Univerzita Hradec Králové

Fakulta informatiky a managementu

Disertační práce

Framework zabezpečeného informačního a management systému v podmínkách biomedicínských laboratoří

Autor: Ing. Pavel Blažek

Studijní program: P1802 Aplikovaná informatika

Studijní obor: 1802V001 Aplikovaná informatika

Školitel: prof. Ing. Ondřej Krejcar, Ph.D.

Katedra/pracoviště školitele: Centrum základního a aplikovaného výzkumu

Hradec Králové 25. březen 2018

Prohlašuji, že jsem disertační práci vypracoval samostatně a s použitím uvedené literatury.

.....

V Hradci Králové dne 25. 3. 2018 Ing. Pavel Blažek

Poděkování

Chtěl bych poděkovat vedoucímu mé disertační práce prof. Ondřeji Krejcarovi za čas, který mi věnoval a podnětné vedení, kterým mi rozkryl možnosti a dopady vědecké práce. Děkuji prof. Kamilu Kučovi, který mě na samém počátku, když jsem se zamýšlel nad svým dalším odborným uplatněním, ke studiu motivoval a při dalších setkáních mě ve správnosti mého rozhodnutí utvrzoval. Děkuji své rodině, manželce a synům, bez jejíž podpory a tolerance bych nemohl studiu po čtyři roky věnovat tolik ze svého - našeho volného času. Děkuji všem za motivaci dokázat v sobě najít sílu a pokračovat k cíli.

Abstrakt

Proces návrhu kvalitního informačního systému je složitý. Musí co nejlépe korespondovat s prostředím, v němž má být nasazen, navazovat na aktuální legislativu a normy. Musí vzít v potaz i další aspekty, které mohou mít vliv na vývoj, implementaci i rutinní provoz. Při budování laboratoří a implementaci laboratorních informačních systémů je nutno zohlednit bezpečnostní rizika. Dostupné manuály a doporučení jsou buď všeobecné a nepostihují technické možnosti nebo jsou detailnější, avšak aktuálnost jejich obsahu se váže k době jejich vzniku. Při vývoji informačního systému je třeba dbát na přívětivost grafického rozhraní a logiku ovládacích prvků, které do jisté míry bezpečnost také ovlivňují. Návrh nového Laboratorního informačního a management systému je třeba od počátku orientovat na využití nových technologií. Integrací miniaturních počítačů, které nacházejí uplatnění napříč obory lidské činnosti, do prostředí laboratoří a tím i do systému LIMS, přibývá nová skupina převážně provozních dat, která primárně navazují na subsystém logistiky. Navýšení informační hodnoty datové kolekce vybízí k vytvoření nových nebo aspoň aktualizovaných funkcí. Ve výsledku mohou přinést snížení množství úkonů, které nesouvisejí bezprostředně s experimenty a jsou plněný personálem laboratoře. Lze je také využít k implementaci bezpečnostních prvků v rámci frameworku, což je primární náplní této disertační práce.

Klíčová slova

Framework, laboratorní informační management systém, bezpečnost

Abstract

The proposal of designing a quality information system is a complicated process. It has to match the best with the environment where it is to be implemented, and has to follow up on current legislation and standards. Other aspects which can affect development, implementation and routine operation should be taken into account as well. Security risks have to be considered when building laboratories and implementing information systems. Available manuals and recommendations are either too general and they do not cover technical possibilities or they are more detailed, however, their content was topical at the time of its creation. When developing the information system, care should be taken of friendliness of graphic interface and logic of controls which also affect security to a certain extent. The proposal of the new Laboratory information and management system is to be oriented, from the very beginning, at the use of new technologies. Integration of miniature computers, which are applied across the fields of human activity, into the labs environment and consequently into the LIMS, a new group of mainly operational data occurs which is primarily built on the logic subsystem. Increasing the information value of data collection encourages a creation of new or at least updated functions. They can result in the decrease of the number of operations which are not connected immediately with experiments, but they are carried out by the lab personnel. They can also be used for implementation of security elements within the framework which is the primary purpose of this dissertation.

Keywords

framework, laboratory information management system, security

ZKRATKY

Zkratka	Význam
API	Application Programming Interface - rozhraní pro programování aplikací
AUDITDB	Databáze logů systému a souvisejících zařízení
AuthApp	Modul pro řízení uživatelských účtů a nastavení uživatelských oprávnění
BT	Bluetooth technologie
CAM	Content access module – modul ověřování přístupu
CMS	Content Management System
CPU	Procesor počítače
CVE	Common Vulnerabilities and Exposures
DATADB	Databáze pracovních dat
DirectApp	Modul podpory manažerských funkcí
DoS	Denied of Service
EduApp	Modul podpory vzdělávání studentů a pracovníků
FDA	Food and Drug Administration Department
GAMP	Good automated manufacturing practice
GxP	Good practise – souhrnné označení pro více oblastí
HAZOP	Hazard and Operability Study
HIPAA	Health Insurance portability and Accountability Act
HW	Hardware
ICH	International Concil of Harmonization
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
IoT	Internet of Things
ISO	International Organization for Standardization

LabApp	Laboratory Applications - modul podpory workflow laboratoře
LibrarApp	Modul pro ukládání elektronických publikací a informací svázaných s experimenty
UserDB	Databáze uživatelských účtů a bezpečnostních politik systému LIMS
LIMS	Laboratorní informační a management systém
LIS	Laboratorní informační systém
LMS	Laboratorní management systém
LogistApp	Modul podpory funkcí logistiky
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
RFID	Technologie Identifikace na rádiové frekvenci
SHA	Secure Hash Algorithm
SIEM	Security Information a Event Management
SW	Software
TOGAF	The Open Group Enterprise Architecture Framework
UM	Univerzální modul
UserDB	Databáze uživatelských účtů a oprávnění
WIFI	Bezdrátová datová síť

Seznam obrázků

Seznam tabulek

OBSAH

1 ÚVOD

Návrh zabezpečeného informačního systému určeného pro laboratoře vychází z poznatků a požadavků tří laboratoří královehradeckého kampusu, které mají podobnou strukturu i workflow [I.1]-[I.3]. Vzešel z myšlenky, vytvořit společný management systém, který by umožnil sdílení informací o projektech a umožňoval distribuovat úkoly mezi subjekty s ohledem na specifičnost jejich zázemí a vybavení. Pilotní návrh byl postaven na znalostech o prostředí laboratoře Katedry toxikologie Fakulty vojenského zdravotnictví, která se jevila v mnoha ohledech nejstriktnější.

Podpora manažérských funkcí je řešena v mnoha aplikacích a informačních systémech ať komerčních nebo pod licencemi Open Source. Analýzou procesů a studiem podkladů pro výstavbu a provoz laboratoří byl zjištěno, že na jedné straně stojí normy přesně definující postupy a na straně druhé všeobecné manuály a doporučení pro výstavbu laboratoří. Skloubení obou stran nemusí jednoznačně vést k vytvoření bezpečného efektivně postavenému systému. Následující studie by k takovému cíli měla směřovat, přičemž management systém hraje v zabezpečení dat významnou roli.

Laboratorní informační a management systém (LIMS) má stejné historické podmínky vzniku jako jiné informační systémy (IS). S rozvojem informačních technologií (IT) a programového vybavení (SW) postupně vznikaly aplikace, které usnadňovaly zpracování informací z experimentů. Z aplikací pro podporu plnění dílčích úkonů se stávaly sofistikovanější celky, které se postupně spojily do nástrojů, které nesou označení LIS, tedy Laboratorní informační systém. Druhý, paralelně vyvíjený, nástroj byl zaměřen na řízení činností v laboratoři. Je označován LMS, což je označení pro Laboratorní management systém. Tyto dva systémy se svým primárním určením rozcházejí. Zatímco prostřednictvím nástrojů LIS se kompletují, zpracovávají a vyhodnocují klinická data a data experimentů, LMS je systémem s podporou řídících a rozhodovacích funkcí, tedy, primárně obsahuje data o organizaci úkolů a činností. Prolnutím funkcí pak logicky vzniká LIMS, který bývá někdy nepřesně označován LMS. LIMS je tedy informační systém postavený na programovém vybavení, které svou nabídkou pokrývá požadavky a potřeby moderního laboratorního prostředí z pohledu managementu i podpory rutinních činností. Vyvíjel se v kontextu doby a technických možností z jednoúčelových aplikací provozovaných na lokálních počítačích, přes komplexnější softwarové produkty po systémy plně postavené na síťovém prostředí [V.1] s architekturou client-server. Obsahem pokrývá potřeby všech zainteresovaných skupin podílejících se na efektivním chodu laboratoře. Laborantům poskytuje elektronický laboratorní deník a moduly pro vyhodnocování vložených dat, logistické funkce napomáhají zabezpečení chodu laboratoře a manažerům poskytuje nástroje pro řídící činnosti. Je pochopitelné, že podpora rutinních činností je základním

stavebním kamenem, ale rozsah nabízených funkcí může běžný rámec překračovat. Prostředí laboratoří je variabilní. Jednoznačná definice konkrétního LIMS proto závisí na potřebách uživatelů [I.4], zaměření a na vybavení laboratoře. Nelze ji proto snadno zevšeobecnit.

Z hlediska plánování a nasazení LIMS, které zahrnuje pohled ekonomický, je pořízení komplexního IS zbytečně nákladné. Je zjevné, že instalace bude mít nadbytečné nároky na hardware (HW). Z toho důvodu jsou informační systémy pro laboratoře všeho druhu vyvíjeny a dodávány jako modulární, kdy není třeba pořizovat kompletní funkcionalitu [1], [2] a při vzniku specifických požadavků lze další modul dotvořit nebo již existující připojit. Model licencování Open source se jeví zajímavým právě z pohledu možnosti přizpůsobit si již existující systém, resp. jeho moduly nebo naprogramovat nové. Z uživatelského hlediska může jít o aplikaci instalovanou na počítač nebo webový nástroj, což je trend poslední doby úzce svázaný s podporou mobilní platformy. Rozšíření komfortu prostředí IS spočívá v tvorbě modulů-rozhraní, jež dovolují propojení s laboratorními přístroji a tedy přímé získávání výstupních dat bez nutnosti manuální konverze formátu [3], [4].

Za klíčové prvky LIMS lze považovat:

- Podporu laboratorních činností
- Modularitu
- Workflow a řízení datových toků
- Systémy analýzy a plánování logistiky
- Finanční analýzy a plánování
- Otevřená rozhraní pro výměnu dat

Rozdílné nároky na LIMS mají klinické laboratoře, které provádí rutinní testování, jsou povinné dodržovat postupy a vést o tom záznamy a laboratoře primárního výzkumu, která má volnější pravidla [5]. Vývoj LIMS pro klinické certifikované laboratoře, které musí dodržovat dané postupy, se staví na všeobecně platných normách a doporučeních tak, aby naplňovaly legislativu dané země. Jde o procesní řízení vesměs postavených na normách ISO 9001 a ISO 17025 [6], [7]. V úvahu je mnohdy nutné brát i zákon na ochranu osobních údajů osob a pacientů, které jsou v platnosti např. v USA od roku 1996 pod označením HIPAA [8], obdobné zákony má Kanada [9], Japonsko [10] a Austrálie [11]. Nařízení EU 95/46/EC bylo podkladem pro Vyhlášku o zdravotnické dokumentaci 98/2012 ze dne 22. března 2012 [I.5]. V ní je přesně definováno, se kterými daty lze bez vědomí pacienta pracovat a jak. Pro pracoviště, která nejsou bezprostředně svázaná s poskytováním péče, z ní vyplývá nutnost tzv. deidentifikace dat [5]. Nově přibyla povinnost ochrany dat na základě GDPR, což je obecné nařízení o ochraně osobních údajů a dotýká se i údajů zaměstnanců, které jsou v IS zpracovávány a uloženy.

Text této práce je rozdělený do jedenácti kapitol. První je úvod, v němž jsou základní informace k problematice a výstavby LIMS. Druhá kapitola je věnovaná analýze současného stavu a shrnuje poznatky o prostředí laboratoří z pohledu provozovaných aplikací. Třetí kapitola obsahuje definici cílů disertační práce. Čtvrtá až osmá kapitola přináší v logickém sledu řazenou pětici bloků, které představují etapy studia problematiky a vlastní práce. Zahrnuje objasnění organizační struktury laboratoře, návrh struktury navrhovaného systému, výběr bezpečné platformy pro realizační fázi, návrh centrálního softwarového modulu, návrh hardwarového bezpečnostního modulu. Poslední, devátá kapitola, obsahuje souhrn možností rozšíření navrhovaný LIMS o další moduly, které již tak zásadní vliv na jeho bezpečnost nemají. V desáté kapitole je pak shrnuto, jak bylo vytyčených cílů dosaženo a s jakým výsledkem. Poslední jedenáctou kapitolou je závěr stručně shrnující obsah práce.

2 ANALÝZA SOUČASNÉHO STAVU

LIMS se lze pořídit jako komerční i Open Source produkty [12], z nichž lze poskládat základní řešení vyhovující podmínkám dané laboratoře [I.6], [I.7], [13]. Pokrytí požadavků specifické oblasti výzkumu se řeší formou na zakázku vyhotovených systémů. Přístup k uloženým datům je v IS mnohdy postaven jen na několika předdefinovaných úrovních skupinového oprávnění, anebo jej decentrálně provozované prostředí neřeší vůbec. Mnohé IS jsou postavené na principu důvěry [I.8], tedy na sdílení informací probíhajících výzkumných prací bez omezení oprávnění k přístupu. Za tímto modelem stojí fakt, že v laboratořích, které takové systémy implementovaly, pracují důvěryhodní pracovníci a z nich sestavené týmy se snaží dosáhnout společného cíle. Bohužel, tento posudek se opírá pouze o odhad osobností a nikdy nelze s určitostí říci, jak se který pracovník zachová např. v případě nátlaku na jeho osobu nebo v situaci vynuceného odchodu. Vývoj globální společnosti, průmyslová špionáž, migrace a infiltrace radikálů do různých komunit a pracovních skupin je dnešní realitou a hrozbám je lépe předcházet než řešit následky. Události poslední doby s sebou přináší změnu pohledu na akt důvěry všeobecně, laboratoře nevyjímaje.

LIMS jsou tvořeny kolekcí modulů, které vytvářejí digitální obraz pracovního prostředí laboratoře, a jejichž úkolem je zjednodušit a urychlit rutinní činnosti. Jádro systému postihuje základní funkcionalitu, doplňkové moduly jej rozšiřují v závislosti na určení laboratoře. Do základní části je například implementovaný modul elektronického deníku laboranta, logistické moduly pro evidenci majetku a materiálu, management moduly pro efektivní řízení dané laboratoře [13], [14]. Rozšířením se pak rozumí moduly s rozhraním pro připojení konkrétních typů přístrojů a s možností zpracovat data z nich načtená. Následující návrh rozšiřuje základní schéma o další moduly, které vycházejí z poznatků o nekoncepčnosti práce se zdroji informací, kdy dochází k časovým ztrátám díky mnohonásobnému vyhledávání stejných informací a zdrojů díky decentrální vědomostní základně. Z provozních podmínek akademického prostředí kampusu, kde je fluktuace osob oproti komerčním laboratořím výrazně vyšší a to především díky praxi studentů [15], [16], vychází koncept modulů zabezpečení.

Nad rámec základních provozních prvků výstavby chemické či biologické laboratoře [17] se stále více uplatňují prvky zabezpečení. Je zřejmý důraz na ochranu duševního vlastnictví organizace coby prevence před vyzrazením a případným zneužitím. Rozhodně nejde o postačující krok, který by zabránil fyzické manipulaci s materiálem. V manuálech a normách lze v kategorii fyzického zabezpečení nalézt postupy, které řeší základní monitoring pohybu osob a vymezení oprávnění jejich vstupu do definova-

ných oblastí [V.2]. K podpoře a zabezpečení chodu laboratoří jsou tyto vybaveny sensory, jejichž výstupy lze využít jen v daném systému. Tato decentralizace omezuje možnost vyhodnocení informací ve smyslu propojení dat a pro okamžité rozhodnutí je nepoužitelná.

Možnost fyzického poškození dat a zcizení informací je další aspekt, který musí být řešen na úrovni výstavby LIMS. Implementace řešení na úrovni samotného LIMS není často vyžadována a je realizována jinými prostředky. V mnoha manuálech pro organizaci laboratoří mají formu doporučení a jsou řešeny jako samostatné bloky. Počínaje fyzickým zabezpečením prostor, přes režim vstupu osob do objektu a jednotlivá pracoviště, elektronický systém vstupu do objektu po požární zabezpečení a hlásiče. Vše je řešeno v samostatných kapitolách věnovaných jednotlivým systémům. LIMS přitom může být silným integrujícím prvkem. Aby jím byl, musí být sám postaven s důrazem na vlastní bezpečnost.

Zabezpečení biomedicínských dat nemusí znamenat jen bezpečnostní funkce integrované ve workflow laboratorního informačního a management systému a objektové bezpečnosti coby dvou vedle sebe stojících celků jak by mohlo vyplynout z doposud prezentovaných informací. Hlavní filozofií diskutovaného bezpečnostního konceptu je stavba LIMS na moderních technologiích a smysluplná integrace funkcí, které v laboratořích fungují autonomně, a které by mohly být integrací přínosné [17]. Do celkového pojetí jsou zahrnuty prvky fyzického zabezpečení i aplikační a systémová nastavení v LIMS. Pro zvýšení komfortu je pak zamýšleno dovybavit pracoviště SMART technologiemi, které by svou funkcí vybrané rutinní činnosti podpořily a zautomatizovaly.

Jen málo pracovišť se blíží vybavením komplexnímu systému zabezpečení. Často bývá na vině nekoncepčnost pořizování vybavení, obnova či výstavba v etapách, neznalost problematiky na straně zadavatele, nedostatek financí či neochota investovat. Příkladem může být systém zabezpečení vstupu do laboratoře. Bývá postavený na RFID technologii, kdy do prostorů laboratoře je povolen vstup jen oprávněným osobám, které se musí identifikovat přiložením ID karty nebo tokenu na čtecí zařízení u dveří. Po zapnutí počítače v kanceláři jsou uživatelé vyzváni, dle velikosti síťového prostředí, k autentizaci pro přístup do prostředí operačního systému nebo prostředí pracovní domény. Pro přístup do PC svázaného s přístroji v laboratoři se tento postup opakuje. Bioaktivní a hořlavé látky se skladují v lednicích a speciálních skříních, do nichž je přístup omezen buď na úrovni objektových úprav, případně v kombinaci s identifikací vstupu ID kartou či tokenem, nebo je takto zabezpečena přímo skříň se skladovaným materiálem. Varianty jsou různé, počínaje doinstalovanou kladkou s visacím zámkem, přes elektronický zámek s tlačítkovým panelem pro vložení přístupového kódu nebo RFID čtečkou, která ale může pracovat s jinou variantou karet, než jsou používané pro vstup.

Shrneme-li výše uvedené body, dostáváme se ke zjištění, že

- Pracovník používá různé typy identifikačních prvků
- Je nucen si pamatovat si různé kódy a hesla
- Složitost daného uspořádání vede k obcházení bezpečnostních pravidel
- Efektivita využití použitých technologií nedosahuje možných hodnot
- Nalezení souvislostí případného bezpečnostního incidentu je časově velmi náročné

3 DEFINICE CÍLŮ DISERTAČNÍ PRÁCE

Základním cílem této disertační práce je vypracování návrhu LIMS se zabezpečeným workflow zaměřeného na biomedicínské laboratoře zabývající se primárním výzkumem. Jde o informační systém, který v souladu s příslušnou legislativou a normami podpoří rutinní činnosti, k čemuž využívá moderní technologie. V jednotlivých krocích je třeba realizovat následující cíle:

- Analýza stávajícího workflow a jeho porovnání se standardy
- Analýza systémů podpory laboratoří vycházející z doporučení a norem pro výstavbu laboratoří
- Analýza rizik kompromitace dat
- Návrh úpravy workflow
- Návrh integrace funkcí a komponent vybraných systémů do integrovaného prostředí
- Návrh zabezpečené infrastruktury datového prostředí

Porovnáním standardů a existujícího workflow je třeba odhalit případné nejednotné postupy v monitorovaných laboratořích a také rozpory vůči platným normám. Analyzovat systémy podpory činnosti laboratoří a možnosti integrace výstupů do bezpečnostního modulu navrhovaného LIMS dle pokynů pro výstavbu laboratoří a následně získat praktické informace s dotčenými systémy z laboratorní praxe. Analýzou získaných dat se zaměřením na bezpečnostní aspekty zhodnotit stávající stav a navrhnout modernizaci, jež by znamenala snížení nároků pracovníků laboratoře na činnosti plně nesouvisející s výzkumnou činností. Pro nově koncipovaný informační systém navrhnout adekvátní infrastrukturu a její zabezpečení.

4 ORGANIZACE BIOMEDICÍNSKÉ LABORATOŘE

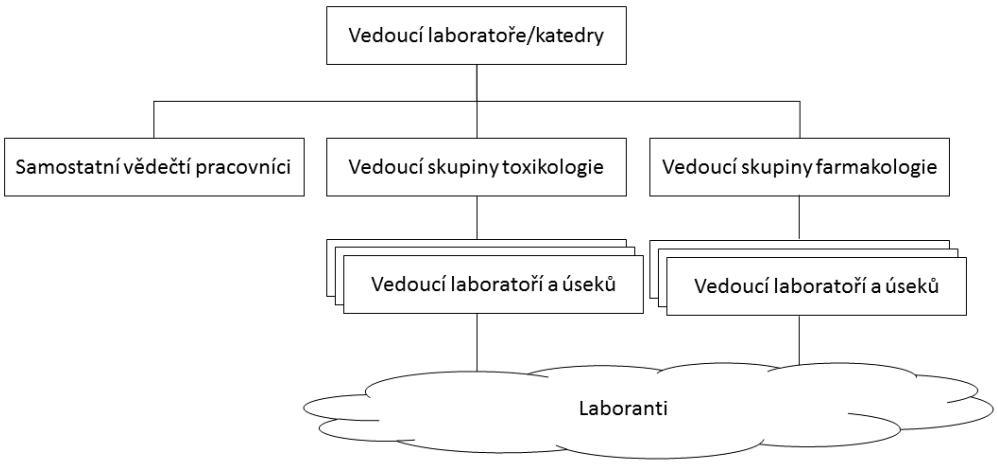
V rámci studia zaměřeného na legislativu, workflow, technologické možnosti a všeobecně realizovaného zabezpečení v prostředí laboratoří bylo provedeno její rozdělení na bloky, které představují obsah kapitol následujícího textu. Vycházejí ze studia teoretických pramenů, reálných podmínek laboratoří a také z předchozí praxe zabezpečení chodu informačních technologií v tomto prostředí. Dále uvedené poznatky byly průběžně prezentovány na konferencích a publikovány jako odborné články [V.1]-[V.7].

