížil datový tok (jelikož nový systém podporuje nové normy kodeků H264, H265 a Zipstream). V novém systému provozujeme aktuálně 320 kamer. Ve starém kamerovém systému GO1984 provozujeme ještě zbývajících 21 kamer, pro které právě pořizujeme licence pro připojení kamer do systému Ateas.

Systém Ateas byl výrobcem rozšířen o nástroj pro automatizované dohledávání objektu, jako je osoba, auto, kolo aj., nebo například možnost rozpoznat barvu a počet objektů. Zatím tuto funkčnost testujeme na jednom PC ve funkci Ateas serveru. Pro praktické použití na dohledávání vytipovaných podezřelých osob by bylo potřeba, aby systém běžel na samostatném serveru.

#  Telefonie

## Testování IP Telefonie

S výhledem na končící životnost pobočkových ústředen testujeme v reálném provozu softwarovou ústřednu 3CX. Stejné řešení používá Přírodovědecká fakulta od roku 2017.

Ústředna je instalovaná na virtuálním serveru se systémem MS Windows Server 2016. Je propojena se stávající ústřednou ve VFN. V současné chvíli je k ústředně připojených 53 IP vrátníků a 10 IP telefonů. V listopadu minulého roku nám byl pro IP vrátníky přidělen další prostor z VFN ústředny, který můžeme využít, a to 4650-4699.

Prověřujeme možnost provozovat softwarovou ústřednu 3CX místo stávajících dosluhujících pobočkových ústředen Siemens.

#  Podpora 3D tisku

Fakulta podporuje rozvoj moderních 3D technologií pro výuku studentů a spolupráci pracovišť, která jsou v této oblasti aktivní.

**Školení studentů**
Na víkendových seminářích školíme studenty ve 3D modelování a na místě jim umožnujeme, aby si své modely vytiskli.

**3D tisk pro výuku stomatologie**
Lídrem ve využití 3D technologií je výuka stomatologie.

O rozsahu těchto aktivit svědčí například počty modelů a přípravků pro výuku stomatologie tištěných technologií SLA:

* Cvičné kavitované kvadranty 280 ks
* Vzorové modely 2. a 3. kvadrantu 180 ks
* Cvičné zuby 1500 ks

Masivní podpora práce na modelech byla a je zvláště významná v době pandemických omezení.

**3D tisk pro výuku praktických dovedností**
Aktuální strategie fakulty klade ve výuce větší důraz na získávání praktických dovedností. Významným inspiračním zdrojem je PROFILES (Principal Relevant Objectives and Framework for Integrated Learning and Education in Switzerland). Student medicíny by měl mimo jiné získat dovednosti potřebné k tomu, aby mohl samostatně provádět vybrané úkony a procedury, v PROFILES označované jako Entrustable Professional Activities (EPAs).

Mezi EPAs patří i provádění tzv. obecných procedur (EPA 5: Perform genearal procedures), např. intravenózní injekce a zavedení intravenózní kanyly (EPA 5b) nebo zavedení intravenózního přístupu (EPA 5c).

Fakulta v současné době disponuje několika typy modelů (fantomů) pro nácvik venepunkce, podávání i.v. injekcí a kanylaci periferní žíly. Jejich dostupnost je přes veškerou snahu dosud omezená. V uplynulém akademickém roce studenti na konci druhého ročníku, tj. před nástupem na ošetřovatelskou praxi, při níž by uvedené úkony měli již být schopni provádět, uváděli, že trénink venepunkce provedli pouze jednou. Vzhledem k tomu, že úkon má řadu dílčích kroků (viz např. WHO guidelines on blood drawing:best practices in phlebotomy,  ISBN 978 92 4 159922 1), je třeba do výuky zavést nové výukové jednotky k nácviku těchto technik tak, aby cílů EPA 5b a 5c bylo dosaženo. K tomu je nutné zvýšit kapacitu dostupných modelů a fantomů.

Nejkvalitnější fantomy pro nácvik venepunkce a kanylace periferní žíly, které jsou na fakultě dostupné, jsou komerční modely od britské společnosti Limbs and Things. Patří mezi světovou špičku v dostupných fantomech. Tomu bohužel odpovídá i relativně vysoká cena spotřebního materiálu a náhradních dílů, kterých je při nasazení ve výuce značná spotřeba. Pilotní zavedení výuky venepunkce do kurzu lékařské chemie a biochemie ve druhém ročníku ukazuje, že jen náklady na spotřební materiál (náhradní žíly a kůže do fantomu, umělá krev) by při plnohodnotném nasazení překračovaly 100 tis. Kč za semestr. Nevýhodou použitých modelů také je, že umožňují simulovat jen relativně snadný odběr – žíly mají velký průsvit, jsou snadno palpovatelné i viditelné atd.