Počáteční práce byly zaměřeny na získání potřebných informací z následujících oblastí:

- Organizační struktura biomedicínské laboratoře
- Legislativa související s podmínkami činnosti laboratoří všeobecně
- Legislativa upravující podmínky provozu klinických laboratoří
- Metodiky vývoje a provozu informačních systémů
- Workflow - datové toky v prostředí laboratoře primárního výzkumu

Cíleným rozborem dostupných informací o operačních a publikačních systémech byl hledán optimální a přitom bezpečný základ navrhovaného IS [18]. Na základě získaných poznatků byly navrženy úpravy stávajícího workflow a jeho doplnění. Jako poslední byl vytvořen návrh hardwarového modulu včetně grafického uživatelského rozhraní, s jehož pomocí lze demonstrovat sílu chytrých komponent v infrastruktuře laboratoří. Tato problematika je v závěru bloku dále rozvinuta. V následujících podkapitolách jsou tyto práce podrobněji rozepsány.

Obecný model organizační struktury biomedicínských laboratoří lze přirovnat k jiným firemním modelům. Jde o pyramidu, v níž špici tvoří management a základnu koncoví pracovníci, v tomto případě laboranti a zaměstnanci podpory laboratoře. Detailnější pohled na strukturu konkrétní laboratoře pak odkrývá dílčí rozdíly [19]. Základem je vedoucí pracovník, zástupce, vedoucí laboratoří a laboranti. Obsazenost dalších pozic souvisí s mírou autonomie. Laboratoře integrované do většího celku využívají jeho podpůrné složky i pro svou podporu. Příkladem může být klinická laboratoř zařazená do struktury Fakultní nemocnice nebo laboratoř primárního výzkumu jako součást katedry fakulty univerzity. Na obrázku č. 1 je pak vyobrazena struktura laboratoře katedry toxikologie.



Obrázek č. 1 – Organizační schéma laboratoře zdroj: vlastní

V její struktuře není zahrnuta personalistika, logistika ani ostraha budovy, které jsou v organizační struktuře nadřazeného organizačního celku. Do funkčního schématu je však nutné zahrnout aspoň ty, které mají bezprostřední dopad na workflow. Nepřímo ho ovlivňuje oddělení personalistiky, neboť nemá přímou vazbu na žádnou část informačního systému laboratoře. Administrace účtů může, ale nemusí, být provázána s personalistickým systém konektorem. Naproti tomu funkce „logistik“, která se stará o materiální zabezpečení chodu v laboratoři, je nezbytná. Bývá sdružená s jinou odbornou funkcí a těží ze znalosti prostředí a problematiky. Osoba pověřená logistickými operacemi má odborné znalosti, je schopna provést fundovanou organizaci nákupu a provést kontrolu dodržení typu, množství a kvality dodaného materiálu.

4.1 Legislativní základ tvorby LIMS

Hlavní filozofií práce je vytvoření zabezpečeného frameworku laboratorního informačního a management sytému. V nabídce je mnoho LIS, LMS, LIMS a to jak komerčních tak dostupných jako open source řešení. Jejich framework je navržený tak, aby plně pokrýval požadavky účelu primárně klinických laboratoří z pohledu workflow [20], [21]. Neboť je počet potenciálních koncových uživatelů/zákazníků poměrně úzký, snaží se firmy a skupiny vyvíjející SW a IS pro laboratoře naplnit požadavky různých národních nařízení a standardů a mezinárodních norem [22], [23]. Ty jsou si v mnohém podobné, neboť musí pokrýt stejnou oblast a náplň činností. Odchylky pak vycházejí primárně z národních zvyklostí a s nimi souvisejících zákonů.

Aby mohly být laboratoře provozované, poskytovat služby, deklarovat kvalitní výstupy a byly konkurence schopné na mezinárodním poli, musí splňovat základní nařízení týkající se provozu laboratoří a projít celou řadou certifikací a akreditací. Jejich počet a výběr závisí na zaměření a rozsahu jejich činnosti a také na zamýšlené geografické působnosti. Kombinací validace využívaných metod a kalibrace přístrojového vybavení lze dosáhnout úspěšných testů mezilaboratorního porovnání. Výsledky stejných testů na stejných vzorcích se nemohou statisticky výrazně lišit. Toho se využívá při kalibračních testech nad vzorky k tomu účelu určenými. V rámci primárního výzkumu a vývoje nových léčiv zadávají farmaceutické firmy u vybraných subjektů k provedení testy na mezilaboratorní porovnání, aby statistiky potvrdili účinnost nových preparátů. S tím souvisí proces a dokumentace o prováděných pravidelných kalibrací laboratorních přístrojů. Ta je při inspekcích stavěna do popředí zájmu komisí. Informační systémy proto obsahují přednastavené elektronické evidenční knihy plně vyhovující inspekčním kontrolám. Záznamy se ukládají a archivují v elektronické podobě, čímž je splněn požadavek na dohledatelnost.

Akreditace znamená pro klinické laboratoře navýšení hodnoty, přičemž vývoj mezinárodních standardů, které jsou pro jednotnou akreditaci nezbytné, zajišťují v laboratořích zlepšení kvality a bezpečnosti. V některých zemích se stále používají pro tuto oblast všeobecné standardy ISO 9001 a 9002 pro systém kvality a ISO 17025 pro testování laboratoří. Některé využívají jen druhý jmenovaný, na který přešly v rámci procesu zvyšování kvality [24]. Naproti tomu narůstá počet zemí a institucí, které používají modernější systém ISO 15189. Tento je pro účel akreditace biomedicínských laboratoří vhodnější, neboť je pro laboratoře cílený, proto lépe vyhovuje požadavku na kompetenci. Zaměřuje se na potřeby zákazníků a navyšuje hodnotu laboratorních služeb. Vliv legislativy lze chápat v rovině validovaných výstupů také jako formu bezpečnostního opatření. Tedy, že vstupní materiály, biologické vzorky, byly korektně zpracovány a výstupy jsou ověřené. Navazující proces léčby může být plně a bez rizika na jejich relevanci postaven. Další, navazující bezpečnostní úrovní, je nakládání s daty získanými, zpracovanými a uloženými v rámci vyhotovených testů v laboratoři. Pro danou oblast existují i další směrnice a metodiky. Například ICH Q2(R1) se stejně jako norma ISO/IEC 17025, kapitola 5.4.5 zabývá validací metod, nebo GAMP 5 (Good automated manufacturing practice) a směrnice FDA (Food and Drug Administration Department) společně s již uvedenou ISO/IEC 17025, kapitola 5.4.7.2 se zaobírají validací softwaru. Zmíněná americká FDA vydala federální standard 21 CFR Part 11 [I.9] v němž jsou, mimo jiné, specifikované požadavky na elektronické záznamy a podpisy.

Pro implementaci norem na pracoviště nebo firmu všeobecně platí, že vedení firmy stanoví své cíle a plány v oblasti kvality své činnosti a tyto jsou postupně pomocí nastavených procesů prováděny. Jejich činnost se monitoruje a měří, aby bylo možné přijmout účinná opatření na změnu. Norma jako taková se zabývá principy řízení infrastruktury, lidských zdrojů a dokumentace. Dále zavádí procesy

komunikace se zákazníky, hodnocení dodavatelů, měří výkonnost procesů. Za účelem získání zpětné vazby definuje jak provádět interní audity.

Zde popisované řešení je zaměřeno na laboratoře primárního výzkumu, jejichž organizace se v jistých aspektech od klinických liší. Především se nemusí řídit legislativou v takovém rozsahu jako laboratoře klinické. Nad rámec běžně řešeného a stále upravovaného workflow se práce zaobírá oblastí zabezpečení, která není buď integrální součástí provozovaných systémů vůbec, anebo je v nich implementována jen částečně. V klinických laboratořích se bezpečnost řeší v rámci akreditace. Ta s sebou přináší vybudování značně unifikovaného prostředí. Důvodem je vytvořit síť mezinárodně srovnatelných laboratoří, s nadnárodní kontrolou, jejichž výstupy lze díky tomu akceptovat v rámci schvalování uvedení léků, potravin a dalších položek ve všech státech, které se k dané iniciativě přihlásí. FDA zastřešuje prostor v USA, v globálním prostoru plní integrátora Organizace pro hospodářskou spolupráci (OECD) jako jednu ze svých aktivit. S OECD úzce spolupracuje Evropská komise, která koordinuje prostředí uvnitř Evropské unie za pomocí nařízení a směrnic. Provoz laboratoří tak upravují směrnice z oblasti Zdraví a bezpečnost práce, podstatněji pak Správná laboratorní praxe (SLP), v originále Good Laboratory Practice (GLP). Tyto zásady byly vypracovány právě v souladu s OECD a EU je a revidované Příručky OECD přijala pro postupy monitorování dodržování SLP jako přílohy k oběma směrnicím SLP [I.10]. Směrnice 2004/9/ES o inspekci a ověřování správné laboratorní praxe (SLP) stanovuje povinnost zemí EU jmenovat orgány odpovědné za inspekce SLP na svém území. V průběhu inspekcí a vykonávání auditů v laboratořích se mají dodržovat Pokyny OECD týkající se postupů pro monitorování dodržování zásad SLP, jakož i pokyny OECD pro provádění inspekcí testovaného zařízení a auditů. Směrnice 2004/10/ES požaduje, aby země EU přijaly všechna nezbytná opatření, aby zajistily, že laboratoře provádějící bezpečnostní studie chemických přípravků budou postupovat v souladu se zásadami správné laboratorní praxe OECD. Mimo uvedených směrnic se v databázi knihovny OECD k danému tématu nachází přes 20 publikací [I.11]. Česká republika se k OECD připojila v roce 1995, členským státem EU se stala v roce 2004. Zákony a vyhlášky Evropské unie (EU) jsou pro nás závazné. Správnou laboratorní praxi stanovuje hlava III § 18 - 20 zákona č. 350/2011 Sb. [I.12] a vyhláška č. 163/2012 Sb. ve znění pozdějších předpisů. Na ni navazuje Zákon č. 356/2003 Sb. o chemických látkách a chemických přípravcích a o změně některých zákonů, ve znění zákona č. 186/2004 Sb. Dále je zde Vyhláška Ministerstva životního prostředí č. 279/2005 Sb., kterou se mění vyhláška č. 219/2004 Sb., o zásadách správné laboratorní praxe. Pro lepší pochopení tematiky je k dispozici Předpis č. 163/2012 Sb., který obsahuje náhled na SLP Ministerstva pro životní prostředí. Povinnost testovacích zařízení zavést zásady SLP je stanovena v §21 zákona č. 350/2011 Sb. ve znění pozdějších předpisů [I.13]. Garantem akreditací pro Českou republiku je Český institut pro akreditaci, o.p.s. Akreditace zdravotnických laboratoří je prová-

děna podle normy ČSN EN ISO 15189:2013 - Zdravotnické laboratoře - Požadavky na kvalitu a způsobilost. Náplň této normy upřesňuje dokument – metodický pokyn MPA 10-02-13, "K aplikaci ČSN EN ISO 15189:2013 v akreditačním systému České republiky".

Pro oblast farmakologie funguje v Evropě od roku 1964 European Directorate for the Quality of Medicines & Healthcare (EDQM), což je ústřední organizace, která chrání veřejné zdraví standardy kvality pro bezpečnou medicínu. Umožňuje vývoj, podporu provádění a monitorování uplatňování norem kvality bezpečných léčiv a jejich bezpečného používání. V České republice najdeme národní ekvivalent ve Státním ústavu pro kontrolu léčiv (SÚKL). Jeho náhled na SLP je obsažený v dokumentech dostupných na jeho webových stránkách [I.14]. Jsou jimi:

- Pokyny SLP-5 verze 1, Dokumenty správné laboratorní praxe OECD, SLP
- SLP-6 verze 4, Národní program monitorování shody se zásadami SLP
- SLP-7, Žádost o vydání certifikátu SLP
- SLP-8, Zásady postupu při sledování dodržování podmínek SLP

Pro konkrétní typy klinických laboratoří platí požadavky na personální zabezpečení diagnostické a léčebné péče. Vychází z legislativy EU a jsou uvedeny ve Vyhlášce ministerstva zdravotnictví 99/2012 Sb. a jejích doplňcích. Mimo jiné definují odbornou způsobilost a praxi pracovníků v akreditovaných laboratořích, což dopad na činnost laboratoří primárního výzkumu nemá. Zatímco pro akreditované laboratoře platí, že by v rámci naplnění ISO 17025 měli mít pro všechny klíčové funkce zástupce a zastupitelnost všech zkušebních techniků, v laboratořích primárního výzkumu jsou takové požadavky mimo rámec potřeb a jen by nadbytečně zvyšovaly počet osob na pracovišti. Pracoviště se zabývá primární badatelskou činností, kterou nelze omezovat postupy, neboť ty zde teprve vznikají.

Jinak tomu je u nakládání s osobními údaji pacientů, kteří jsou součástí výzkumného projektu. Zde se již vyhláška ministerstva zdravotnictví č. 98/2012 sb. o zdravotnické dokumentaci na jejich ochranu vztahuje a má přímý dopad na provozovaný LIMS, pokud v něm jsou data uložená. I ona má základ ve směrnici EU, konkrétně jde o 95/46/EC. V porovnání normativ lze najít značné shody. Z uvedeného lze usoudit, že při plánování vývoje informačního systému, který má pokrýt funkce laboratoře a zároveň být v souladu s legislativou, není nutné brát tolik zřetel na zemi původu dokumentu, kterým se prostředí upravuje, jako na faktickou podstatu dané úpravy, na její přínos.

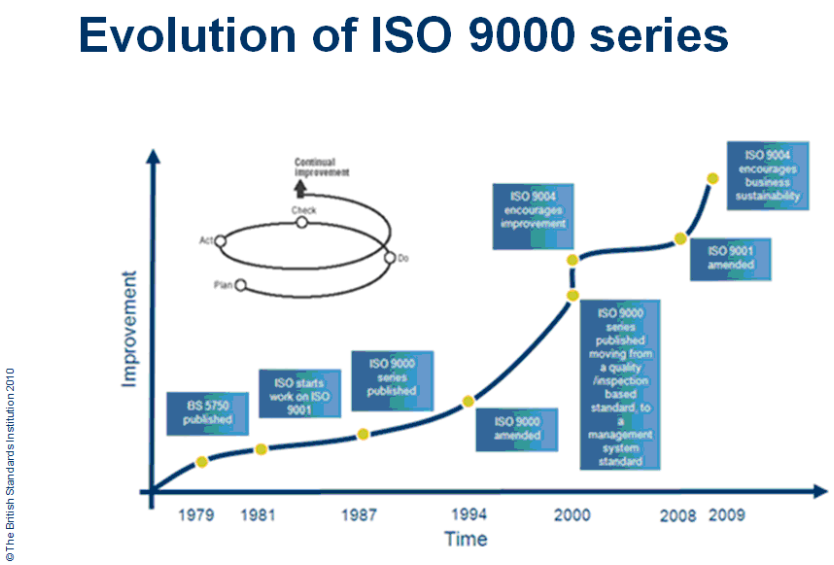
Lze říci, že certifikaci a re-certifikaci pracovišť se specifickým zaměřením je vhodnější využívat model postavený na normách integrujících jiné do svého znění. Ne vždy je to však možné, ne vše lze unifikovat jedinou normou. Pro laboratoře je důležitý management jakosti (ISO 9001) a věrohodnost naměřených výsledků (ISO 17025) [25]. Proto moderní laboratoře staví svou seriózност na ISO 15189.

Výše uvedená fakta jsou hlavní linií a jsou zde uvedena pro nastínění složitosti problematiky prostředí laboratoří. Počet akreditovaných laboratoří se mezi evropskými zeměmi značně liší, velké rozdíly jsou dány přístupem k podpoře akreditací správními orgány států, rozdíl je i v použitých metodikách. Pro činnost laboratoří primárního výzkumu lze v uvedeném nalézt, pro vybrané části workflow, jisté paralely. Bez ohledu na množství vydaných nařízení, ať jde o kterýkoli druh laboratoře, je třeba při návrhu jeho zabezpečeného frameworku detailně prostudovat a řešit všechny oblasti, které mohou na bezpečnost celého systému mít vliv.

Pravidla pro primární výzkum jsou také postavená na opakovatelnosti postupů a následném statistickém vyhodnocení výsledků experimentů k prokázání jejich věrohodnosti. K přispění obhájení výsledků je důležité, aby vybavení laboratoří bylo pravidelně kontrolováno a přístroje kalibrovány stejně, jako tomu je u laboratoří klinických. Součástí systému kalibrace je i její evidence čímž se dostáváme k ovlivnění činnosti laboratoře primárního výzkumu podle ISO 17025. Implementace norem do IS vede v k vyšší efektivitě laboratoří, redukci úkonů rutinních činností díky zvýšené automatizaci a lepšímu nastavení vnitřních procesů. Elektronizace dokumentů ve spojení ukládáním dat do databáze přináší usnadnění dalšího zpracování výsledků. S tím je spjatá všeobecný základní požadavek na chod laboratoře a tím je evidence. Pojem v sobě ukrývá dohledatelnost vzorků, dokumentace, dat, výsledků, přístrojů a zařízení a chemikálií. Forma elektronických laboratorních deníků pro klinické laboratoře může být v jistém ohledu jednoduší. Za pomoci šablon pro jednotlivé postupy se sleduje jejich dodržení a tím zaručení kvality. Naproti tomu se v laboratořích primárního výzkumu laboratorní deníky plní poznatky a postupy které slouží jako podklady zachování know-how, jako manuál pro opakování experimentu při prokazování možnosti dosáhnout popisovaného výsledku a také jako zdroj informací pro psaní závěrečných zpráv a vědeckých článků. Slučitelnost LIMS pro klinické laboratoře se systémy laboratoří primárního výzkumu je v tomto bodě vyloučena.

Druhým vymezením pro tuto práci je, že není jejím cílem hledat a nalézt metodiku vývoje SW, zda využít spirálu, vodopád, evoluci nebo extrémní programování. O výhodách použití různých metodik je možné se dočíst v různých pojednáních [22], [23], [26]-[28]. Je třeba zmínit, že jde o krok přicházející po důkladném pochopení místa, nebo též domény, v němž má být SW systém nasazený. Chybějící porozumění požadavkům uživatele může vést jedině k zdlouhavému vývoji, umoření finančních prostředků převyšující předpokládanou výši a nejistému výsledku. Problémem vývoje SW jsou měnící se požadavky zadavatele – uživatele, což nemusí být dáno jeho nerozhodností. Systém organizace práce se přizpůsobuje podmínkám, trendům a legislativě.

Dále zmíněné mezinárodní normy mohou tento fakt velice dobře ilustrovat. Zásadní vliv na firemní prostředí přináší rozhodnutí managementu organizace sledovat efektivitu odvedené práce a zajistit neměnnost vysoké kvality výstupů, tedy, implementace mezinárodní normy ISO 9001 – Management jakosti do podnikové struktury. Historie vzniku ISO 9000 spadá do roku 1987, kdy byly v Anglii vypracovány její základy. Jako mezinárodní norma pod označením ISO 9000 byla poprvé vydána v roce 2000 a slučovala tři standardy 9001, 9002 a 9003. Od roku 2008 se kolekce rozrostla o normu ISO 9004, který věcně rozšiřuje předešlé. Náhled na její vývoj lze získat z obrázku č. 2. V rámci jednotlivých řad lze ještě sledovat tzv. revize., které upravují, nahrazují a doplňují nevyhovující zastaralé části. Verzi normy rozeznáme podle názvu, kódového označení, kde je uveden rok revize. Zmíněná ISO 9001 měla uzavřenu revizi v roce 2008 a pak v roce 2015, název poslední revize má tvar ISO 9001:2015.



Obrázek č. 2 - Vývoj normy ISO 9001, zdroj [I.15]

Vývoj SW pro pracoviště s certifikací nebo akreditací [22] vyžaduje zahrnutí podmínek, které je nutné dodržovat. Jak již bylo zmíněno, dochází u znění norem k periodickým revizím, které by měly mít, dle informačního materiálu ISO [I.16] v cyklu pěti let. Takové rozpětí nepředstavuje problém, lze ho považovat za běžnou součást životního cyklu počítačové aplikace. Co zůstává nejdynamičtějším prvkem ovlivňujícím vývoj, jsou měnící se požadavky zadavatele - uživatele [29]. Ten tímto způsobem reaguje

na podněty přicházející se novým zadáním úkolů. O co více se doba vývoje IS prodlužuje, o to složitější je jeho dokončení.

Mimo výše uvedených standardů a metodik, existují i další, které se fungování podnikové IT struktury dotýkají. Dále jsou zmíněny ty, které se byly při vytváření frameworku shledány zajímavými pro svůj obsah, případně jeho stavbu ovlivnily.

ITIL (Information Technology Infrastructure Library) Je metodika zaměřená na běžné obchodní a administrativní modely, je brána jako standard v poskytování IT služeb a je založena na procesním řízení organizace[26], [27]. Lze ji snadno použít pro konsolidaci různých systémů, neboť není závislá na platformě. I v našem modelu je IT službou, která napomáhá činnosti laboratoře. Rozdílem je množství omezení daných zákony, která je třeba respektovat. To je důvod, proč pro zde navrhovaný model není právě tato metodika zcela vhodná. Lze však konstatovat, že při jejím studiu lze nacházet shodná nebo velmi podobná řešení či filozofii s metodikami konkrétně zaměřenými na podmínky laboratorních provozů.

NIST (National Institute of Standards and Technology) je laboratoř měřicích standardů, která spadá pod ministerstvo obchodu USA. Jejím cílem je kvalitní standardizace v průmyslu a obchodu, jejímž prostřednictvím napomáhá zvyšování konkurenceschopnosti USA. Na standardy, jež vydává a zmínky o souladu s nimi, lze je nalézt na stránkách mnoha firem i mimo území USA. Díky detailnímu zaměření jednotlivých dokumentů na konkrétní problém, přináší pro všechna odvětví mnoho využitelných standardů. Pro biomedicínskou laboratorní praxi a IS můžeme uvést SRD 69 obsahující seznam chemických látek doplněných o metadata potřebná pro další zpracování, pro oblast IT je to pak NIST 800-128, což je Příručka pro řízení bezpečnosti informačních systémů.

ICH (International Concil of Harmonization) je instituce zaměřená na standardizaci v laboratořích. Své výstupy shrnuje do čtyř oblastí označovaných písmeny Q, E, S, M, což jsou počáteční písmena anglických slov shrnujících obsah. Kvalita (Q) je oblast, v níž se snaží o nastolení harmonizace za pomoci definování prahových hodnot v testech příměsí, flexibilní přístup farmaceutické kvality založené na řízení rizika dobré výrobní praxe. Efektivita (E) se zabývá návrhem, chováním, bezpečností a hlášením klinických studií. Zahrnuje také nové typy postupů a použití farmakogenetických / genomických technik k výrobě lépe cílených léčiv. Bezpečnost (S) zahrnuje komplexní sadu bezpečnostních pokynů pro odhalení potenciálních rizik, jako je karcinogenita, genotoxicita a reprotoxicita. Multidisciplinarita (M) je pak oblastí, do které patří témata, která nelze jednoznačně zařadit do předchozích tří, pro ICH stěžejních. Zahrnuje tzv. ESTRI, což jsou Elektronické standardy pro přenos regulačních informací, jinými slovy, jde o rozhraní, které zahrnuje podporu i jiných národních standardů.

Systém řízení bezpečnosti informací, označovaný zkratkou **ISMS** (Information Security Management Systém) je součástí ISO 27000 [I.16], což je souhrn řady norem týkajících se bezpečnosti informací. Jde o dokumentovaný systém, podobný ITIL a COBIT, který přináší trvalé monitorování a zlepšování systému řízení bezpečnosti informací. Nabízí přechod od nesystémového a neuceleného řízení bezpečnosti k systému komplexní řízené bezpečnosti. Díky tomu dochází ve společnosti, kde je systém implementovaný, ke snížení rizik v oblasti informačních systémů. Staví na zvýšení povědomí a odpovědnosti zaměstnanců při práci s informacemi.

GAMP 5 představuje poradní nástroj využitelný pro efektivní vytvoření výpočetního systému, který má splňovat jednak požadavky na něj kladené ze strany zadavatele, ale také bude zohledňovat zákony a normy platné v pro daný obor činnosti. Podporuje přístup životního cyklu založeného na ověřených postupech (GxP), objasňuje funkce rolí a jejich zodpovědnost. Je kompatibilní s širokou škálou dalších metod, metodologií a schémat. Zahrnuje standardy systému kvality institutu IEEE a také certifikační schémata mezinárodně platné normy ISO 9000, modely SW procesů dle ISO 12207, metody vývoje SW i principy výše zmíněné ITIL, COBIT a ICH.

Ověřenými postupy GxP se rozumí základní mezinárodní požadavky na farmacii. Vycházejí ze souhrnů uvedených v amerických zákonech FD&C a US PHS, nařízení FDA, směrnic EU, japonských předpisů nebo jiných příslušných vnitrostátních právních předpisů nebo nařízení, podle nichž se společnost řídí. Patří sem mimo jiné:

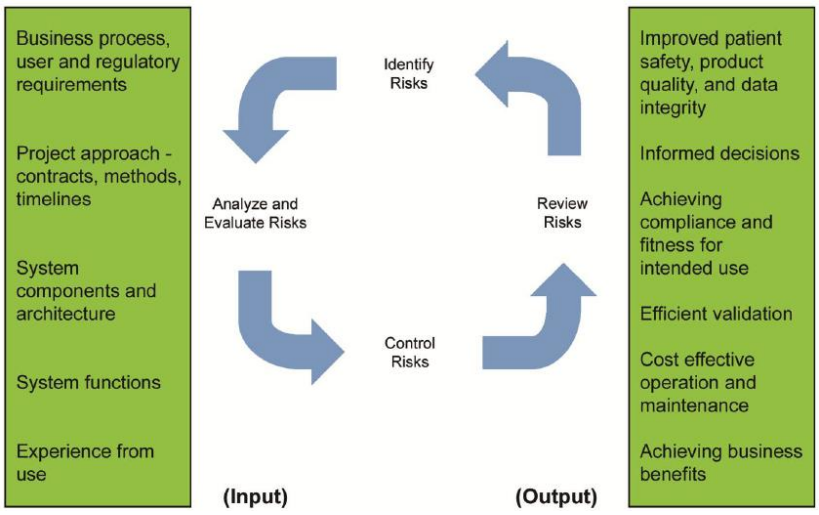
- Správná výrobní praxe (GMP)
- Správná laboratorní praxe (GLP)
- Správná distribuční praxe (HDP)
- Dobrá praxe v oblasti kvality (GQP)
- Dobrá praxe v oblasti farmakovigilance
- Dobrá klinická praxe (GCP)
- Pravidla zdravotnických prostředků
- zákon o předepisování léků (PDMA)

4.2 Základy modelu frameworku

LMS a LIMS obsahují funkce podpory činností a efektivního řízení laboratoře. Neboť je pro řešení informačního systému použitý elektronický informační systém postavený na výpočetní technice, je zde další oblast, která ovlivňuje jeho použitelnost [30]. Při vývoji informačního systémů je vhodné použít ověřených postupů řízení životního cyklu [31].

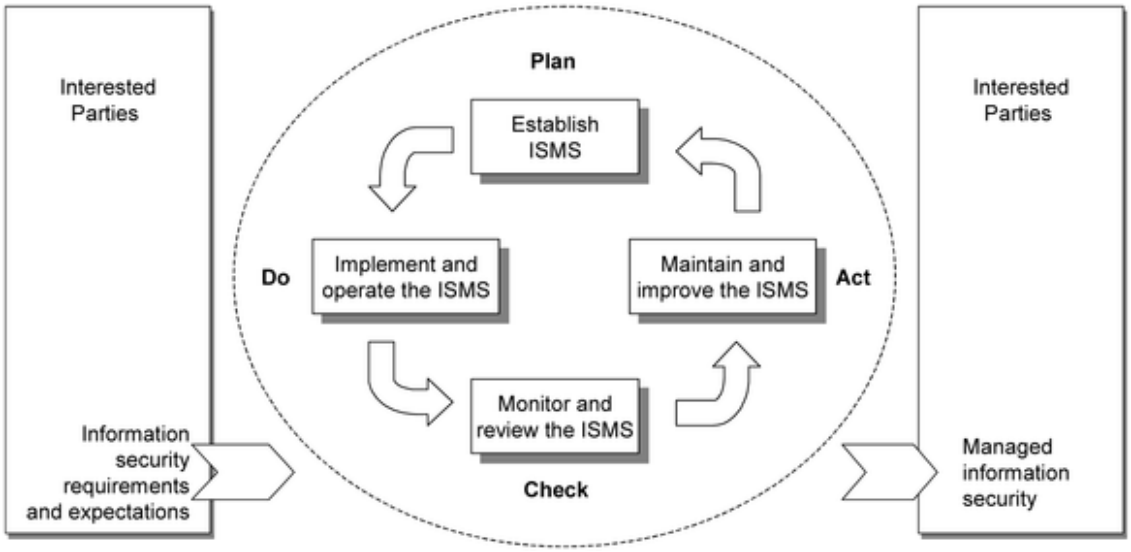
Pro podporu rozhodnutí, zda využít v případě LIMS laboratoře primárního výzkumu všeobecný model pro stavbu podnikového informačního systému na základě podnikové architektury, např. TOGAF nebo některý z nástrojů uvedených v kapitole 4.2, je třeba na samém počátku vyhodnotit, jestli se jedná o kritický systém. V případě laboratorního systému, který je nasazen v prostředí toxikologické, biologické nebo biomedicínské laboratoře, je zřejmé rozhodnutí navíc podloženo faktem, že tyto typy laboratoří podléhají zákonným normám vztahujících se k jejich provozu.

LIMS lze chápat jako informační systém bezpapírové laboratoře, neboli, elektronický dokument management systém. Pro uvedení klinického informačního systému do praxe je třeba provést jeho validaci, což je proces, který vyžaduje vytvoření centrálního validačního plánu. Pro posouzení rizik se využívá Frameworku některého z výše uvedených systémů. Konkrétně GAMP 5 je postavený na životním cyklu řízení rizik, jak je znázorněno na obrázku č. 3 a nabízí ucelený soubor průvodců jednotlivými fázemi celého procesu. Od konceptu, přes projektování a provoz k odstavení a migraci dat. Řízení jakosti rizik je, dle ICH Q9, systematický proces hodnocení, kontroly, komunikace a přezkumu rizik pro kvalitu léčiv po dobu celého životního cyklu produktu. Životní cyklus zahrnuje všechny fáze v životě produktu od počátečního vývoje až po jeho ukončení a je v metodikách často uváděný.



Obrázek č. 3 – Životní cyklus řízení jakosti rizik, zdroj [28]

Jde o vyobrazení všeobecně chápaného životního cyklu, který je upraven k účelu řízení rizika. Podobný obrázek (obrázek č. 4) nabízí např. ISO 27001 pro ISMS – Information Security Management System, který se v překladu uvádí jako Sytém řízení informační bezpečnosti.



Obrázek č. 4 - Životní cyklus dokumentace ISO 27001:2005, zdoj [I.17]

Existují studie, které porovnávají různé standardy, frameworky a doporučení, používaných pro zlepšení mapovaných procesů. V [32] se uvádí porovnání COBIT (Control Objectives for Information and Related Technologies) s podobnými frameworky, např. ITIL, TOGAF, CMMI asociací ISACA. Srovnávány jsou z pohledů dopadu na IT výkonost, nebo k hodnocení používané metodiky k analýze nákladů, přínosů a rizik, které souvisejí s používáním norem a nástrojů.

Pokud bychom chtěli opravdu na IS laboratoře primárního výzkumu tento model aplikovat, stačilo, aby další postup následoval jednotlivé kroky některého z manuálu. Dopad na výběr dodavatelských firem i rozsah možností prováděných experimentů [33] by mohl vést k omezení kreativity, která je v primárním výzkumu potřebná.

5 NÁVRH STRUKTURY LIMS

LIMS navrhovaný v této práci [V.3] vychází ze známé organizační struktury uvedené v 4.1 a z workflow získaného studiem prostředí laboratoří primárního výzkumu. Má blokovou strukturu, která je vyobrazena na obrázku č. 5. Jde o sadu základních a rozšiřujících modulů, jež mají následující funkce:

LabApp

Hlavní modul podpory činností v laboratoři. Je rozhraním k databázi DataDB, kde jsou uložená data z výzkumů. Primárně plní funkci elektronického laboratorního deníku.

LibrarApp

Jedná se o modul aplikace, pomocí níž uživatelé ukládají elektronické publikace dotýkající se prováděných experimentů do příslušné databáze. Zdrojem mohou být například dokumenty vyhledané na Internetu nebo získané v rámci odborných přednášek a konferencí.

EduApp

Zamýšlený modul podpory vzdělávání studentů a pracovníků. Materiály v něm uložené by mohly být

- manuály k vybavení používanému v laboratoři
- Směrnice provozu laboratoře
- instruktážní videa

ArchApp

Modul je předurčen pro archivaci výsledků projektů, jejich data již nejsou déle využívána, avšak jejich informační hodnota není zdaleka nulová.

AuthApp

Je modulem pro správu a řízení uživatelských účtů uložených v databázi UserDB. Jeho prostřednictvím se definují základní uživatelská oprávnění pro celý LIMS.

DirectApp

Manažerský modul obsahuje funkce potřebné pro řízení laboratoře. Umožňuje zadávání, přidělování, sledování a vyhodnocování úkolů. Dovoluje vyhodnocovat skupiny i jednotlivce podle aktivit v systému logovaných.

LogistApp

Modul podpory funkcí logistiky nemá za úkol nahradit funkci účetního pracoviště. Za jeho pomoci lze řešit dílčí úkony spojené se sledováním spotřebního materiálu uloženého a používaného v rámci prováděných experimentů.

DevIn a Connect

Nejsou moduly v pojetí aplikace s grafickým uživatelským rozhraním, které by bylo využíváno laboranty. Mají za úkol zprostředkovat načtení dat do datové DB informačního systému z externích zdrojů dat. Může jít o laboratorní přístroje, které disponují standardizovaným rozhraním, případně externí datové zdroje národních klinických DB systémů. Dále moduly poskytnutí zabezpečené připojení k databázi externím aplikacím určeným pro statistické vyhodnocování dat. Jsou standardizovaným rozhraním pro vstupně výstupní operace.

AgentTech

Zamýšlený modul má obdobnou funkci jako DevIn. Rozdíl spočívá v typu zařízení, která připojuje k IS a databázi, do níž dovoluje zápis. V souladu s cílem návrhu LIMS založeného na moderních technologiích je tento modul zprostředkovatelem zápisu dat z autonomních systémů postavených na agentech ambientní inteligence do syslog databáze označené AuditDB.

UserDB

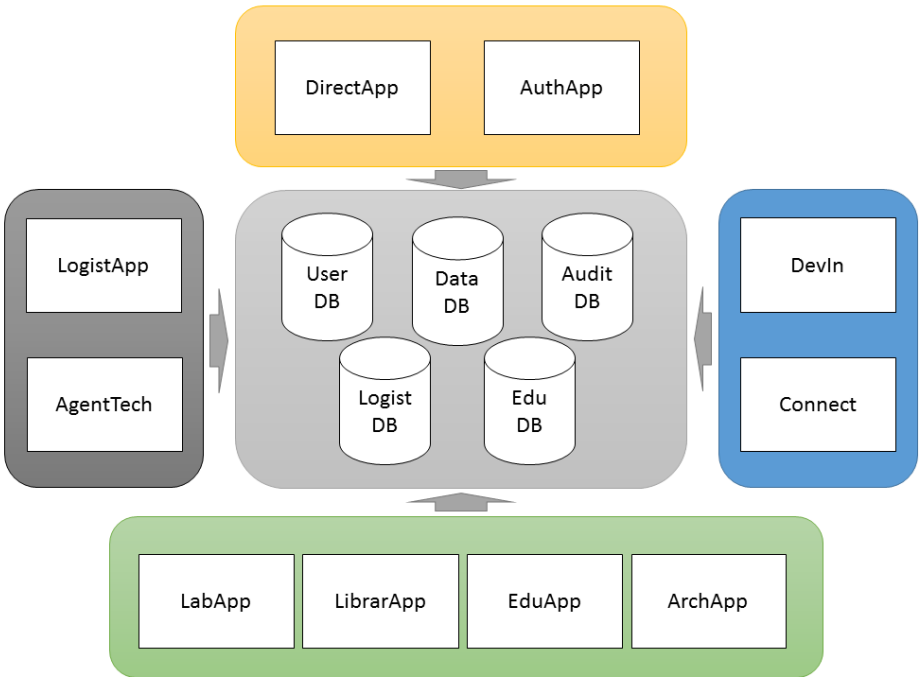
Centrální databáze uživatelských účtů, skupin a bezpečnostních politik základních i rozšířených modulů systému LIMS. Je místem pro ověření oprávnění pro přístup k výpočetní technice laboratoře, ke grafickému rozhraní modulů systému, ale také k ověření oprávnění vstupu do jednotlivých zón laboratoře.

AuditDB

Centrální syslog databáze, tedy místo uložení logů informačního systému i externích zařízení, která se systémem komunikují.

DataDB

Centrální databáze pro bezpečné uložení pracovních dat a metadat s nimi svázanými. Řízený přístup k datům je realizovaný pouze prostřednictvím aplikací a konektorů LIMS.



Obrázek č. 5 – Blokové schéma LIMS, zdroj: vlastní

Bloky na obrázku č. 5 zahrnují pouze oblasti činnosti laboratoře, které lze informačním systémem podpořit. Nebyl do něj zahrnutý blok podpory informačního systému, neboť lze sledovat, že laboratoře bývají zahrnuty do struktury jiných subjektů a pokud ne, je vhodné, aby se o IT služby staral externí dodavatel. HELPDESK, jak jej můžeme jednoduše označit, nemá vazbu na žádnou část navrhovaného LIMS. Oddělení podpory nadřazených subjektů mívají svůj nezávislý systém sběru požadavků a ne jinak tomu je i u komerčních poskytovatelů IT služeb.

5.1 Popis funkcí

Výše popsané moduly je třeba chápat jako články mozaiky, které na sebe navazují. Základní moduly, které tvoří jádro LIMS jsou DirectApp, AuthApp, LabApp. S nimi jsou bezprostředně svázány databáze UserDB, DataDB a AuditDB. Další moduly a databáze rozšiřují komfort nabízených funkcí.

Základní funkcí LIMS je podpora rutinních činností. Jejím základním prvkem je elektronický laboratorní deník (ELD). Pro laboratoř primárního výzkumu je třeba ho koncipovat mnohem volněji v porovnání s jeho obdobou v LIMS klinické laboratoře. V deníku je třeba uchovávat postupy a údaje, které se váží k zadání, které dostal laborant v rámci realizovaného experimentu. Zápis v databázi tedy bude obsahovat nad jejich rámec metadata, z nichž bude zřejmé, kdo a kdy činnost prováděl v rámci jakého

experimentu. Jednotlivé zápisy je třeba opatřit časovými značkami, které např. dovolí manažerovi laboratoře detailnější vyhodnocení práce laboranta, který se na experimentu podílel. Některé experimenty jsou postavené na zpracování chemických látek, které je třeba dopředu připravit. Takto vedené záznamy umožní lepší časovou a materiální koordinaci experimentů jako celku. Všeobecnou výhodou elektronicky vedených záznamů je možnost rychlého vyhledávání v nich. Zde jde o zásadní parametr. Pro výše uvedený popis funkcí nelze modul LabApp zjednodušeně označit za ELD.

Záznamy v laboratorním deníku slouží k evidenci a následné archivaci průběhu a výsledků laboratorních činností konkrétní osoby laboranta. Mají umožnit dohledání detailů pracovního postupu a to včetně data a jeho výstupů. Pokud dojde k situaci, kdy je třeba experimenty zopakovat, jsou k tomu využity právě tyto záznamy. Forma vedení laboratorního deníku se odlišuje podle určení laboratoře. Zde je příklad vedení deníku chemickotechnologické laboratoře. Na očíslovaných stránkách se píší chronologicky následující položky:

- datum záznamu
- jasný název činnosti
- důvod (návaznost, souvislost s projektem s uvedením jeho názvu), postup (průběžný, přesný záznam pracovního postupu), veškerá aktuální data (navážky, koncentrace, teploty, látky včetně čistoty, dodavatele/výrobce a čísla šarže, přístroje …)
- místo uložení dat (pokud jsou s výsledkem spjaty výstupy z počítače, název datového souboru vč. jeho umístění)
- další důležitá pozorování (netypické jevy, problematické jevy, odlišnosti od obvyklostí jako sraženina, zbarvení, …)
- záznam čísla stránky do obsahu deníku

Do elektronických souborů, které s daným měření souvisí s výsledky/daty je vždy třeba zanést metadata o osobě, která měření prováděla, datum měření, název měření:

- jméno osoby, která měření provedla
- datum měření
- název měření
- stručně podmínky měření, použitý materiál, roztoky...
- odkaz na laboratorní deník (ID deníku, záznam)

Proces autentizace a autorizace je součástí všech IS. Ověření identity uživatele, ale i aplikace nebo autonomního zařízení, které v systému plní funkci zdroje informací, je pro zachování bezpečnosti a integrity dat nezbytné. Vybrané implementace, které pojetí navrhovaného systému staví bezpečnější, budou zmíněny dále v textu.

Pro provedení experimentu v rámci výzkumu je třeba mít dostatek informací. Příprava se staví jednak na informacích z výsledků dosažených vlastním bádáním, ale také na informacích, které jsou dostupné na Internetu ve vědeckých databázích. Dnešní výzkum je prací týmu a činnost jednotlivce je stavebním kamenem. Popis výsledku experimentu se skládá z částí, dílčích činností. Získat kolekci zdrojových informací tak mohou poskytnout jen ti, kdo se podíleli a svědomitě zpracovávali poznámky. Ke zjednodušení procesu se nabízí řešení, napojení databáze, v níž se použité dokumenty budou ukládat. Je vhodné unifikovat formát dokumentů, což s ohledem na zdroje většinou bývá standard PDF. Se souborem se automaticky ukládají metadata. Obsahují primárně informaci o času vložení, osoby, která vklad provedla a kód experimentu, pro který byla vložena. Laboratoře se obvykle zabývají určitou problematikou, proto je vhodné doplnit základní soubor metadat o klíčová slova, která pomohou najít v databázi takovéto knihovny dokument znovu pro podobný experiment v době budoucí a ušetřit tak čas při opětovném vyhledávání v globálním prostředí. Týmy v laboratořích nebývají vždy stabilní, a pokud jde o laboratoře na univerzitách, je pochopitelné, že lokálně uložené soubory laborantů zmizí společně s jejich odchodem, pokud není organizačně vytvořený jiný systém ochrany know-how. V popisovaném LIMS je modul LibrarApp zamýšlený právě pro tento případ. Návrh modulu i v dalším vychází ze specifických potřeb laboratoří primárního výzkumu. Zmíněné prostředí univerzitních laboratoří a fluktuace osob laborantů s sebou přináší nutnost časté a periodicky se opakující edukace. K odlehčení času pedagoga nebo vedoucího laboratoře lze použít kurzy uložené v elearningovém systému. Laboratoře běžně takový nemívají k dispozici, proto jej lze řešit jako modul, zde označený jako EduApp, a který je součástí LIMS. Nespornou výhodou řešení je, že nevyžaduje další instalaci prostředí pro svůj běh. Integrace do systému ve formě kategorizace výukových materiálů dovoluje nabídnout uživateli užší výběr témat pro právě realizovaný typ experimentu. Mimo to lze tímto způsobem nabídnout elektronické verze manuálů používaných přístrojů, metodiky základů práce a pohybu v laboratoři nebo materiály pro pravidelná povinná bezpečnostní školení.