Zmiňované pilotní zavedení výuky venepunkce do výuky biochemie ukázalo, že by bylo možné náklady podstatně (řádově) snížit, pokud bychom dokázali některé součásti fantomu a náhradní díly připravovat sami. Potřebné materiály i technologie jsou dostupné. Části cvičných žil s požadovanými vlastnostmi se nám již podařilo experimentálně vyrobit z běžně dostupných polymerů. Kromě razantního snížení nákladů by ale vlastní výroba umožnila na míru připravovat pomůcky např. pro nácvik obtížné venepunkce, odběru u seniorů, pediatrické populace atd.

Chybějícím článkem pro takový přístup je v tuto chvíli vytváření forem pro odlévání žil a výroba drobných součástek (spojky, různé příchytky, součásti pump na umělou krev apod.). Tyto drobné součásti a díly jsou značně variabilní a je třeba je vyrobit pokaždé v počtu několika, maximálně několika desítek kusů, nutná je však jejich značná variabilita jak tvarová, tak i materiálová. Jako ideální řešení se proto jeví využití technik 3D tisku. Výhodou je zde tisk z polymerních pryskyřic, neboť ten umožňuje podstatně širší variabilitu vlastností výsledného výtisku (např. výrobu měkkých či pružných dílů).

S využitím těchto technologií tiskneme sady náhradních dílů k odběrové ruce, formy na cévy pro odběrové ruce a další.

#  Podpora testování

## Upgrade systému Rogo

Na fakultě provozujeme testovací systém Rogo (<https://www.rogo.cz/>), vyvinutý na University of Nottingham. V systému je aktuálně 15 000 otázek, 342 testů, 6554 vyzkoušených. Testovací systém prošel významným upgradem na verzi 7.3.0., který řeší mnoho drobných problémů.

Souběžně s aktualizací jsme vyvinuli modul, který nově řeší synchronizaci uživatelů se SIS. Nový plugin, který jsme připravili, funguje, všichni studenti se do Roga přihlásí na základě své identity v SIS.

## Položková banka a příprava a tisk testů pro přijímací řízení

Výběr studentů patří ke klíčovým činnostem fakulty, které dlouhodobě ovlivňují kvalitu školy samotné. Proto musí být výběru věnována mimořádná pozornost. V posledních letech bylo úsilí o zlepšení přijímacího řízení věnováno snaze o převedení procesu na Evidence Based základy. Tj. každý krok v procesu musí být posuzován a optimalizován podle měřitelných kritérií.

Fakulta za tímto účelem vyvinula a provozuje položkovou banku, ve které je aktuálně 3098 otázek z biologie, 2415 otázek z fyziky a 3390 otázek z chemie. Každý rok probíhá řada školení autorů, kde probíráme, jak se chovaly v ostrých testech autory navržené položky. Autory motivujeme k tvorbě nových položek, které vkládáme do položkové banky. Nově vytvořené položky jsou před prvním použitím recenzovány a podle výsledku recenze pak použity, nebo zamítnuty.

Z nově vytvořených položek a z položek, jejichž psychometrické charakteristiky se osvědčily v předchozích kolech, jsou autory testů v položkové bance sestaveny ostré testy. V potaz se bere obtížnost úlohy, schopnost rozlišovat mezi kvalitními a méně kvalitními uchazeči, zda je nová, zda je početní a tak podobně. Testy jsou pak podrobeny další recenzi, kdy se odstraňují poslední pochybnosti, opravuje typografie a podobně. Každý korektor dostává výtisk "testu před korekturou". Korektoři zkontrolují faktickou stránku každé otázky, zda je skutečně správně (včetně aktuálního názvosloví) a početní příklady na místě ověří výpočtem. Korektury testů korektoři zkontrolují, opraví a opravený výtisk testu (imprimatur) podepíšou. Podepsané testy s poznámkami korektorů se archivují.

K vytvořeným testům jsou vygenerovány krycí listy a připraveny tiskové sestavy. Proces je nastaven tak, aby hotové testy nikde neležely. Aby nemohlo docházet k podvodům s odevzdáním jiné verze testu, je tisk individualizovaný. Celý proces tisku je monitorován kamerovým systémem a pravidlem čtyř očí. Všichni účastníci procesu mají podepsanou mlčenlivost.

V reakci na incident zjištěný při přijímacím řízení před několika lety byl změněn postup přípravy a tisku testů tak, aby nebylo možné s testem manipulovat při odevzdávání. Nyní je každý výtisk testového sešitu unikátní.

Tiskne se krycí list, vlastní zadání testu, košilka balíku, krycí list testového zadání, QR kód pro anonymizaci testů před vyhodnocením. Tiskový soubor (PDF) je speciálním softwarem nutné dělit na části – dílčí soubory, tak, aby žádný dílčí soubor neobsahoval víc, než 49 testových zadání. To znamená, že pro konkrétní místnost se tiskne několik balíků, které mají vlastní košilku.

Testové sešity se před balíkováním ručně kontrolují. Počet výtisků na jedno přijímací řízení přesahuje 120 tisíc listů. Systém je na jednu stranu velmi bezpečný, ale současně je velmi náročný na přesnou, kvalifikovanou a bezchybnou práci (a spolupráci) řady lidí.

V Praze 1.11. 2021

RNDr. Čestmír Štuka, Ph.D.