Základní skladba záznamu

- digitalizovaný nebo digitální informační zdroj nalezený na Internetu převedený do off-line PDF podoby
- možnost přidat odkaz v rámci prohledávání DB knihovny při práci na jiném experimentu

Vazba modulu na IS:

- spojení s probíhajícím experimentem
- nástroj kontroly duplicit
- logování akcí vytvoření záznamu v knihovně (časová známka, autor záznamu, název příspěvku, experiment ID, doplňkové informace)

Data starších experimentů a uzavřených projektů není nezbytné držet v produkční databázi společně s aktivními daty. ArchApp je modulem, který dovoluje provádět operace vedoucí k přesunu a údržby takových dat, která se již pravidelně nepoužívají. Opětovnou dostupnost je možné řešit na vyžádání, což zvyšuje jejich zabezpečení.

Laboratoře využívají pro realizaci experimentů zařízení, která jsou dnes často postavená na integrované výpočetní technice. Tyto, mimo funkce ovládání periferií, jsou schopná vytvořit kolekci dat a ta poskytnout na výstupu ve formě textu, grafu a tabulky ve standardizovaném formátu. V zájmu jejich automatizovaného přenosu do informačního systému se programují tzv. konektory, jimiž je možné provést přenos přímo do databáze. Odpadá tak pravděpodobnost vzniku chyby přepisem, data lze provázat s ELD. Modul DevIn patří mezi volitelné položky a jeho použití závisí na znalosti rozhraní pro programování rozhraní (API), které se de facto pro každé zařízení liší. Nespornou výhodou je použití přístrojů s rozhraním, které je běžně s výpočetní technikou využíváno, např. z radiologie je znám systém PACS a formát DICOM.

LogistApp je posledním ze seznamu modulů uvedených výše. Jak z akronymu vyplývá, jde o integraci soubor logistických funkcí, které rozšiřují portfolio nabídky o oblast zabezpečující chod laboratoře. V rámci informačního systému je vhodné mít přehled o dostupném materiálu v laboratoři. Plánování experimentů i provádění experimentů je postaveno na skladových zásobách. Podobně jako lze vytvořit konektor propojující laboratorní přístroj s LIMS, lze provést napojení na podnikové systémy a umožnit tak zjednodušení manipulace s materiálem, jeho evidenci, spotřebu i objednání. Pro osobu zodpovědnou za logistiku propojení znamená, že nemusí vybrané operace provádět duplicitně. Periodicky zpracovávané zprávy o zásobách a spotřebě jsou takto dostupné online. Jejich validita závisí na kvalitě vložených informací, což je věcí nastavení organizačních procesů. Existuje i možnost zvýšení automatizace, která bude zmíněna dále v textu.

Management modul

Běžně tento modul obsahuje funkce pro organizaci činnosti organizace/pracoviště. Bezpečnostní pravidla jsou zakomponována do procesů řízení workflow na úrovni skupin a konkrétních uživatelů.

V rozsahu práce není třeba se jimi zabývat, neboť nepřispívají k rozvinutí tématu.

Rozšířením funkcí navrhovaného systému je napojení na DB logů činností. Tu lze hlavně využít k řešení bezpečnostních incidentů. Z nadhledu ale zjistíme, že informace v ní uložené mají značnou vypovídací hodnotu o pracovním nasazení osob pracujících v laboratoři. Jestliže jsou zde dostupné záznamy ze systému ochrany vstupu, lze vyčíst, kdy byl pracovník na pracovišti a kolik času zde strávil. Při vyšší míře upřesnění dotazu můžeme zjistit, kolik kdo strávil času v laboratoři za určité období. Moderní informační systém by měl mít prvky ambientní inteligence, tedy HW komponenty (sensory a čidla), která mohou v rámci naprogramované role fungovat autonomně, ale mohou odkládat periodicky některé záznamy do databáze logů. Ze záznamů a se znalostí problematiky procedury lze odvodit, jak si počínali vybraní pracovníci při plnění úkolů.

Všeobecně lze pak, na základě vyhodnocených aktivit, provést hodnocení celkové aktivity konkrétních pracovníků, jejich přínos pro tým množstvím doplněných relevantních informačních zdrojů do databáze knihovny, rychlostí zpracování úkolů, šetrnou spotřebou materiálu.

Pro rychlý náhled jsou vhodné přednastavené šablony dotazů na často sledované akce. Možné je provést manuální definování filtrů, které lze doplňkově uložit mezi vlastní šablony.

5.2 Kategorizace dat

V uvažovaném LIMS se setkáváme se čtyřmi kategoriemi dat:

- **Data z experimentů** se v LIMS zpracovávají na úrovni modulů, které jsou nastaveny k jejich vyhodnocení a reportování. Podpora validity vědecké práce je postavena na statistických metodách, proto je třeba, aby výstupy z databáze výsledků byly dostupné v požadované formě. Může jím být export do CSV dokumentu nebo možnost připojení statistického SW přímo k ní.
- **Kolekce elektronických studijních materiálů**, vkládaných z modulu LibrarApp, je plněná pracovníky laboratoře ručně v průběhu hledání a doplňování informací k prováděným experimentům. Záznamy jsou provázány s experimenty a ELD. Vstup dat musí být ošetřen proti vzniku duplicitních záznamů, což v případě modulu LibrarApp může být kontrola kódu DOI, ISSN, ISBN. Ne všechny dokumenty je mají, proto bude třeba nalézt další možnosti jak zabránit nepřiměřenému nárůstu databáze.
- **Databáze auditu** je citlivým zdrojem data vyjma zdrojů, které do ní logují informace, by žádný další prvek neměl mít právo zápisu. Veškeré další přístupy by měl být jen k výběru informací zde uložených a to buď v základních šablonách pro rutinní kontrolu běhu laboratoře, anebo na

základě filtrování dat definovaném uživatelem. Některé incidenty mohou mít dlouhodobější průběh a při jejich objasňování, vzhledem k předpokládanému velkému objemu různorodých dat, bude vhodné využít dataminingových metod. U Záznamů je třeba ošetřit integritu dat, ochranu proti neautorizované modifikaci. Jako vhodné se jeví kontrolní součty a hash [34].

- **Databáze uživatelských účtů a přístupových oprávnění** je spravovaná centrálně v rámci serveru a je pod dohledem administrátorů.

U všech uvedených databází je třeba, aby

- jejich struktura byla postavená tak, aby pokryla požadavky LIMS.
- bylo prováděno pravidelné zálohování
- byla pravidelně prováděna údržba, při níž by se data starší, než bude definované, buď archivovala, anebo mazala.
-

5.3 Řízení oprávnění

Zabezpečení přístupu k obsahu LIMS má dvě úrovně. První je tvořena autentizací uživatele k vlastnímu počítači. Tím je ověřena oprávněnost osoby všeobecně. Druhou tvoří autentizace vůči samotnému LIMS. Většina systémů je postavena na důvěře pracovního kolektivu a tedy neobsahuje detailní členění oprávnění [I.8]. Přístup k datům je definován na bázi rolí uživatele. Může jím být administrátor, manažer, logistik, laborant. Každá role má v systému definovaná oprávnění přístupu k určité části dat a způsobu manipulace s nimi. Uživatelský účet, ač je jedinečný, má přiřazenou roli, která mu umožní shodný přístup, jako má každý člen skupiny se stejnou rolí. Tedy, pracovníci stejné úrovně vidí do všech experimentů a mají možnost data číst i modifikovat bez ohledu na fakt, zda v něm jsou zainteresovaní. V certifikovaných systémech se provedené operace logují, což přináší personalizaci případné nekalé aktivity a snadnější identifikaci autora. Je pak jen na odolnosti systému, zda lze a jak obtížně tuto překážku obejít. Zatímco v certifikovaném systému je systém logování definovaných informací podmínkou akreditace laboratoře, ostatní systémy mohou mít k sledování aktivit vágnější až odmítavý přístup. Na takových pracovištích se provozují autonomní aplikace nebo LIS/LIMS řešení, která jsou primárně zaměřená na podporu činnosti v laboratoři jako takové [I.18]-[I.23] a ostatní moduly systému mají podobu odlehčených verzí nebo zcela chybí.

Dále navrhovaný systém vychází z nutnosti vyššího zabezpečení zpravovaných dat. Oprávnění pro uživatele v něm lze proto nastavit na úrovni skupiny i na úrovni osoby a přiděleného úkolu. Aktivity

se v mnohem vyšší míře logují, aby je bylo možné v případě potřeby spojit do stopy vedoucí k objasnění incidentu.

Z toho důvodu je celý systém postavený na třech fyzicky oddělených a přitom na aplikační vrstvě provázaných databázích.

Databáze pracovních dat obsahuje vstupní data a výsledky badatelské činnosti.

Databáze uživatelů nese informaci o uživatelských účtech a oprávněních.

Do **databáze auditu** se logují informace o úspěšných i neúspěšných aktivitách osob v dosahu LIMS.

Navrhovaný LIMS si neklade za cíl mít plně integrované SIEM funkce, ačkoli k nim agregace dat patří. Kolekce logů událostí z LIMS nepochybně může být zdrojem pro takový systém. Zdroje SIEM jsou obvykle síťová zařízení, v našem jde především o aplikace a jejich aletry na výstupu. Technologie umožňuje jejich online analýzu s ohledem na bezpečnostní dopad v reálném čase.

5.4 Prvky ověření identity

Autentizace a autorizace jsou všeobecně základními stavebními kameny ochrany duševního vlastnictví, ať jde o informace o výzkumu a vývoji nebo postupech výrobního procesu. Proces Autentizace osoby přistupující k systému a Autorizaci jejích oprávnění je třeba vidět z pohledu prostředí, v němž jsou nasazené. Informační systém primárně určený pro podporu administrativních úkonů je schopen běhu na běžně dostupných HW prostředcích. Autentizace uživatele spočívá v zadání uživatelského jména a hesla při přihlašování do operačního systému pracovní stanice, případně do prostředí IS organizace. Tato prostředí jsou jistým způsobem „slepá“ vůči reálné identitě přihlašované osoby. Jde o akt důvěry nastavený na úrovni systémové bezpečnosti organizace. Jejím základem je systém autentizace podpořený proškolením pracovníků o dodržování postupů, které mají zamezit bezpečnostním incidentům. K tomu je nutné mít zpracované směrnice, které ne vždy musí vycházet z norem a doporučení. Tato volnost pojetí se dotýká převážně malých firem, středně velké a velké pak již jsou k dodržování mezinárodně uznávaných postupů nuceni systémem certifikací, motivované možnou ztrátou konkurenční výhody.

Heslo, coby zmíněný řetězec znaků, je historicky nejpoužívanější způsob autentizace provázející lidstvo. Jeho elektronická podoba, kdy uživatel vypíše sekvenci znaků na klávesnici terminálu, zajišťuje vstup do různých systémů již několik desítek let. Jeho prolomitelnost závisí na kombinaci faktorů technického a lidského. Je třeba najít soulad mezi oběma. Pod technickým můžeme vidět snahu o dosažení

komplexnosti hesla a to v definici, které znaky lze k jeho tvorbě využít a v jaké míře, Lidský faktor omezuje rozmach technického faktoru schopnostmi mozkové kapacity. Heslo může v mnoha operačních systémech dosahovat 32 znaků délky (ačkoli manuál pro MS Windows 2003 deklaruje 127 znaků), v některých aplikacích není délka omezena vůbec (na Facebooku odzkoušeno heslo 1000 znaků) nebo se využije jen první blok 8 znaků a ostatní se ignorují (IOS). V praxi použitelné heslo musí být snadno zapamatovatelné a výrazně kratší. Dostatečná délka je pojem, který odvozen od technických možností, odolat případnému útoku, kdy je heslo generováno z předpokládaných znaků v rozsahu předpokládaného počtu znaků. Existují též slovníkové útoky, kdy hesla nejsou generována, ale načítána při pokusech o prolomení ze seznamu. Proto by se hesla neměla tvořit ze slov, rozhodně ne z frekventovaně používaných a s vazbou na osobu či prostor nasazení.

Jak snadné či složité je prolomit heslo při dodržení výše uvedeného vychází z počtu znaků virtuálního jazyka a počtu znaků použitých pro vytvoření hesla. Velikosti virtuálního slovníku pak můžeme pro jednoduchost vyjádřit jako variaci s opakováním.

$$VVS(D, PZJ) = PZJ^D$$

Kde:

VVS … velikost virtuálního slovníku

PZJ … počet znaků jazyka

D … délka hesla

Pro jazyk složený z 62 znaků to znamená 218,340,105,584,896 možností., tj. když použijeme velká a písmena abecedy a číslice (a-z; A-Z; 0-9). V případě použití běžně užívaných speciálních znaků se základní množina znaků jazyka navýší na 78 a počet možných hesel na šestinásobek předešlé hodnoty. Počet speciálních znaků je pro uživatele omezený na ty, které lze bez problému zadat z klávesnice s převážně českým rozložením kláves. Po podrobném prozkoumání souboru lze konstatovat, že asi 1/3 takto vygenerovaný hesla nesplňuje požadavek komplexity, což není zcela v souladu s všeobecným modelem uvedeným v [35] věnujícímu se bezpečnosti autentizace. Výpočet se zde opírá o doporučení používání minimální délky hesla osm znaků [I.24] při dodržení podmínek komplexity.

Komplexní heslo, jež se skládá z dostatečného počtu znaků v kombinaci alfanumerických a speciálních znaků, může v zabezpečeném systému, který dovolí jen určitý počet špatných pokusů v definovaném časovém intervalu, s vynucenou dobou platnosti, s vysokou pravděpodobností odolat různým druhům útoků.

V kontrastu ke snaze ochránit cenné informace hesly se v současné době potýkáme s nutností časté autentizace. Internet je plný služeb, na nichž závisí mnoho rutinních činností jedinců, firem i států. Emaily počínaje, přes sociální sítě, podnikovými informačními systémy konče, neustále zadáváme identifikační údaje, přičemž se mnohdy necháme zlákat nabídkou prohlížečů ke zjednodušení života tím, že se údaje uloží a budou použity při příští návštěvě stránek. Otupění a přehnaná důvěra v aplikace působí, že jen málo uživatelů přemýšlí nad tím, v jaké podobě a kam se hesla uloží, zda nemohou být zcizena.

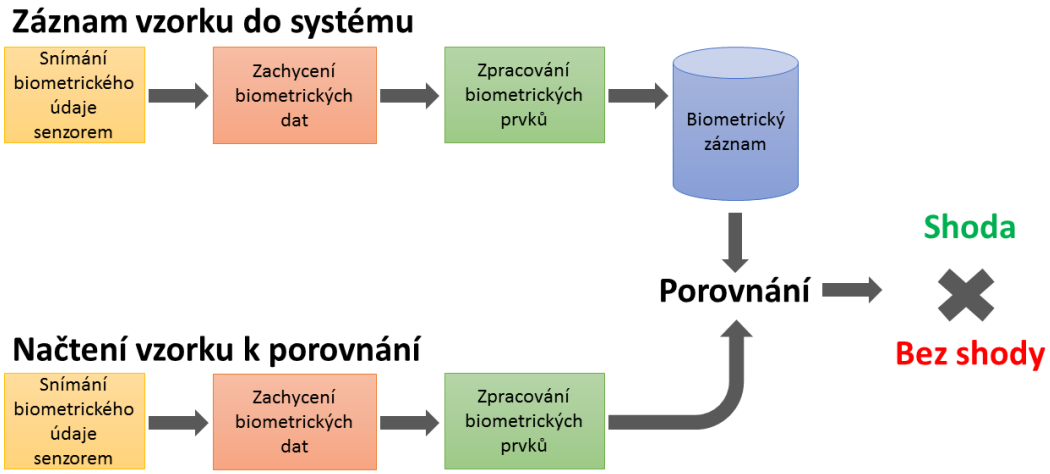
Podnikové systémy nabývají složitosti, která ne vždy dovoluje použití federativních služeb pro propojení navazujících systémů do jednotného přihlášení tzv. Single Sign On. Důvodem mohou být rozdílné bezpečnostní politiky, které definují odlišnou konvenci pro tvorbu hesla a její exspiraci. Množství přihlašovacích údajů a jejich vynucená obměna uživatele vede ke snaze si situaci usnadnit bez ohledu na doporučení či nařízení.

V prostředí podnikových sítí, navzdory osvětě a školením zaměstnanců, se nelze zcela zbavit sdílení účtů mezi spolupracovníky, psaní hesel na nástěnky, rámy LCD panelů či zadní stranu klávesnic. Vedení hesel v elektronické podobě v textovém souboru uloženém na ploše pracovní stanice nebo v mobilním telefonu, k němuž má přístup jen přihlášený uživatel, je iluzorní. Vyspělejší uživatelé k tomuto používají aplikace, které vložená citlivá data uchovávají v šifrované podobě v cloudu. Je však otázkou, do jaké míry lze takovému systému důvěřovat, jakou míru rizika představuje rozkrytí uložených informací pro jednotlivce nebo společnost, jejíž přístupové informace jsou takto kompromitovány. Spojení uživatelského jména a hesla je označováno jako jednofaktorová autentizace.

Pro zvýšení bezpečnosti lze doplnit použití přihlašovacích údajů vícefaktorovým ověřením. Dvoufaktorovým v praxi rozumíme rozšíření jednofaktorového například o bezkontaktní kartu s kódem, kterou je třeba vložit do čtečky připojené do USB portu počítače. Jiná varianta je postavená na hardwarovém klíči, v podobě USB zařízení (dongle), které se musí v rámci ověření oprávnění připojit k PC.

S využitím biometrických údajů lze již identitu uživatele ověřit s vyšší přesností a spojit ho s akcí nebo událostí v systému v daném čase. Využívá se jich pro silnou, například třífaktorovou, autentizaci. Jde o případ, který je složením více faktorů do jednoho celku. Uživatel zná své přihlašovací údaje, ty ale může mnoha způsoby vyzradit. K tomu vlastní nosič s kódem, který mu může být zcizen. Třetím údajem je unikátní identifikátor osoby, jenž je vlastní jen ověřované osobě. Tou je zde biometrická charakteristika daného člověka, ale může jím být i charakteristika jeho chování.

Mezi běžně používané prvky a metody patří porovnání otisků prstů, obrazu duhovky či sítnice, tváře, geometrie ruky, anebo hlasu se vzorky, které se před tím uloží v zabezpečovaném systému. Obrázek č. 6 daný postup popisuje.



Obrázek č. 6 – Obecný model porovnání biometrických údajů, zdroj: [I.25]

Biometrické markery jsou jedinečné a průkazné, avšak nelze je chápat jako samostatný prvek autentizace. Lze je považovat za podobný identifikátor, jakým je uživatelské jméno. Snahy o kompromitaci biometrických záznamů zdaleka nejsou naprosto neúspěšné, jen nejsou v poměru s úsilím a vynaloženými prostředky efektivní. Z toho vyplývá, že je nelze klást na úroveň přístupového hesla, což ne zrovna vhodně deklaruje materiál firmy DELL [I.25] z roku 2006, coby prvek silné autentizace. Chápeme-li heslo jako řetězec volitelných znaků, je možné jej v případě prozrazení nahradit jejich jinou kombinací. Naproti tomu je biometrická informace jedinečná, proto se nehodí pro zabezpečené systémy jako komplexní náhrada kombinace uživatelského jména a hesla. Navíc je silným identifikátorem vlastníka, proto by se měla využívat jen ve skutečně přínosných situacích.

Jak bylo uvedeno, použití biometrických údajů je spojené s jejich načtením a vyhodnocením. Jednotlivé varianty mají své klady a zápory, které ve spojení s technickými nároky na realizaci určují, masivnost využití v praxi.

Autentizace na základě otisků prstů patří mezi nejstarší a nejrozšířenější aplikace. Má relativně vysokou přesnost, je rychlá a snadná. Pro její využití stačí relativně malé snímací zařízení. Pokud chceme využít geometrii ruky, musíme počítat s mnohem většími snímači, což při použití k autentizaci

osoby při vstupu do objektu nevadí, ale jako periferní zařízení počítače není v mnoha situacích použitelný. Dále lze využít porovnání charakteristických rysů tváří popsaných rozměry a jejich poměry. Vyhodnocení se provádí na základě fotografií nebo videozáznamů. Omezení metody vychází primárně z rozlišení snímacího čipu a světelných podmínek, dále pak z použití brýlí, výrazu tváře a změn způsobených například úpravou vousů. K porovnání hlasových vzorků s hlasem identifikované osoby stačí mikrofon, tedy jde o velmi levnou implementaci, navíc je jazykově nezávislá. První nevýhodou je, že k porovnání se používají slovní fráze, jejichž vzorky mají velký objem. Přesnost je silně ovlivněna hlukem na pozadí a změnou hlasu z důvodu stresu a onemocnění. Podobně jako snímek obličeje, lze využít snímek duhovky. Jde o proces nasnímání běžného odraženého světla a porovnání s uloženým snímkem. Limitující je detailní nasnímání oka osoby, což vyžaduje vyšší interakci s ověřovanou osobou a může působit problém citlivým osobám. Stejný problém je to i pro nasnímání sítnice, kde navíc dochází k jejímu aktivnímu osvětlování.

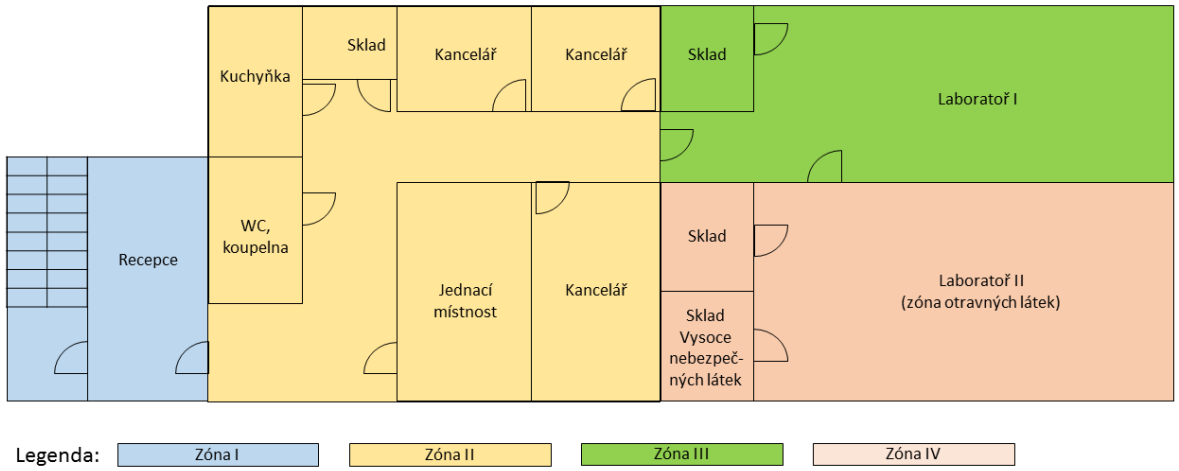
Řešením pro jisté modely systémů se nabízí vícefázové ověření, které je běžně užívané právě pro bezpečný přístup ke kritickým aplikacím, kompromitací jejichž rozhraní by mohlo dojít k velkým škodám. Využívají jej jednak bankovní instituce, firmy, které poskytují přes datovou síť svá cenná data, ale také poskytovatelé služeb. Mimo informací, které zná a zadává uživatel pro přístup do daného systému, je třeba zadat další, jednorázový, kód. Ten může být vygenerovaný zařízením v držení uživatele, nebo aplikací v jeho mobilním telefonu, anebo mu může být na základě požadavku provedení transakce vygenerovaný a poslaný na telefonní číslo mobilního telefonu, jenž má evidované u poskytovatele služby. Doplňkovým bezpečnostním prvkem samotného kódu je zde časové omezení doby platnosti kódu a nemožnost kód použít opakovaně.

Ve specifickém pracovním prostředí, jakým laboratoř je, se dostáváme k zásadním limitám použití všech výše uvedených metod. Jejich striktním vynucením by došlo ke znemožnění rutinní činnosti v reálném čase nebo k enormnímu zatížení pracovníků zvýšením nadbytečných úkonů, což by, dle zvyklostí, vedlo k obcházení nasazených bezpečnostních procedur a zhoršení situace.

Využití biometrických prvků je snadné, avšak v prostředí laboratoře jen těžko realizovatelné. Brání tomu používání ochranných pomůcek. Přes rukavice nelze získat otisk prstů, ochranné brýle mohou působit odlesky, které znemožní načtení rohovky. Rouška přes ústa utlumí hlas. Navíc rouška a brýle mění fyziognomii obličeje, tedy ani rozpoznání tváře uživatele se nejeví vhodným způsobem identifikace.

Pokud pojmeme laboratoř jako objekt, který není tvořený jen prostorem, v němž se provádějí experimenty, jsme schopni rozdělit danou plochu do zón s definovanou úrovní zabezpečení. Tím se situace změní a úměrného zabezpečení lze dosáhnout.

Počet zón vychází z určení laboratoře a látek, které se zde zpracovávají a uchovávají. Základem jsou tři zóny, které jsou blíže rozpracovány dále v textu. Pracovník se v nich pohybuje podle fáze pracovního úkolu a podle denního harmonogramu.



Obrázek č. 7 – Ilustrační obrázek rozložení zón v budově biomedicínské laboratoře, zdroj: vlastní

Na zjednodušeném modelu pracoviště uvedeném na obrázku č. 7 lze ukázat modelový případ o čtyřech zónách. V následujícím textu není uváděno plné technické vybavení, které je nutné pro provoz laboratoře. Pohyb pracovníků je třeba udržet plynulý, nerozptylovat a nezatěžovat je nadbytečnými, potažmo zbytečnými úkony. Průchody mezi zónami jsou proto řešeny bezkontaktními čtečkami a mechanismy automatického mechanického ovládání dveří. Výjimku tvoří přechod mezi první a druhou zónou.

První zónu tvoří vestibul s recepcí, kam mohou bez omezení vcházet z vnějšího prostoru jak zaměstnanci, tak návštěvy a dodavatelé. Zaměstnanci procházejí po provedení autentizace do vnitřních prostor laboratoře, ostatní jsou buď odbaveni službou na recepci. Pokud tato není součástí laboratoře, je spojení mezi první a druhou zónou řešené interkomem do zvolené kanceláře nebo místnosti.

Druhá zóna je přístupná dvojicí terminálů, které tvoří redundantní prvek primární kontroly vstupujících osob. Samotný prostor je tvořený prostorem s možností volného pohybu osob. Nachází se zde kanceláře, jednací místnost, odpočinková místnost s kuchyňkou, WC, koupelna a úklidové zázemí.

Třetí zóna je prostorem, v němž se provádějí přípravy experimentů a chemických látek. Je zde také sklad chemikálií a biologických vzorků. Na rozdíl od čtvrté zóny se zde nepracuje s nebezpečnými, toxickými či psychotropními látkami. Přístup do ní mají všichni pracovníci laboratoře podílející se na experimentech.

Do čtvrté zóny pak má vstup povolen jen úzký okruh pracovníků. Pracuje se zde s potenciálně nebezpečným materiálem, jehož pohyb a zpracování je třeba sledovat, a k jehož používání je třeba mít dostatečnou kvalifikaci. Prostory jsou oddělené dveřmi s elektrickým zámkem nebo rámy, které jsou s to identifikovat průchod osob a propustit jimi jen ty, které mají patřičné oprávnění.

Uživatel při příchodu do laboratoře z venkovního prostoru musí projít recepcí, tedy první zónou, do vnitřní části pracovní oblasti, zóny druhé. Je mu povolený volný pohyb šatnou, odpočinkovou částí a do kanceláře, kde má zázemí pro studium, plánování a zpracování výsledků bádání na výpočetní technice. V případě participace na praktickém experimentu může vstoupit do laboratoří, třetí zóny, vyzvednout si potřebný materiál a využívat laboratorní přístroje a pomůcky. Volitelně může být pohyb v těchto prostorách monitorovaný.

Ve čtvrté zóně, v závislosti na její velikosti a uspořádání nebývá nezbytné, aby pohyb laborantů byl neomezený. Pracuje se zde primárně s toxickými látkami a jedy. I zde však platí, aby pohyb po tomto pracovišti, v prostoru se zvláštním režimem, byl maximálně plynulý a to včetně přístupu k materiálu potřebnému k provádění experimentů. Manipulace s materiálem zde podléhá precizní evidenci o zpracování a uložení.

Zjednodušeně lze říci, že do zóny jedna mají přístup osoby ke vstupu do zóny dva oprávněné i neoprávněné. Kontrolovaným přechodem se do zóny dva dostávají jen osoby oprávněné a část neoprávněných v doprovodu oprávněných. Do třetí zóny mají teoreticky přístup jen osoby oprávněné. Vybrané typy návštěv však nelze striktně zakázat, neboť jde o prostor, do něhož musí mít přístup pracovníci servisu přístrojů a zařízení. Čtvrtá zóna je přístupná jen po provedení bezpečnostních opatření, která musí zabránit jednak nepovolené manipulaci s materiálem, jeho zcizení nebo intoxikaci.

Hlavní důraz je položen na přechod mezi zónami. Mezi první a druhou zónou není problém využít kombinace jakékoli metody z výše uvedených. Mezi druhou a třetí a uvnitř třetí pak nastupují omezení výše popsaná omezení pro biometriku. Počáteční ověření musí proto být maximálně přesné, aby následný pohyb byl postaven jen na bázi např. jednofaktorové autentizace.

Pro praktickou realizaci u výše popsaného modelu se jeví technologicky vhodné propojení biometriky a čipů s dosahem cca 50cm. Mohlo by jít například o RFID Class 0+ a novější, u nichž lze do čipů zapisovat, což je zásadní požadavek pro funkci zabezpečeného systému. Pro zápis je k dispozici prostor 256 bitů, přičemž technologie umožňuje čtení 1000 tagů/sec, což je limit důležitý pro průmyslové využití a v logistice. V podmínkách navrhovaného využití v laboratoři je tento údaj silně předimenzovaný. Pro využití při identifikaci osob a monitorování jejich pohybu je zajímavější využití fyzikálních vlastností technologie pro vyšší přesnost údajů získaných ze čtecích zařízení. Systém RFID využívá různé frekvence, které ovlivňují dosah, rychlost čtení a zápisu a mají různé pronikání vln materiály. Anténa pasivního tagu je mnohonásobně větší než samotný čip. S rostoucí frekvencí klesá dosah, což vede k potřebnému zpřesnění pohybu načtením jen nejbližších čipů. Problém je, že s frekvencí zároveň narůstá elektromagnetické rušení, což by mohlo v blízkosti některých přístrojů vést k chybám ve čtení, ale zároveň lze tuto vlastnost využít ve spojení s cíleným stíněním k načítání tagů v určitém výseku.

Na místě přechodu první a druhé zóny lze provést autentizaci pomocí čipu a například načtení otisku prstu. Radiofrekvenční technologie není zcela odolná proti kompromitaci, proto je třeba pravidelně měnit kód uložený v čipu. Na terminálu mezi první a druhou zónou by se pracovník identifikoval otiskem prstu. Byl by vyzván k přiložení čipu na zařízení pro čtení a zápis. Po načtení kódu by tento byl porovnaný se záznamem v bezpečnostní databázi. Při shodě by byl vygenerovaný kód nový, který by se zapsal jednak do čipu a také do databáze. Blok pro zápis má RFID různý, odvíjí se od modelu a použité frekvence. Class 1 Gen 2 nabízí 512 bitů, což dovoluje až 2^{512} různých variant binárního kódu. Pokud bychom vycházeli ze základní ASCII tabulky, kde je 512 znaků kódovaných dvojicí hexadecimálních znaků, pak můžeme použít 64 takových znaků. Ve shodě s výpočtem v části věnované bezpečnosti hesla jde o řetězec 8x delší. Odpadá zde zátěž lidského faktoru, není třeba si jej pamatovat, změna probíhá s každým vstupem na pracoviště. Ochranu vloženého kódu lze v souladu s dokumentem NIST číslo 2015-19181 [34], který definuje SHA-3 jako standard, realizovat jeho uložením do čipu jako hash.

Do druhé zóny vstupuje ověřená osoba. Pokud by někdo vlastnil kopii kódu z předešlé přítomnosti sledované osoby na pracovišti, nebude jej moci využít. V návaznosti na úspěšném projití procesem ověření vstupujícího pracovníka laboratoře mu systém povolí další pohyb a manipulaci s materiálem uvnitř zón. S odchodem z pracoviště, registrovaným průchodem do první zóny, se jeho kód zneplatní. Vzhledem k propojení s centrální autentizační autoritou je možné takto zabezpečit i přístup k aplikačnímu profilu v LIMS. Pod daným uživatelským účtem může být na PC v laboratoři spuštěný několikadenní experiment, deaktivace účtu by jej mohla přerušit.

Pro další pohyb se jako vhodné provedení jeví zabudování čipu do náramku. Jeho nošení na pravé ruce není podmínkou, ale vychází z logiky, že na levé ruce bývají hodinky. Snímače v prostoru by

pak mohly být umístěné tak, aby anatomicky vyhovovaly snadné manipulaci a třeba i automatickému online vyhodnocování přítomnosti osob v konkrétní místnosti na pracovišti. Dveřní pohybová čidla, ve spojení s bezkontaktní čtečkou čipu a v návaznosti na bezpečnostní systém, uvolňují průchod do dalších prostorů a místností. K tomu by u vstupu do režimových zón nedošlo, pokud by v jejich těsné blízkosti stála neoprávněná osoba. Současné načtení dvou a více RFID, které bezpečnostní autorita vyhodnotí pro danou zónu protichůdně, vede k anulování požadavku na vstup.

Pohyb osob v laboratoři se řídí interními předpisy. Každá laboratoř musí mít vypracované bezpečnostní předpisy, které mimo jiné definují podmínky pohybu osob zónami laboratoře. Je nezbytně nutné do nich zahrnout postupy pro situace, kdy je nezbytné mechanismus ovládání dveří vyřadit a zabezpečit volný průchod. Jde o případy selhání mechanické nebo elektronické části elektronického zámku, výpadku elektrické energie, kdy jej není možno v reálném čase nahradit z vlastních zdrojů, havárie technologie laboratoře nebo při požáru či jiné živelné pohromě.

5.5 Komunikace a GUI pro LIMS

Grafické uživatelské rozhraní je třeba mít pro celý systém LIMS jednotné. Neboť se ve své podstatě jedná o SaaS implementaci řešení, které má svou infrastrukturu mimo objekt laboratoří a k přístupu do něj je potřebná konektivita do sítě Internet, bylo dohodnuto, že primárně využívaným interface bude webové rozhraní postavené na standardu HTML5 s podporou mobilních zařízení [36]. Komunikace prochází potenciálně nebezpečným prostředím, proto bylo využito běžného komerčního standardu jejího zabezpečení implementací SSL certifikátu. Bezpečné vkládání dat do databáze LabApp a LibrarApp bylo třeba umožnit, dle zadání, z libovolného místa s konektivitou, což se tímto podařilo vyplnit. Důvodem požadavku je fakt, že některé experimenty zabírají mnoho hodin strojového času, jejich ukončení nelze přesně odhadnout a mohou zasahovat do víkendů. Data z přístrojů, na nichž se tyto experimenty provádějí, lze často vyčíst přes webové rozhraní, které je dostupné při povoleném vzdáleném přístupu do sítě organizace z externí sítě.

5.6 Infrastruktura

Laboratoř není prostředí s rozsáhlou a složitou strukturou výpočetní techniky. Základem je infrastruktura tvořená routerem pro připojení k Internetu a přepínači. Dále jde vesměs o soubor koncových zařízení v jednom síťovém segmentu, který se často nemění jak ve smyslu změn HW vybavení tak nainstalovaných aplikací. Přesto je z pohledu zabezpečení datové bezpečnosti specifická.

Nejméně problematickými se jeví pracovní stanice. Zde je běžnou praxí automatická aktualizace operačního systému i nainstalovaných aplikací a to včetně antivirového zabezpečení. I v menších sítích je vhodné mít přehled o stavu a využít byť jednoduchou variantu nástrojů centrální správy.

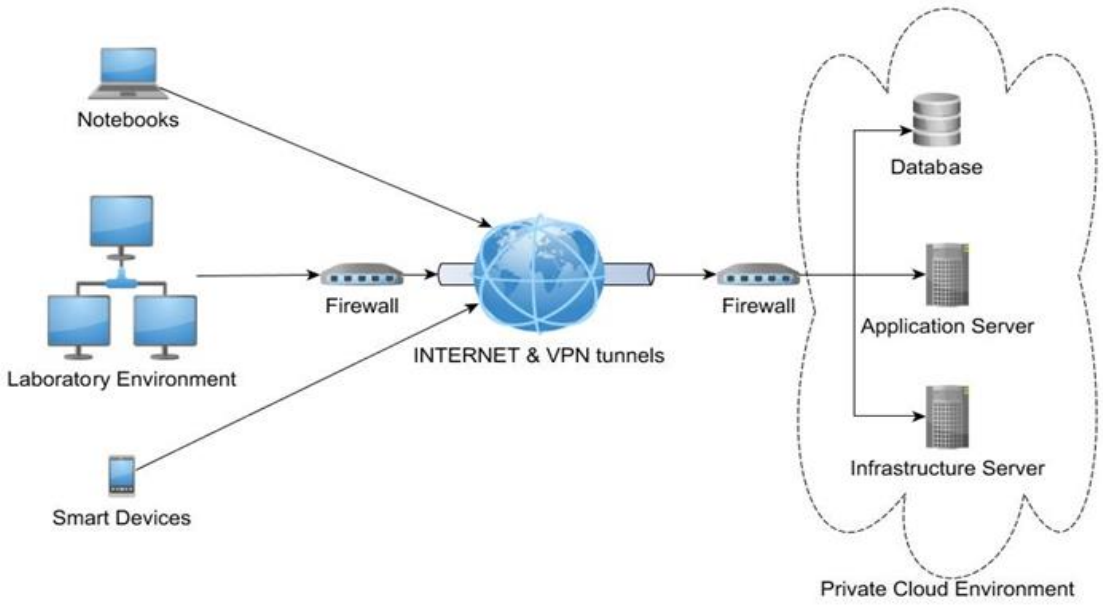
Specifickou kategorií výpočetní techniky v laboratořích jsou měřící, monitorující a vyhodnocovací přístroje založené na platformě počítačových komponent. Z pohledu nákladů je jejich pořízení nemalou investicí do vybavení laboratoří. Specifičností je, že jejich ovládací a vyhodnocovací SW je vytvářen v malých sériích a implementován na skupinu počítačů povětšinou shodného HW. V reálném provozu mnohdy životností překračují podporu HW i implementovaného operačního systému. Vývoj aplikační vrstvy bývá úzce svázaný s aktuální verzí operačního systému v čase dodání. Aktualizace navazující na vývoj operačního systému nebývá pružná. Může nastat situace, kdy po aktualizaci operačního systému program přestane fungovat nebo se stane nestabilním. Aktualizace se tak stávají řízeně opomíjené což je v rozporu s požadavkem na bezpečnost při připojení k síti kvůli online přístupu. Neaktualizovaný, nebo jen omezeně aktualizovaný speciální počítač, jehož operační systém již nemá podporu ze strany výrobce, se tak stává kritickým prvkem sítě. Takový stroj nebývá v dané síti jediný.

Do infrastruktury sítě laboratoří patří též servery. V souladu s trendem je navrženo jejich umístění do privátního nebo veřejného cloudu [37]. Hlavní benefit takového řešení jednoznačně je oddělení správy IT od laboratoře. Data a aplikace jsou uložená na nosičích mimo organizaci a o provoz služeb se starají IT specialisté daného centra [I.26], [I.27]. Převedení serverů do cloudu znamená zjednodušení topologie lokální sítě LAN. Odpadá její fragmentace, jejímž důvodem je oddělit síť uživatelů od serverové pomocí back firewalu, jenž brání šíření škodlivého kódu mezi segmenty. Výkon služeb na vyžádání tak plně závisí na prostředí, v němž jsou servery nasazeny. Non-IT pracovníkům laboratoře tak nastavený model dovoluje bezproblémovou rutinní činnost a jednoduchou správu na aplikační úrovni.

Uživatelé masivně využívají počítačovou síť k přístupu do LIMS a na Internet k vyhledávání informací, komunikaci a přenosům dat. Kritickým se tak stává spojení pracovišť s aplikacemi v cloudu a Internetem. Nová generace firewallů umožňuje nejen vytvoření VPN spoje mezi lokální sítí a cloudem, ale především ochranu před útoky [38]. Ty mohou přicházet jak z Internetu, tak z kompromitovaných

stanic. K jejich identifikaci se využívá sofistikovaných metod pro inspekci datových toků. Při dostatečném výkonu se nabízí využití online vyhodnocování monitorování provozu, založeném na porovnávání zachycených paketů se vzorky známých útoků uložených v databázi. Nevýhodou řešení je identifikace pouze zadaných, již známých, řetězců. Dané řešení je závislé na včasných aktualizacích. Útoky lze též identifikovat na základě sledování provozu, respektive odchylek od rutinního provozu, kdy lze takto podchytit i jeho nové formy [39]. Některé metody jsou založené na teoretických základech neuronových sítí [40]. Monitorování aktivit v síti se stává při množství hrozeb ve firemním prostředí nutností a má své místo při zabezpečení ochrany citlivých dat výzkumu a vývoje proti lokálním a externím útokům [41]. Při současném sledování bezpečnostních logů provozovaných systémů lze celkovou efektivitu výrazně navýšit. Daný systém se může v mnoha situacích rozhodnout autonomně, bez zásahu operátora. Aby nedocházelo k planým poplachům a následnému automatickému zablokování síťového provozu, je třeba pečlivě připravit rozhodovací algoritmy [42]. Finální rozhodnutí stejně zůstává na vyhodnocení stavu operátorem - zodpovědnou osobou, která je o potenciálním útoku vyrozuměna emailem a SMS zprávou na mobilním telefonu. Lze však říci, že známé formy DDoS útoků jsou jednoznačně identifikovatelné a proto je lze vyhodnotit systémem přímo a zásahem operátora protiopatření odvolat.

Realizace zabezpečení síťového provozu popsaným způsobem vede k použití inteligentních firewallů, které poskytnou ochranu serverům stejně jako pracovním stanicím pracovníků laboratoře a zvláště pak laboratorním přístrojům, jejichž řídící jednotka je založená na počítačových komponentách (Obrázek č. 8).



Obrázek č. 8 – Napojení laboratoře na infrastrukturní servery, zdroj: vlastní

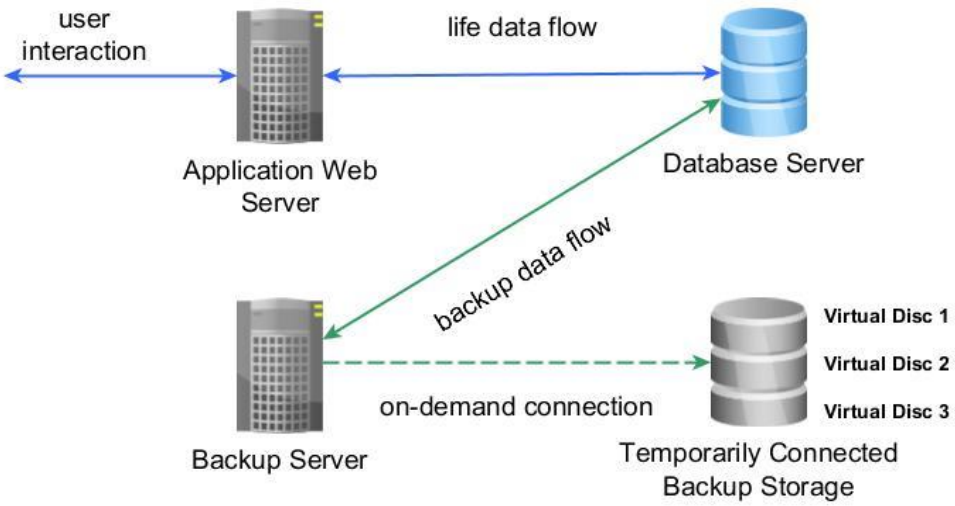
Ochranu dat ukládaných v prostředí cloudu je vhodné postavit na bezobslužném šifrování [V.5]. Problém je v implementaci, kdy je třeba provést rozhodnutí, která část ponese zátěž onoho procesu. Při snaze ušetřit procesorový čas na straně serverů cloudu lze data lze šifrovat na koncových stanicích. Jednak se tím rozdělí výkon potřebný na šifrování a dešifrování dat a zároveň data opouštějí pracovní stanici i server zabezpečená. Ne vždy je tato varianta vhodná. Při velkém množství zdrojů a jednoho šifrovacího klíče může dojít ke kompromitaci jednoho z nich a tím vystavení dat útočníkovi. Stejně tak je rizikem šifrovat data až na straně serveru, kde společně s daty může při jeho kompromitaci útočník získat jak data, tak i klíč, což ve výsledku může vést k situaci podobné Randsomware. Bez ohledu na zvolený model, nutnost zabezpečit datový spoj mezi laboratoří a Cloudem neodpadá. Lze k tomu využít různé metody (šifrovaná VPN, MPLS,…).

5.7 Zálohování

Zálohování dat je nedílnou součástí každého informačního systému. Na úrovni stanic se běžně neprovádí, neboť data jsou primárně ukládána v centrálním, cloudovém uložišti [I.18], [I.28]. Služby LIMS se zálohují na úrovni virtuálních strojů cloudu, přičemž stěžejní služby lze provozovat v clusterech. Data uložená v databázích jsou periodicky zálohována na úrovni systému s možností konkrétního nastavení v prostředí aplikace administrace. Záloha databáze účtů je nedílnou součástí zálohovacího schématu operačního systému. Z důvodu dohledatelnosti účastníků případných incidentů je nezbytné, aby se účty osob, které již nejsou zaměstnanci laboratoře, archivovali minimálně po dobu definovanou pro archivaci logů.

Vzhledem k reálné hrozbě, kdy byla data uživatelů zašifrována Randsomwarem, byl systém zálohování upraven tak, aby v případě proniknutí nákazy do vnitřní sítě a k uloženým datům, vznik škod byl eliminován na co nejnižší úroveň. Díky dostatečnému diskovému prostoru v privátním cloudu si systém záloh s každou novou úlohou vytvoří nový virtuální disk, který se připojí k systému provádějícímu zálohování a po ukončení zálohování zas odpojí. Virtuální disky jsou dynamické, záloha má proto adekvátní velikost. Po provedení nové plné zálohy se disky s nejstaršími závislými zálohami odstraní. V případě kompromitace dat, případně i provedení zálohy šifrovaných dat, není dotčena celá záloha ale jen virtuální disk v té době připojený (Obrázek č. 9). Obnova dat po eliminaci zdroje nákazy nebo po obnově havarovaného systému má reálnou šanci vrátit systém do stavu odpovídajícímu době provedení poslední použitelné zálohy. Jde de facto o imitaci zálohování na výměnná média, odpadá zde

však zásadní problém fyzické manipulace s nimi, životnosti a čitelnosti přepisovatelných médií. Duplikováním zvoleného virtuálního disku, obsahujícího plnou zálohu, můžeme vytvořit archivní médium, které je v případě potřeby možné k produkčnímu systému snadno připojit.



Obrázek č. 9 - Logické schéma zálohování s odděleným uložištěm s připojením na vyžádání, zdroj: vlastní

6 VÝBĚR BEZPEČNÉ PLATFORMY PRO LIMS

Jak vyplynulo již v úvodní části, je třeba pro tvorbu IS znát úroveň zabezpečení od nejnižších stavebních prvků. Je proto nezbytné prověřit i nestranná hodnocení použitého HW a platformy, na níž IS bude portovaný. V základu lze říci, že LIMS pod Open Source licencí lze rozdělit do dvou skupin. Buď jde o kompletně naprogramované dílo anebo upravené aplikační prostředí CMS (content management system). Úskalí systémů z první skupiny je jednoznačně závislost na podpoře týmu, který daný IS vytváří. Ačkoli se může takový systém jevit jako modulární, možnosti programování vlastního rozšíření a úprav stávajícího je jen velmi problematické. Instalace vyžaduje přísnější podmínky pro nastavení prostředí. Testování zranitelností takového systému je náročné časově i technicky. Naproti tomu je zde druhá skupina, jejíž nástroje se implementují snadněji. LIMS programované v CMS jsou vesměs na platformách operačních systémů nezávislé. Systémy lze získat i jako předinstalované virtuální stroje v tzv. „virtual appliences“ nebo jako balíčky, které se do již nainstalovaných operačních systémů integrují. Programovacím jazykem je ve většině případu PHP a JAVA, svoje místo však mezi nimi má i Python. I tyto systémy jsou závislé na podpoře komunity, která je vyvíjí, avšak díky otevřenosti jejich kódu i CMS je vyšší možnost v podpoře a ladění nástrojů a modulů na míru. Společně pro ně platí, že výběr Open Source systému pro implementaci v produkčním prostředí, musí být postaveno na pečlivém výběru. Je třeba zvážit dobu vývoje projektu, jeho podporu ze strany komunity vývojářů, pravidelnost vydávání oprav a vydání poslední verze, kvalita dokumentace pro administraci i uživatele, velikost a organizovanost komunity. V užším výběru systémů je třeba se zaměřit na přirozenost ovládání GUI, zda se v kódu plně odráží workflow laboratoře, možnosti administrace, zálohování, možnosti propojení s externí uživatelskou databází. Směr, pro úspěšný vývoj prostředí, jsou programovací standardy. Dle metodiky FDA se jedná o písemné postupy popisující konvence kódování (programování). Jsou v nich stanovena pravidla pro používání jednotlivých konstrukcí poskytovaných programovacím jazykem a pojmenování, formátování a požadavky na dokumentaci, které zabraňují programovým chybám, kontrolují složitost a podporují srozumitelnost zdrojového kódu.

Vývoj Open Source nástrojů pro různé vědní disciplíny komunitami je realizován již několik let. Následující porovnání vybraných operačních systémů a CMS je vázáno k době provedení, tedy počátku roku 2016. Nejsnazší cestou pro jejich vývoj je, pokud to určení aplikace dovoluje, využití CMS, který nabízí mnoho užitečných funkcí již ve svém základu. Vhodnou volbou lze získat základní prvek pro malý komunitní web, jakož i pro podnikový systém či laboratoř. Na Internetu je hned několik zdrojů, na nichž lze vhodný systém vyhledat (www.sourceforge.net, www.contentmanagementsoftware.info, www.wikilims.org). Nespornou výhodou nástrojů CMS je, že usnadňují vývojářům i administrátorům

správu webu i obsahu. Ačkoli CMS s sebou přináší zjednodušení tvorby aplikací a administrace prostředí, nejsou tyto systémy rozhodně bez chyby. V množství dostupných CMS může být velmi obtížné vybrat ten pravý. Jako jedno z hlavních kritérií je třeba brát i bezpečnost systému. Silné stránky i slabá místa CMS se přenášejí do prostředí aplikace v něm implementované. Z toho důvodu bylo rozhodnuto podmínit výběr LIMS prostředím v němž tato aplikace poběží a položit hlavní důraz na prověření stability, podpory a bezpečnosti na těchto složek.

6.1 Hodnocení rizik prostředí laboratoře

Z pohledu metodiky uvedené v [28] je řízení jakosti rizik systematický proces hodnocení, řízení, komunikace a přezkumu rizik ohrožujících bezpečnost pacientů, kvalitu výrobků a integritu dat založené na frameworku, který je v souladu s ICH Q9.

Používá se:

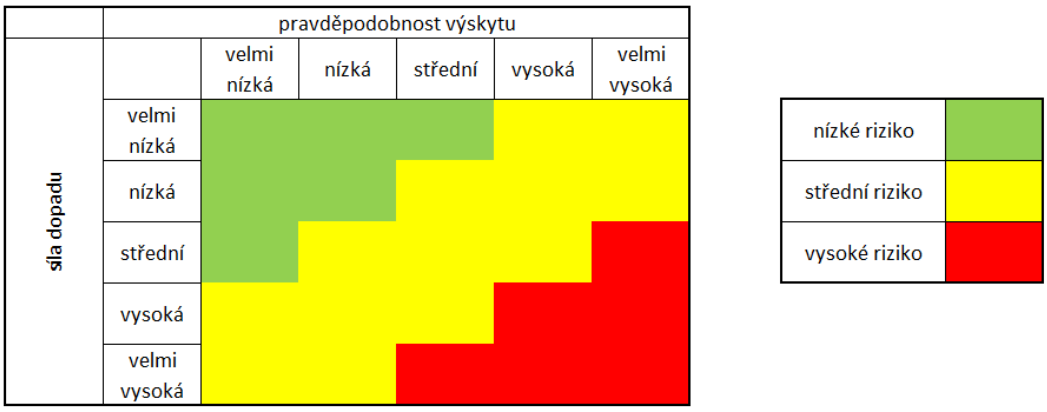
• k identifikaci rizika a jeho odstranit nebo snížení na přijatelnou úroveň

• jako součást škálovatelného přístupu, který umožňuje regulovaným společnostem vybrat vhodné činnosti životního cyklu na základě specifičností systému.

Proces budování zabezpečeného informačního systém je nutné podložit fakty, které dají reálný podklad rozšíření funkcionality modelů, které se běžně pro stavbu IS používají. Podrobit hodnocení je třeba všechny úrovně, na nichž bude výsledný systém vybudovaný. Lze vycházet z norem a jejich metodik zmíněných v 4.2. Volba je závislá na situaci, z níž vychází realizační tým. Avšak, pro komplexnost, lze doporučit systém GAMP 5, který zahrnuje mnoho z norem a nařízení ostatních a proto nabízí dostatečnou variabilitu, která se jeví vhodná i pro laboratoře primárního výzkumu a jejich laboratorní a management informační systém. Mimo ni existují metody všeobecnější, které nejsou úzce specializované na daný typ pracoviště. Potenciálem jejich použití je nalezení rizik v kontextu přesahujícím hranice běžně chápaného a interpretovaného elektronického informačního systému podpory rutinních činností organizace.

Lze například postupovat metodou What-If nad celou organizací a prostorem laboratoře. Lze takto získat přehled o (ne)dostatečnosti nastavených procedur přístupu na pracoviště, zabezpečení prostorů a skladů s materiálem různé úrovně citlivosti, odolnost proti výpadkům energie, nastavení

workflow různých interních procesů. Metoda byla ve formě brainstormingu použita i ve zde popisovaném případě. Pro přesnější vyjádření míry rizika pak existují jiné metody, např. HAZOP. Pro detailnější vyjádření a následné vyhodnocení je pak vhodné využít např. nástroje založené na mapě rizik, kdy každá událost je hodnocena z pohledu pravděpodobnosti výskytu a míry dopadu. Mapa obsahuje zóny, které jsou bodově ohodnoceny. Hodnoty pak vyjadřují závažnost. Často, pro rychlejší orientaci jsou zóny podbarveny, jako je tomu na obrázku č. 10. Jednotlivé hodnocené položky pak lze umístit do matice rizik.



Obrázek č. 10. - Grafické vyjádření zón různého stupně rizika, zdroj: [I.17]

Podobně lze metodu modifikovat a aplikovat na hodnocení míry dopadu opatření nastavených v souladu s normami, které u laboratoří primárního výzkumu nejsou nezbytné. Získáme tak přehled o místech a procesech, v nichž zachování nezávislosti na metodikách neovlivní tvůrčí prostředí. Tato práce se opírá o výsledky zjištěné při plánování nasazení LIMS do prostředí, kde takovýto systém nebyl nasazený. V rámci uvažovaného rozsahu funkcí byly některé položky řešeny rámcově, jiné nebyly definovány vůbec.

Z provedeného průzkumu v dotčených laboratořích a následného vyhodnocení vzešlo jako jednoznačné nejvyšší riziko možná ztráta výsledků vědecké práce a duševního vlastnictví organizace. Nižším, ale ne nezanedbatelným rizikem pak je manipulace s látkami a její evidence. Uvedené se stalo základem dále prezentované práce. Při hodnocení stavu, v kontextu znalosti nastupujících trendů, byly definovány směry možného dalšího technologického rozvoje zabezpečení pracoviště v návaznosti na plánovaný informační systém. Jejich popis je uveden v deváté kapitole.

Definice kvality informačního systému pak byla spjata s pojmy:

- spolehlivost provozu
- ochrana údajů uložených v systému
- důvěrnost definovaná oprávněností přístupu k uloženým informacím
- integrita dat (s důrazem na záznamy logů událostí)

Následující kapitoly se proto zaobírají vybranými úrovněmi a technologiemi, které na celkovou kondici systému mají vliv.

6.2 Výběr operačního systému

Problematika stavby LIMS počíná na úrovni volby operačního systému. Neboť CMS a tedy i aplikovaný LIMS jsou na volbě operačního systému nezávislí, je možné zvážit různé varianty. Jako možné se jeví též nasazení komerčního operačního systému Microsoft Windosws 2012 R2, který je sice placený, ale jeho cena, v rámci programu akademických licencí, nepředstavuje pro organizaci zásadní výdaj. Do jeho prostředí bude třeba naistalovat tradiční aplikace potřebné pro běh CMS a následně LIMS, tedy webový server Apache, databázový server MySQL a balíček podpory jazyka PHP. Jde o tradiční a prověřené stabilní Open Source prostředí oblíbené pro svou jednoduchou údržbu, modulární strukturu a snadné uživatelské nastavení plně respektující požadavky klientů. Nespornou výhodou je i jeho možná implementace ve velmi krátkém čase. Pravdou je, že tyto prvky byly vyvinuty pro platformu Linuxu, a že v prostředí MS Windows je jejich výkon nižší. Dále uvedené údaje jsou platné k datu, kdy byl tento blok připravovaný na prezentaci. Neboť se jak komunita vývojářů Linuxu, tak i programátoři Microsoftu snaží o udržení svých operačních systémů co nejvíce bezchybných a tedy i bezpečných, lze na základě průběžného sledování informací konstatovat, že se stav nezměnil.

6.3 Bezpečnost operačních systémů

Porovnání stavu bezpečnosti operačních systémů a jejich vyhodnocení proběhlo na základě prostudování záznamů CVE (Common Vulnerabilities and Exposures) společnosti MITRE v online databázi zranitelností [I.28].

Operační systém Microsoft Windows 2012 má od roku 2012, kdy byl uveden na trh, v záznamech 223 zranitelností. S operačními systémy Linux je situace méně přehledná, zde se lze odkázat na údaje vztažené k verzi jádra Linuxu. Uvedený údaj 1298 je třeba brát jako souhrnný od roku 1999. Po odečtení záznamů z roku 2011 a starších dojdeme k hodnotě 498, která je i tak podstatně vyšší než u konkurenčního systému. Jistou nepřesností v porovnání je, že neporovnáváme konkrétní edice OS Linux, které v rámci jejich sestav mohou počet zranitelností ještě navýšit. Pouhé porovnání výsledných hodnot je zavádějící, neboť OS Linux byl již plně nasazen, tedy potýkal se s problémy vývoje a hlavně rutinního provozu, kdežto OS MS Windows byl uveden a jeho chyby se teprve začaly objevovat. Tento fakt lze pozorovat v tabulkách č. 1 a 2, kde je postupný nárůst chyb u OS MS Windows 2012 R2 viditelný, kdežto v případě LINUX Kernel je zřejmý takřka konstantní výskyt chyb v jednotlivých letech.

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Mem. Corruption	Bypass Something	Gain Information	Gain Privilegs	# of exploits
2012	5		2	2		1		2	
2013	51	12	17	18	3	2	2	21	4
2014	38	9	11	5	3	6	5	12	4
2015	129	14	38	9	6	26	23	47	1
Total	**223**	**35**	**68**	**34**	**12**	**35**	**30**	**82**	**9**

Tabulka č. 1 – Zranitelnosti MS Window 2012 R2

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Mem. Corruption	Bypass Something	Gain Information	Gain Privilegs	# of exploits
2012	115	83	4	24	10	6	19	11	
2013	189	101	6	41	13	11	57	26	6
2014	133	89	8	21	10	11	30	20	8
2015	61	37	6	12	2	7	6	14	
Total	**498**	**310**	**24**	**98**	**35**	**35**	**112**	**71**	**14**

Tabulka č. 2 – Zranitelnosti jádra Linuxu

Z uvedeného lze odvodit, že zranitelnost obou OS je na přibližně stejné úrovni, a že volba nakonec nemusí být podmíněna jen porovnání jejich bezpečnosti. Lze ji postavit na firemní politice a schopnostech administrátorů o daný operační systém pečovat.

Pokud bychom zůstali plně na platformě Open source produktů, byla by logická volba buď některého operačního serverového systému Linux nebo CentOS. I zde by se prostředí doplnilo o již zmíněnou trojici Apache, MySQL a PHP.

Variantou může být i hybridní prostředí, jež spočívá ve využití specifických služeb obou platforem. Pokud by šlo o výstavbu zcela nového systému, je možná unifikace, avšak tato možnost není příliš pravděpodobná.

6.4 Výběr redakčního systému

Výběr CMS byl ovlivněn cílovou potřebou a to výběrem bezpečné platformy pro LIMS, nebo lépe, volbou bezpečné platformy, na níž se již LIMS nabízí. CMS programů je velké množství a proto je třeba na ně nahlížet podle definovaných kritérií. Jednou z možností je vycházet z podporované platformy. K dispozici jsou všechny běžně používané i některé spíše raritní (PHP, JAVA, Python, ASP.NET, Perl, Ruby on Rails,…) viz tabulka č. 3.

Platform	**CMS**
Java	Alfresco, Ametys CMS, Apache Roller, Dotcms, DSpace, Enonic, eXo Platform, Fedora Commons, Hippo CMS, Jahia, Liferay, LogicalDOC, Magnolia, Nuxeo EP, OpenCms, OpenKM, OpenWGA, XWiki
ASP.NET	Composite C1, DotNetNuke, KooBoo, mojoPortal, Orchard Project, Umbraco, BetterCMS
PERL	EPrints, Foswiki, Ikiwiki, TWiki, WebGUI
PHP	ATutor, b2evolution, CMS Made Simple, Dotclear, Drupal, DynPG, Exponent CMS, eZ Publish, Geeklog, ImpressPages, Joomla!, MediaWiki, MODX, Moodle, PHP-Nuke, PivotX, ProcessWire, SPIP, Textpattern, TYPO3, Wolf CMS, WordPress, XOOPS
Python	Mezzanine, Django-cms, MoinMoin, Plone, Wagtail

Tabulka č. 3 - Seznam Open source CMS řazený dle platformy

Nejvíce zastoupenou platformou je PHP, která se těší velké oblibě. Z toho důvodu se na jejím seznamu nachází nejvíce nasazované CMS – Wordpress, Joomla a Drupal. Společné pro ně je, že si za dobu své existence vybudovali silnou komunitní podporu, mají své projekty kvalitně zdokumentované. Neboť jde o modulární systémy, je pro jejich prostředí dostupné nepřeberné množství doplňků a šablon, které rozšiřují jejich funkcionalitu a zdokonalují design. Zmíněná fakta vedla k tomu, že se dostali do úzkého výběru. Každý z těchto systémů má své silné stránky a nedostatky.

Mnoho rozšiřujících modulů je poskytováno zdarma. Jde vesměs o jednoduché běžně používané funkcionality, avšak v nabídce jsou i moduly svázané s činností v lékařských zařízeních a laboratořích. Často plní jen dílčí úkoly, které jsou v rutinní praxi bez využití výpočetní techniky zdlouhavé. K dispozici jsou moduly elektronické laboratorní knihy, pro specifické výpočty nebo sběr a vyhodnocení dat z přístrojů. Komplexních nástrojů, které lze hodnotit jako LIMS, je jen velmi málo. Zvláště pokud chceme volit z pohledu dlouhodobé perspektivy, je třeba se držet splnění podmínek výběru:

- délky podpory
- pravidelné aktualizace
- možnost úprav modulů vlastními silami
- podpora mobilních zařízení
- oddělení práv administrátora od provozních dat
- bezpečnostní testy

Na základě studia dostupných LIMS, byl mezi testovaná prostředí přidaný CMS Plone postavený na programovacím jazyku Python. Nepatří mezi nejpoužívanější, ale svou podporu má a navíc je tento jazyk používaný statistickým software provozovaným v kampusu. Nabízí se myšlenka integrace vybraných výstupu dat ze systému přímo ke statistickému pracování.

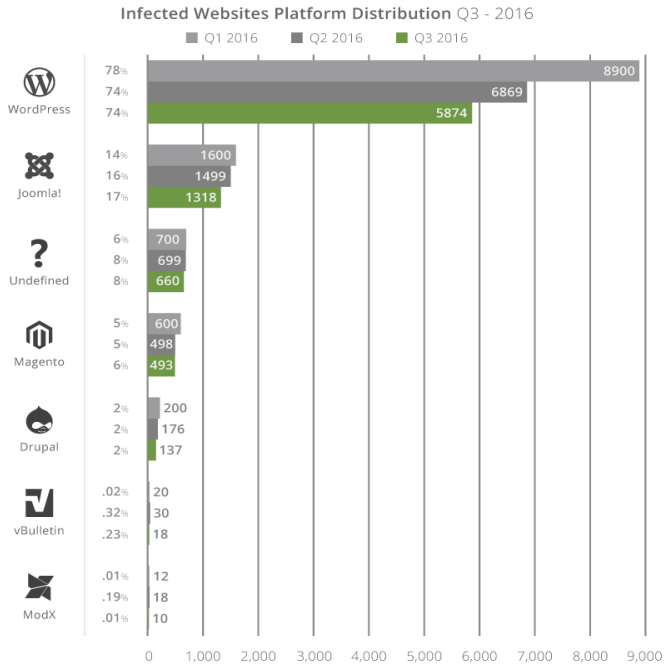
6.5 Bezpečnost CMS

Porovnání stavu bezpečnosti CMS a jejich vyhodnocení proběhlo na základě prostudování záznamů NVD (National Vulnerability Database), která je dostupná na stránkách (https://nvd.nist.gov/). NVD je vládou USA spravovaný na standardech založený depozitář dat o zranitelnostech. Souhrn provedený z kolekce dat je uvedený v tabulce č. 4.

	Joomla	WordPress	Drupal	Plone
Genealogy				
First release	Nov-22-05	May-27-03	Dec-31-04	Dec-31-02
Last release	Apr-05-16	Apr-12-16	Feb-08-16	Apr-07-16
Last rel.No.	3.5.1	4.4.2	8.1.0	5.0.4
Vulnerabilities				
Last 3 month	10	57	117	0
Last 3 years	81	654	504	40
All	811	1054	964	61

Tabulka č. 4 - Tabulka vyjadřuje v první části porovnání údajů o vývoji zvolených CMS, ve druhé sumární výpis zranitelností

Lze dohledat testy provedené jinými komerčními subjekty. Ze stránek SUCURI [I.29] lze stáhnout dokument s již vypracovaným hodnocením, jehož součástí je i grafické vyjádření stavu a rozložení napříč testovanými systémy. V tomto případě jde o CMS systémy WordPress, Joomla! a Magento. Z něj i pochází graf na obrázku č. 11.



Obrázek č. 11 – Graf s rozložením zranitelností testovaných CMS v Q3 2016, zdroj: [I.29]

Přes prvenství v celosvětovém nasazení má nejvyšší deklarovanou zranitelnost Wordpress, čím se jeví jako nejméně vhodným pro nasazení v informačním systému laboratoří. Stejný je verdikt i pro Drupal, který je na tom s bezpečností jen o málo lépe. Joomla patří mezi nejmladší ze systémů, avšak

úsilí jeho komunity jej vypracovalo na stabilní a v pojetí získaných výsledků, bezpečný systém. Nejlépe v testech vyšel Plone, který se jeví jako systém vyvíjený s důrazem na bezpečnost.

6.6 Test CMS

Test nasazení CMS proběhl na virtuálních strojích s operačním systémem MS Windows 2008, k nimž byly dostupné licence. Testovací HW byl sestaven ze serveru HP DL160 G6 v konfiguraci uvedené v tabulce č.5.

Systém VMWARE je nainstalovaný na flash kartě, úložný prostor pro servery byl dedikován na externím diskovém poli. Součástí testu byla instalace CMS dle dokumentace, ověření možností administrace, vytvoření jednoduchého webu a otestování jeho dostupnosti přes webové rozhraní v síti Intranetu.

Test byl proveden na posledních stabilních verzích CMS v souladu s dokumentací, s ověřením možností administrace, nasazením modulů, vytvořením jednoduchého webu a následným testováním dostupnosti z různých prohlížečů.

Wordpress nebyl v průběhu výběru adeptů na LIMS dobře ohodnocen kvůli množství deklarovaných útoků. Je třeba si ale dát do kontextu, že jde o nejrozšířenější systém, je pro něj nepřeberné množství doplňků, které mají na jeho bezpečnostní hodnocení bezprostřední vliv. Z toho důvodu je mnohem více napadaný hackery. Do testu byl zařazen kvůli velké oblibě a rozšířenosti. Ta je dána jednoduchostí implementace, administrace i údržby, kterou zvládne i průměrně zkušený uživatel. Plusem administrace je možnost volby z menu v režimu administrace systému, automatické aktualizace. Komunita kolem projektu je velká a snaží se eliminovat zjištěné zranitelnosti co nejdříve od jejich objevení. Seznam zranitelností je uveden na Internetových stránkách WPScan Vulnerability Database [I.30]. Na Internetu také existují online služby pro kontrolu webů založených na CMS WordPress [I.31]. Možnosti nasazení jsou, díky mnoha zdarma dostupným modulům, rozsáhlé. Své uplatnění najde coby redakční systém pro malé informační portály, které bez zásadních úprav nepožadují silné bezpečnostní prvky. Výchozí role based autorizace je pro náš případ nedostačující.

Server HP Proliant DL 160 G6

Položka	**Parametr**
Konfigurace HW	
Procesor (CPU)	2x Intel Xeon E5556@2.13 (8 core)
Operační paměť (RAM)	10GB
pevný disk (HDD)	4x 500GB
Síťový adaptér (NIC)	2x Intel NC362i (with VLANs support)
Aplikační vybavení	
Hypervisor	vSphere 5.5 Hypervisor
konfigurace virtualního serveru	
počet jader procesoru	2
dedikovaná operační paměť (RAM)	4GB
Pevný disk (HDD)	160GB (virtual disc)
Operační systém	MS Windows 2008 R2
Nainstalované aplikace	Avast! Business edt.; Visual Studio 2012 VC 11; WAMP pkg.(Apache 2.4.9; MySQL 5.6.17; PHP 5.5.12; PHPMyAdmin 4.1.14)

Tabulka č. 5 – Konfigurace testovacího serveru

Joomla je CMS založený na PHP a dle výsledků testů bezpečnější než Wordpress. Jeho instalace je snadná, ačkoli již není tak intuitivní jako v případě WordPressu. Nástroje administrace jsou dobře organizované, avšak pro provedení změn nastavení vzhledu a funkcí již pro průměrného uživatele znamenají nutnost prostudování manuálů nebo webů diskusních skupin. Z pohledu plánovaného nasazení LIMS tento nedostatek nehraje významnou roli, neboť se nepředpokládá, že by do systému zasahovala osoba nemající zkušenosti s programováním či administrací. V rámci průzkumu dostupnosti hotových aplikací byl nalezen modul J!Research 2.1.3. Jeho funkcí je pomoci organizovat činnosti spojené s vědeckým výzkumem. Před i po nahrání zmíněného modulu byla otestována dostupnost. Načtení úvodní stránky trvalo nejdéle z testovaných CMS.

Drupal měl dle NVD aktuálně více bezpečnostních problémů než uvádí SUCURi. Z pohledu robustnosti konstrukce je vhodnější pro větší webové projekty s vysokou frekvencí provozu a tedy i pro korporátní prostředí. Problém který pravděpodobně stojí za jeho nižší oblibou je složitost jeho administrace a méně srozumitelná dokumentace. Přesto patří do trojice nejčastěji srovnávaných Open

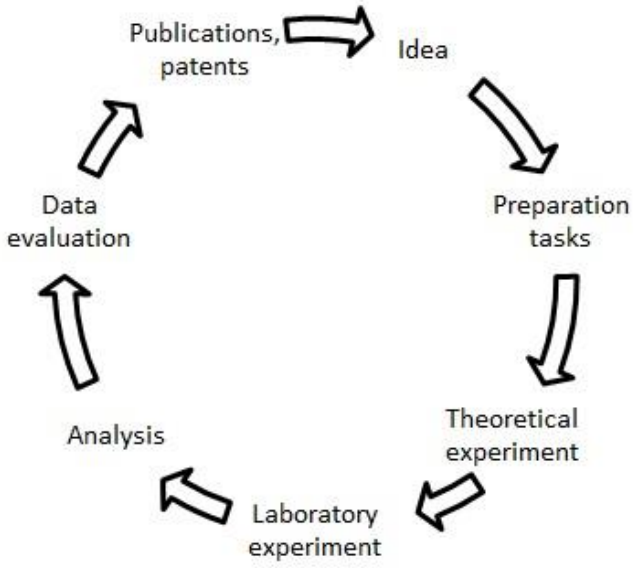
Source CMS řešení. Také pro něj existují online databáze a skenery zranitelnosti. V porovnání s WordPressem je množství bezplatných šablon, pluginů a motivů pro něj minimum. V rámci našeho testu, po instalaci, napojení na databázi a konfiguraci výchozího webu, bylo načtení první stránky velmi svižné.

Plone je robustní řešení postavené na aplikačním serveru ZOPE. Implementace byla ze všech testovaných CMS nejsložitější. Dokumentace je vcelku strohá a k dokončení instalace bylo třeba intenzivnější hledání potřebných informací ve fórech na Internetu. Jde o nejbezpečnější volně dostupný CMS systém, jehož konstrukce brání vzniku zranitelností vlivem špatné konfigurace. Vyhledávání relevantních informací o jeho zranitelnostech mimo stránky NVD a oficiální stránky je de facto nemožné. Přes uvedené existuje i pro něj nástroj na otestování. Post instalační načtení první stránky proběhlo nejsvižněji a to i po instalaci rozšiřujících modulů.

Z testovaných řešení založených na PHP se jeví vhodným Drupal díky snadné implementaci, rychlosti, s níž generoval stránky a množství doplňků. Systém Plone není snadné instalovat a obsluhovat, avšak má výborné reference v oblasti bezpečnosti. Není proto divu, že již v tomto prostředí existující LIMS implementace [I.20]. Většina zkoumaných CMS má v základu shodné funkce a mnoho šablon a pluginů. Vysoká bezpečnost Open Source aplikací je velmi těžko dosažitelná, neboť je kód volně k dispozici pro prozkoumání. Porovnávané systémy mají širokou podporu komunit, které je vyvíjejí a udržují i po stránce bezpečnostních záplat. S tím koreluje i udržení nízkého počtu neošetřených zranitelností. Na celkovém hodnocení je také podíl administrátorů, kteří mají systémy spravovat. Pokud jsou CMS postaveny tak, že je schopen je spustit kterýkoli uživatel bez hlubší znalosti problematiky provozu a úskalí, je pochopitelné, že nebudou nastaveny s ohledem na možná rizika a nebudou ani pravidelně a včas aktualizované. Profesionálně naprogramovaná aplikace (modul) pod správou podnikového administrátora by takovým rizikem být neměla.

7 LIMS - MODUL LABAPP

Modul je postaven na klasickém životním cyklu modifikovaném pro řešení problému, který je zobrazen na obrázku č. 2. Je v něm zachycený zrod myšlenky opřený o studium dokumentů, která nabývá teoretického rozměru vize nového řešení. Následně je v experimentálním prostředí realizována a výsledek analyzovaný. Data související s celým procesem jsou zpracována a následně publikována.



Obrázek č. 12 - Proces laboratorního experimentu, Zdroj: vlastní

Aplikace sama je pak fyzicky založena na rozšířeném obsahu laboratorního deníku převedeného do elektronické podoby. Je databázovou aplikací určenou pro laboratoře pracující na syntetizaci látek. V prostředí kampusu Hradec Králové se primárně jedná o dvě pracoviště, která mají srovnatelné pracovní postupy. V čase návrhu modulu bylo možné porovnávat jejich specifičnost a informační systém následně navrhnout tak, aby zohlednil požadavky obou stran. Snaha byla o vytvoření jednoduchého prostředí, do nějž nebude nutné vkládat nadbytečné bloky z pohledu libovolné strany. Práce proteomického týmu má v postupech odlišnosti [41], které nelze jednoduše do stávajícího modelu začlenit. Bylo tedy rozhodnuto, že se jejich modul bude řešit samostatně v případné další fázi.

Z reakce ze strany budoucích uživatelů bylo jasné, že chtějí vybudovat systém, kterému by se nemusely zásadně přizpůsobovat již zažité rutinní činnosti, a který by vyžadoval jen minimální, nejlépe žádné investice. Aplikace má za cíl pokrýt všechny fáze činností všech participujících týmů v laboratoři a přenést papírové a autonomní digitálně vedené záznamy do centrálního systému. V rámci průzkumu a následné analýzy navazujících činností byly nabídnuty uživatelům nové funkcionality, které mají návaznost na normy, a které mohou přispět k vyšší efektivnosti. Zmapování logických vazeb prostředí

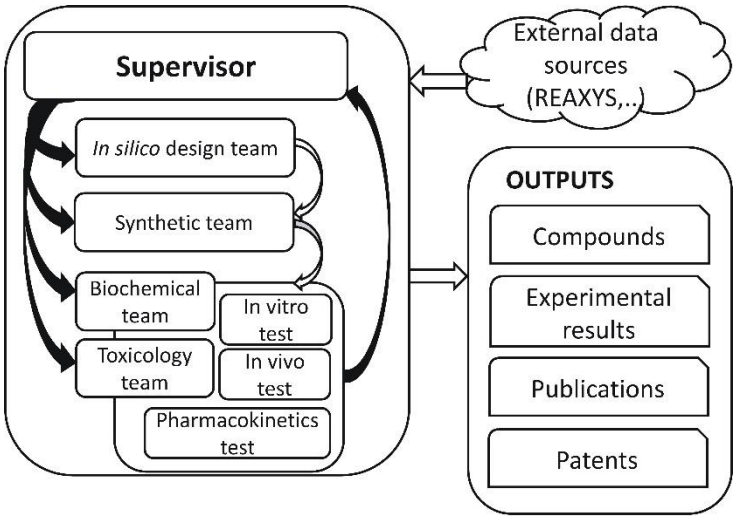
laboratoře se stalo základem návrhu budoucího informačního systému. Přihlédnuto bylo však též k požadavkům na bezpečnost, tedy zabezpečení dat před jejich zcizením, poškozením nebo ztrátou z důvodu chyby HW. Propojením na modul AuthApp, který přes grafické rozhraní DirecApp dovoluje kompetentní osobě definovat práva jednotlivých uživatelů podle role v organizaci, zjednodušuje Supervizorovi administraci systému při přidělování dílčích úkolů. Pro pochopení rolí je třeba uvést popis obsluhované struktury.

7.1 Organizační struktura

Na skladbu modulu LabApp má vliv soubor činností a workflow pracovních skupin, které má podporovat v rutinních činnostech. Pokud podrobíme rozkladu schéma z podkapitoly 4.1 podle na sebe navazujících činností, nalezneme pětici týmů, které v rámci úkolů úzce spolupracují. Výsledky činnosti jedné skupiny jsou vstupními položkami skupiny navazující. Výstup poslední z nich pak tvoří finální produkt. Neznamená to však, že finální výstup generuje vždy jedna konkrétní skupina. Vliv na úroveň výstupu může mít zadání experimentu i jeho úspěšnost.

Členy laboratorního teamu lze rozdělit do pěti skupin:

- Management – vedoucí osoby, které řídí činnost laboratoře a přidělují oprávnění a úlohy ke zpracování.
- *In silico* team – skupina počítačové chemie shromažďuje informace a data k přidělenému úkolu. Její členové vytváří modely molekul, studují jejich vazby. S pomocí počítačové simulace, modelují a analyzují chování a síly vzájemných vazeb. Výstupy slouží managementu k rozhodnutí, která sloučenina bude fyzicky syntetizována.
- Syntetický team – je skupinou, která se zabývá praktickým prováděním experimentů. Syntetizují látky dle dodaných teoretických podkladů a hledají metody pro nová řešení, zanášejí do laboratorních deníků informace o postupech a výsledcích.
- Biochemický, toxikologický a farmakokinetický team – skupiny, které nezávisle na sobě podrobí syntetizovaný vzorek základním testům *in vivo* a *in vitro*, případně i farmakokinetickým testům. Výsledkem je zjištění vlivu testované látky na živé organismy ve smyslu ověření biologického účinku, pro který byla látka navržena, její toxicita, případně i schopnost živých organismů odbourávat látku. V rámci experimentů doplňují do laboratorního deníku údaje o svých pozorováních.



Obrázek č.13 – Struktura a workflow laboratoře, zdroj: vlastní

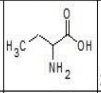
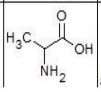
Jak je patrné z obrázku č. 13, je celý proces řízený skupinou managementu. Ta zadává úkoly všem týmům. První požadavek většinou směřuje na *In silico* team, k provedení teoretických testů. Příprava spočívá, mimo teoretické roviny, ve vytvoření lokální databázi ligandů a modelu biologických cílů. Získat data pro vlastní databázi není složité díky možnosti stáhnout různé molekulární sety (např. lead-like, fragment-like, drug-like) z velkých on-line databází léčiv. (např. zinc.docking.org). Aby data byla dále zpracovatelná v dokovacím programu, je třeba provést konverzi formátu a předběžné chemické kalkulace. Obdobně tomu je i u proteinů, jejichž struktury lze získat v on-line databázích (např. www.pdb.org) již připravené pro dokování molekul. Konfigurační soubor pak obsahuje údaje, které definují parametry běhu modelovacího programu (např. AutoDock Vina). Ke zpracování je pak třeba dostatečný výpočetní výkon, který je schopné nabídnout prostředí dedikované v cloudu [37], [43]. Výstupem z výše uvedené procedury jsou potenciální biologické a fyzikální vlastnosti zkoumaných látek. Tým k vytvoření modelu využije buď údaje uložené ve vlastní databázi, nebo z externího zdroje. Modelováním chemických struktur získá team soubor možných látek, které vyhovují zadání. Jejich selekcí pak dostane vzorec jedné či více teoreticky významně zajímavých látek, kterou předá k posouzení Supervizorovi. Na jeho rozhodnutí pak závisí další postup, například zdali a která z látek bude syntetizována. Její vzorec s doprovodnými poznámkami pak přidělí konkrétní osobě v teamu syntetiků. Po jejím vyhotovení se látka cestou Supervizora předává k hodnocení biologických aktivit a následně toxikologických vlastností. Zde opět dojde cestou Supervizora k přidělení testované látky osobě, která za příslušný test odpovídá, látku otestuje a zpracuje požadované reporty. Pokud je experiment celkově úspěšný, následují farmakokinetické testy, v nichž se testuje schopnost živého organismu potenciální léčivo udržet a vyloučit.

7.2 Funkční návrh

Nyní se na stejnou proceduru podívejme z úhlu návrhu systému. Jak již bylo zmíněno, data jsou od *In silico* teamu předávána ve tvaru chemický vzorec a poznámky, tedy metadata (obrázek č. 14). Právě tento tým se nejvíce podílí na vzniku metadat, konkrétně vkládání odkazů na vnější informační zdroje. Tyto pak mohou mít vazbu na více než jeden experiment, proto bylo rozhodnuto o provázání modulu LabApp a LibrarApp vazbou N:M. Informace, získané z externích zdrojů, o chemických vlastnostech a postupech jsou ukládané do systému digitální knihovny LibrarApp. Odkazy na ně jsou pak ukládány do databáze LabApp s možností vytvoření vlastních poznámek ke konkrétnímu experimentu, tedy 1:N, která se zde ukládají do tabulky metadat s příznakem daného experimentu. Společně s nimi se automaticky zde uloží identifikátor osoby, která je do systému vložila společně s časovou značkou. Ta definuje relevanci pro případ konfliktu s daty v následných ověřujících experimentech. Takto připravený záznam pak usnadňuje zpracování zdrojů citací do reportů, vědeckých článků nebo pro patentové řízení. (Obrázek č. 15)

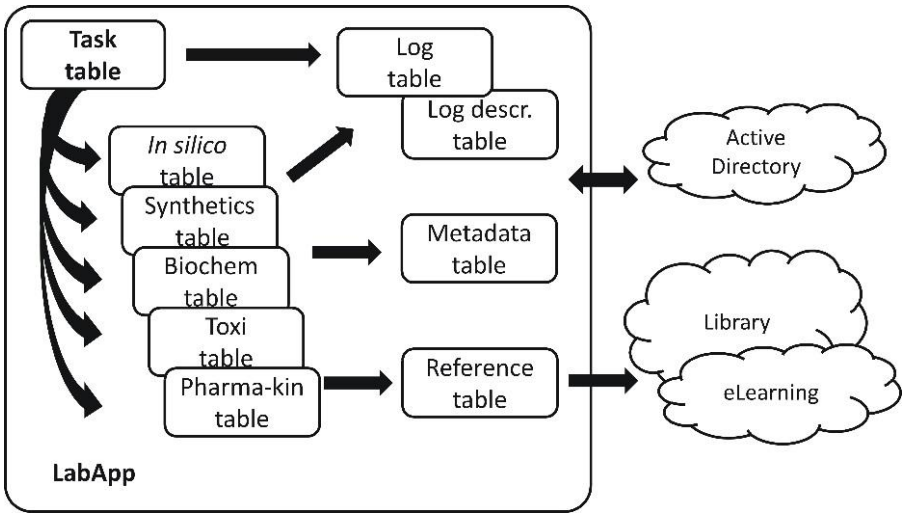
Neznamená to však, že by ostatní osoby neměly shodné oprávnění. Vkládat odkazy na dokumenty z LibrarApp a komentovat je může každý, kdo se na přiděleném úkolu podílí. Jen pro pochopení logiky systému je třeba dodat, že do systému LibrarApp může vkládat Dokumenty každá osoba, která má právo přístupu do LIMS, tedy má vytvořený uživatelský účet.

Organic synthesis table

Pkey	Code1	Barcode	K-code	Structure [file]	Chemical name	Reference	Storage location	Amount [g]	Mol. Weight [g/mol]	Solubility	Exp. elem. analysis	Melting point [°C]
562	120566	120566	k25		2-aminobutyric acid							
563	100012	100012	k01		alanine							

Obrázek č. 14 – Příklad tabulky organické syntézy, zdroj: vlastní

Mimo výše popsanou funkcionalitu byl systém doplněn o sub-modul sledování uložení zhotovených látek, neboť každý finální produkt je jinak stabilní a může vyžadovat pro bezpečné uložení jiné klimatické podmínky. Po ukončení přípravy sloučeniny či zpracování, odpovědná osoba doplní v databázi místo a množství ukládané látky. I zde se automaticky uloží „user ID“ a „časová značka“ pro případ řešení nesrovnalostí.



Obrázek č. 15 – Návaznost workflow LabApp na další moduly, zdroj: vlastní

7.3 Databázové prostředí

Vytvořit pro daný účel jednoduchou databázi, která by zahrnovala výše popsaný postup je vcelku snadný úkol. Dá se vyřešit na stolním počítači například pomocí aplikace MS Access z nástrojů kancelářského balíku MS Office a ošetřit integrovaným grafickým rozhraním. Ze zadání však vyplynulo hned několik požadavků, které tuto možnost popírají:

- Předpoklad zpětné digitalizace záznamů z laboratorních knih
- Paralelní zpracovávání dat a přístupy do databáze
- Zabezpečení dat na všech úrovních zpracování
- Integrace s ostatními částmi LIMS (AuthApp, LibrarApp, EduApp)
- Dostupnost z různých zařízení (PC, notebooky, tablety, mobilní telefony))
- Jednotné rozhraní
- Možnost vyhledávání v uložených datech dle zvolených parametrů

Najít objektivní porovnání DB prostředí není snadné. V mnoha ohledech jsou informace zkreslené neochotou vývojářů připustit, že obcházení absence funkcí, které v jiných systémech jsou přítomny, je opravdu obcházením [I.32]. Naše vlastní zkušenosti z realizace a údržby jiných projektů a s tím provedené testy na různých typech HW způsobily, že do užšího okruhu se dostaly MySQL, PostgreSQL, Oracle a MS SQL. Poslední dva jmenované produkty v komerční, tedy placené, verzi byly vy-

loučeny hned na začátku. Funkcionalita jejich LITE verzí je vesměs pro navrhovaný systém nepoužitelná. Množství záznamů a současných přístupů by mohli v rozvíjejícím se prostředí brzo uživatele limitovat.

MySQL 5.5.4.2

ORACLE vlastě úplně z výběru nevypadl, neboť MySQL patří do jeho portfolia. Jde o velmi oblíbený open source relační databázový systém, který získal akvizicí. Z oficiálních stránek produktu lze vyčíst, že za dobu jeho existence, bylo staženo více než 100 milionů kopií. MySQL je často využívána na webových serverech pro potřeby webových aplikací. V kombinaci Linux, PHP a Apache tvoří oblíbený zaklaní web serverový balíček, známý pod zkratku LAMP. Tuto multiplatformní databázi lze získat výběrem buď podle verze, anebo dle licenčního modelu. Základní verze, MySQL Community Server, je zdarma distribuovaná pod licencí GNU. Ostatní verze jsou komerční, tedy placené. Parametry jsou závislé na verzi a typu použitého úložného místa.

PostgreSQL 9.3.4

Jedná se o objektově-relační databázový systém, šířený pod licencí MIT. Je tedy zdarma a jako bonus jsou k dispozici i jeho otevřené zdrojové kódy. Jde o multiplatformní databázový systém, použitelný pod systémy Linux, UNIX i Windows. Podporuje transakční zpracování dotazů i kontrolu cizích klíčů. Je tedy plně ACID kompatibilní a automaticky zaručuje konzistenci dat v databázi. Jsou zde také implementovány vnořené transakce.

Naší volbou byla MySQL, se kterou již máme zkušenosti z jiných, převážně webových, aplikací, ačkoli z některých zátěžových testů vyplývá, že při větší zátěži by lepší výkon podala PostgreSQL. MySQL nabízí širokou škálu úložných míst. Námi vybraný InnoDB splňuje požadavky na podporu požadovaných vlastností systému (např. transakce, zamykání řádků, cizí klíč,…) Dále nás zaujala podpora Cloudu, které je základem i naší implementace.

7.4 Datová bezpečnost

Zabezpečení informací uložených v datech můžeme vnímat v několika rovinách. Vždy však jde o ochranu investic, duševní práce společnosti a v případě laboratorních výzkumů o ochranu před zneužitím informací. Při tvorbě LabApp byl hlavní důraz kladen na zabezpečení dat, aby se bezpečnostní rizika eliminovala na minimum.

- Autentizace uživatele (AuthApp)
- Přístup do LIMS založený na rolích a funkcích pracovníků v IS
- Šifrované přenosy dat
- Uložiště dat (šifrovaný veřejný či privátní cloud)
- Fyzické zabezpečení na všech úrovních
- Zálohování

Bezpečnostní modul AuthApp je jedna z hlavních součástí LIMS [V.4], jenž sdružuje uživatelské účty všech osob v centrální databázi UserDB. Jeho centrem může být MS Windows Server v roli doménového řadiče, nebo jakýkoli LDAP server. V rámci výstavby LIMS byl integrován do jeho struktury. Jednotlivé moduly, mezi nimi i LabApp, využívají ověřování uživatelských účtů v UserDB. Jako rozšíření funkcionality dostupnosti jednotného přihlášení lze zvážit nasazení služby, která umožní i ověření externích spolupracovníků proti jejich firemním databázím uživatelských účtů (např. Shiboleth). Je však třeba přihlédnout k výslednému počtu takových osob, aby bylo vynaložené úsilí a prostředky efektivní.

Z důvodu nebezpečí úniku informací např. konkurenční skupině, bylo třeba tyto důsledně zabezpečit. Z rozboru informačního toku a sledovaných údajů bylo zjištěno, že dílčí data (chemický vzorec, teplota tání, teplota varu, rozpustnost,…) samy o sobě nedávají žádnou relevantní informaci o biologické aktivitě testované látky. Analogicky nelze z dat popisujících biologickou aktivitu *in vitro* či *in vivo* získat zpět chemický vzorec látky. Proto navržený model pro aplikační rozhraní nedovolí zobrazení celé skupiny dat nikomu jinému než roli Supervizor. Z toho vyplývá následující logika předávání dat v rámci úkolu.

Pověřená osoba *In silico* teamu připraví výše popsaným způsobem podklady pro Syntetický team. Vzorce a související informace jsou uloženy v databázi LabApp. Datové řádky se odevzdáním Supervizorovi pro všechny označí jen pro čtení a vyjma jeho všem skryjí. Supervizor se rozhodne, která z připravených dat se budou fyzicky realizovat a tyto přidělí pod kódem daného úkolu konkrétnímu laborantovi v teamu syntézy. Ten ze svého uživatelského rozhraní zjistí kód úkolu a s ním související zadání. Data o průběhu syntézy laborant zaznamenává do polí v rozhraní systému, která souvisí se zadáním a která jsou mu jediná viditelná. Po splnění úkolu je nádobka s připravenou látkou a s nalepeným identickým kódem předána Supervizorovi. Ten z ní odstraní nalepený kód, předá úkol k provedení testů osobě z biochemického týmu, čímž se v systému vygeneruje nový kód. Nádobku jím označí a předá ji i fyzicky. Data zadaná do systému syntetiky jsou označena jen ke čtení a viditelná jen supervizorovi. Pole související s novým úkolem se společně objeví v systému osoby, která další část úkolu obdržela. Tento postup se opakuje pro všechny následující testy. Mělo by tak být zabezpečeno, že nikdo nebude schopen získat kompletní data k dané látce mimo systém.

8 NÁVRH HARDWAROVÉHO BEZPEČNOSTNÍHO MODULU LIMS

V návrhu zabezpečeného LIMS [44], [45], [V.5] se pracuje s aplikačními moduly, které postihují potřeby pracovníků laboratoře v různých fázích provádění experimentu. Vychází z prostředí s centrální autoritou pro ověření vstupu uživatele do systému, databází, v níž se ukládají data a metadata k chystaným a prováděným experimentům a také aplikační vrstvou, která upravuje dle přiznaných oprávnění množství zobrazených informací.

Následující rozšíření navazuje na uvedené moduly a technicky rozšiřuje zabezpečení manipulace se vzorky chemikálií a biologických materiálů coby zdroji citlivých dat. LIMS se tak stává systémem nejen s funkcemi pro management laboratoře a místem pro uložení dále zpracovávaných dat, ale také systémem pro audit událostí na fyzické i datové úrovni.

Centrem navrhovaného řešení je AuthApp – centrální autentifikační modul, který obsluhuje seznam všech oprávněných osob z UserDB. Jejím základem může být jak LDAP databáze Linuxu tak Active Directory systémů Microsoft Windows. Důležité je, aby bylo možné data uživatelských účtů svázat s provozovanými identifikačními kódy např. RFID tokenů, které slouží pro identifikaci osob na daném pracovišti. AuthApp se tak stává opravdovou centrální autoritou pro ověření oprávněnosti osob při vstupu do objektu a v něm definovaných prostorů, stejně tak pro jejich přihlášení do informačního systému LIMS s vymezenými oprávněními.

Navazujícím modulem je Databáze auditu událostí AUDITDB. V ní se shromažďují informace o výskytu událostí jak z dohledového systému, tak i z činností v LIMS. Uložená data lze filtrovat, analyzovat a vyhodnocovat. Bez problému můžeme vysledovat četnost neoprávněných pokusů o vniknutí do systému či prostor nebo naopak přístup k datům a pohyb osob podezřelých z vynesení citlivých údajů či materiálu.

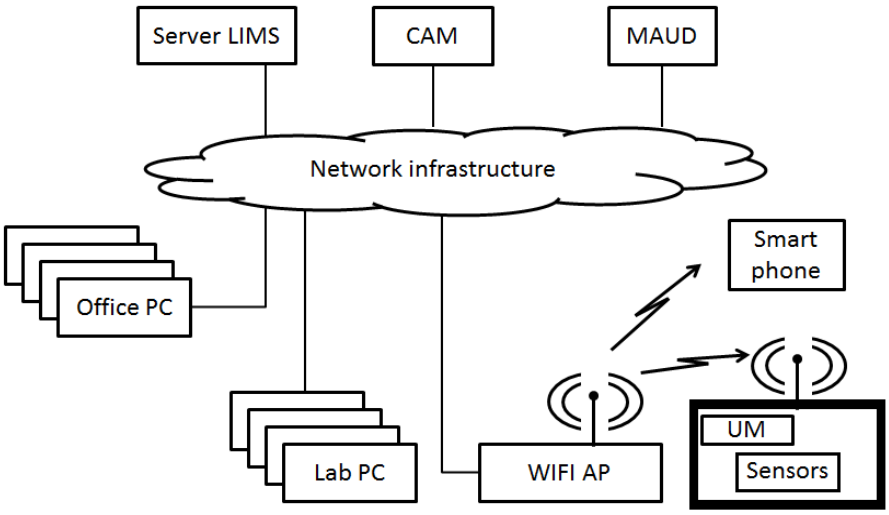
Napojení na oba uvedené moduly tak může mít nejen LIMS a systém evidence vstupu na pracoviště. Do uvedené sestavy lze integrovat další zařízení, která souvisejí s činnostmi v laboratoři a jejichž výstupy ovlivňují nebo bezprostředně navazují na data LIMS a bezpečnostní audit.

Moderní systém je chápán již ne jako pomocník lidí, ale jako inteligence, jíž operátoři předkládají data a zpět dostávají informace, které mohou využít v rozhodování. Aby měl takový systém požadované úplné údaje, je třeba laboratoře dovybavit SMART technologiemi. Mohou rozšířit možnosti zabezpečení a zároveň poskytnout potřebné údaje pro management či logistiku. Principem se jedná o

implementaci zařízení Internet of Thinks (IoT). Mimo systémů pro řízení chodu domácností se dominantně jedná o průmyslové aplikace, které mohou být nasazené i v prostředí laboratoří. Všeobecně lze říci, že aplikační vrstva nad IoT zabezpečuje chod svázané entity v místě, kde jsou její HW prvky integrovány. V našem případě by se v jistých případech v součinnosti s AUTHAPP dalo rozšířit funkci do role bezpečnostního prvků a jako zdroje auditu událostí. Pokud zůstaneme u příkladu s omezením přístupu k biologicky aktivním látkám a jejich evidenci, mohou být tato zařízení jednoduše integrována například do lacinějších modelů skříní a lednic společně s elektronickými zámky a čidly.

Miniaturizace elektronických čipů, integrace různých funkcí do jednoho pouzdra a nízká cena jsou faktory, které umožnily fenoménu IoT expandovat do širokého portfolia služeb a průmyslových odvětví. Je tedy nasnadě, že najdou své uplatnění i v laboratořích různého zaměření. Zde se mimo vybavení laboratorními přístroji a počítači určenými ke zpracování a vyhodnocování výsledků badatelské činnosti setkáme s dalšími systémy, bez nichž by byl provoz nereálný. Mnoho těchto autonomních systémů vyhodnocuje online data z primitivních rozhraní a některé je i na definovaný čas ukládají. Fyzické oddělení a datová nesourodost nedovolují jednoduché a rychlé vyhodnocení viděné v patřičných souvislostech. Jako žádoucí se proto jeví systémy vzájemně propojit. Modularita a široká škála funkcí IoT zařízení přímo vybízí k nahrazení morálně zastaralého vybavení. Ekonomickou podmínkou je prokazatelné navýšení užitné hodnoty a usnadnění rutinních činností. Za naplněním těchto požadavků stojí i intuitivnost ovládání sofistikovaného systému, tedy, aby jeho rozhraní bylo pro obsluhu snadno a rychle zvládnutelné.

Pro funkci zabezpečení se zásadní jeví autentizace osoby v různých oblastech přístupu. Jako řešení lze využít modul, který je dále v textu označený jako univerzální (UM). Jeho doplněním o různé periferie dosáhneme zabezpečení potřebných funkcí, které mohou mít příznak osoby, která je s ním interakci. Tím se UM podílí na auditu událostí laboratoře. Ať jej použijeme na vstupních dveřích do objektu či režimové sekce laboratoře, anebo na dveře skříně se sledovaným materiálem, vždy nám bude generovat informace o použití identifikační karty, kterou ověří uživatele vůči databázi UserDB a dle individuálního nastavení pak provede požadovanou operaci. Deklasovat počítač na službu vrátného by bylo mrháním peněz. Existují levnější komerčně vyráběné moduly, které k tomuto účelu plně postačují. Pokud ale k UM připojíme mimo RFID čtečky ovládání zámku, snímač kontaktu dveří a teplotní čidlo, které bude snímat vnitřní teplotu zabezpečeného prostoru, jsme již schopni mnohem vyšší variabilnosti výstupu. Na obrázku č. 16 je znázorněno začlenění UM do LIMS ve variantě modulu ověřování přístupu (CAM), v dále popsaném případě jde o lednici.



Obrázek č. 16 – Zapojení UM do sítě laboratoře, zdroj: vlastní

Primárním úkolem CAM je na základě načteného kódu z ID karty ověřit jejího držitele vůči databázi osob v UserDB a definovanému seznamu oprávnění LIMS a následně povolit či odmítnout přístup k obsahu lednice. CAM je pak schopen do databáze auditu AUDITDB poskytnout informaci nejen o úspěšném či neúspěšném pokusu o otevření lednice, ale také časový údaj o době, po kterou byla otevřena a rozdíl teplot mezi okamžiky otevření a uzavření dveří. Na základě interakce s obsluhou též, se kterými látkami bylo manipulováno, případně kolik roztoku bylo z které nádoby odebráno.

Interakcí s uživatelem rozumějme nenáročný postup, který ho nezatíží časovou náročností a nadbytečnou manipulací nad rámec běžné praxe, což vyžaduje splnění jistých vstupních podmínek. Pro usnadnění identifikace obsahu lednice bylo třeba ustanovit jistá pravidla. Prostor byl rozdělen do logických zón, které jsou vymezeny regály. V dále popisovaném příkladu jsou tři.

První zónu tvoří zkumavky se vzorky spojenými s výsledky experimentů. Tyto jsou polepeny čárovým kódem generovaným v logistickém modulu LIMS a umístěny do stojanu.

V druhé zóně se nacházejí provozní zásoby látek potřebných pro chod laboratoře. Jedná se o nádoby definovaného tvaru a materiálu, které mají pevné víčko, na němž je nalepený čárový kód nebo RFID čip.

Třetí zónu pak tvoří dočasný odkládací prostor. Zde se nachází materiál, který nemá identifikační štítky a je organizován dle dohody o přidělení prostoru.

Sjednotit technologii a použít RFID nálepky i v první zóně by neúměrně prodražovalo experimenty. Z toho důvodu je nutné mít k dispozici nejen RFID čtečku, ale též i čtečku čárového kódu. Obojí je svázáno s UM a navíc doplněno o display, na němž se zobrazují informace a pokyny pro uživatele.

Funkce je vyjádřena v následujícím popisu logických kroků. Po úspěšném ověření oprávněné osoby RFID tokenu je uvolněn na 5 sec zámek dveří. V té době je třeba dveře otevřít. Posunem dveří se oddálí snímač zavřených dveří a zaznamenává se čas. Pokud jsou přinášeny nebo odnášeny nějaké nádoby, je třeba je identifikovat a to buď přiložením ke čtečce RFID kódů nebo čárových kódů. Při načtení dané nádoby je třeba potvrdit směr přesunu, tedy zdali je odnášena nebo přinášena, přičemž při jejím vracení je třeba vyjádřit její stav, spotřebované množství nebo doplnění. Pokud se zvýší teplota v prostoru chladícího zařízení nad kritickou mez, je spuštěn varovný signál. Stejně je tomu v případě, že doba otevření dveří překročí definovaný čas.

V prostředí LIMS lze sledovat a vyhodnocovat různé údaje. Z výše uvedených informaci lze mít představu o průběhu činností v laboratoři, vědět o pohybu materiálu, předpokládat jeho spotřebu a na deklarovaný stav reagovat včasným nákupem.

Aby nedošlo ke zničení uložených vzorků, lze monitorovat vnitřní teplotu chladícího zařízení i při zavřených dveřích a odhalit výpadek napájení či poruchu kompresoru.

U chladicích boxů, kde teplota neklesá pod bod mrazu, se jeví jako efektivní monitorování obsahu polic resp. obsazení pozic nádobami v polici. Pod danou pozicí je umístěno váhové čidlo, které mimo obsazení může hlídat i hmotnost uložené nádoby. Jinou variantou pak je optické sledování prostoru police, kdy snímaný obraz je rozčleněný na sektory. Barevnými víčky nádob jsou označeny obsazené pozice, zatímco neobsazené jsou buď bílé anebo definované jinou barvou.

Mrazicí boxy, kde se teplota pohybuje mezi -70 a -18 °C, nedovolí použití běžně dostupných polovodičových a pasivních součástek neboť se rozmezí jejich pracovních teplot na dolní hranici liší.

8.1 Návrh technické realizace

S rozmachem miniaturizace počítačových komponent a tedy i počítačů takových, je dnes k dispozici několik platforem, které se prosazují a soupeří o obsazení trhu. Jde o souboj jak HW, tak SW platforem. K našemu byly použity nejvíce používané komponenty platforem Raspberry Pi a Arduino. Za nejvhodnějšího kandidáta byl vybrán mikropočítač Raspberry Pi 3 s operačním systémem Raspbian,

který nabízí dostatečný výkon a má v sobě již integrované WIFI rozhraní pro komunikaci s ostatními moduly a databázemi LIMS. Modularita činí prostředí vhodné pro experimentování s různými variantami zapojení i kombinace funkcí, stačí zvolit vhodné komponenty. Příkladem může být, že dostupnými moduly lze obsáhnout všechny běžné varianty RFID frekvencí, což potvrzuje tabulka č. 6. Pro otestování lze využít libovolnou variantu. V souladu s podkapitolou 5.4 je však třeba počítat, že pro reálný provoz bude třeba počítat s variantou, která bude splňovat požadavky na kapacitu uživatelské paměti pro uložení přístupového klíče. Momentálně se jeví, na základě nabídky trhu, jeví jako vhodný modul TRF7960 pracující na frekvenci 13,56 MHz.

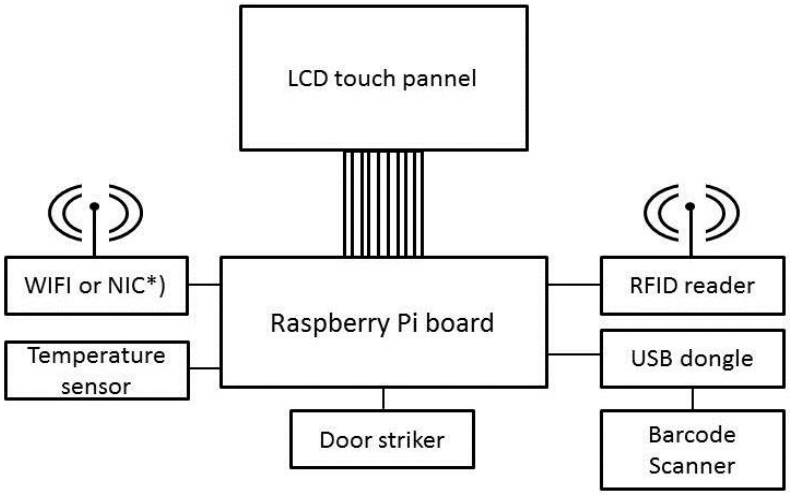
Modul	**Pásmo**	**Frekvence**
RDM6300	Low frequency (LF)	125 – 134 kHz
TRF7960	High frequency (HF)	13.56 MHz
LSID-0702	Ultra-high frequency (UHF)	433, and 860-960 MHz

Tabulka č. 6 – Příklady modulů pro běžné frekvence

Pro sledování přístupu oprávněných osob s čipovými náramky do lednice a kontroly teploty v lednici byl navržen modul, jenž se skládá z následujících komponent:

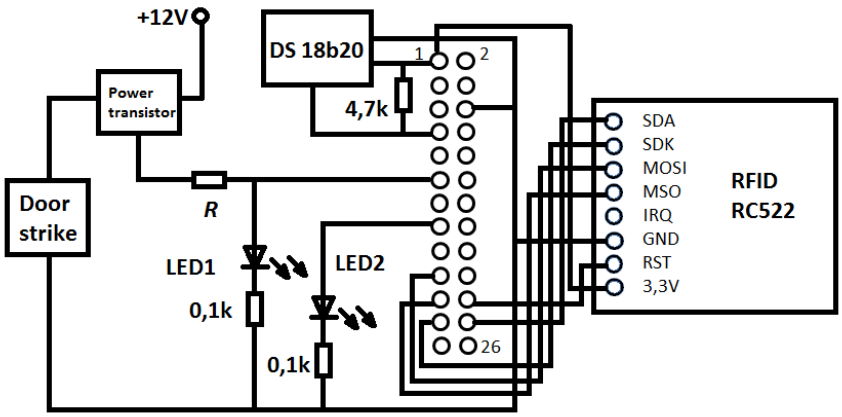
Raspberry Pi 3 základní deska
USB flash disk 16GB
RFID čtečka TRF7960
Čtečka čárového kódu
12V Elektrický dveřní zámek
5V 2A Napájecí zdroj elektronické části
12V 1A Napájecí zdroj elektrického zámku
LED dioda pro indikaci stavu zámku
Digitální teplotní sensor DS18B20
7" dotykový display 4DPi R-2.0

Na obrázku č. 17 je blokově znázorněno zapojení komponent. K desce Raspberry Pi je jsou připojeny všechny potřebné komponenty. Komunikační NIC a WIFI jsou uvedeny jako modul, ale ve skutečnosti jsou integrované na desce počítače. Čtečka čárového kódu je zařízení komunikující přes sériový port, který je zde modulem USB2SERIAL. LCD dotykový display je zapojený na konektor DSI.



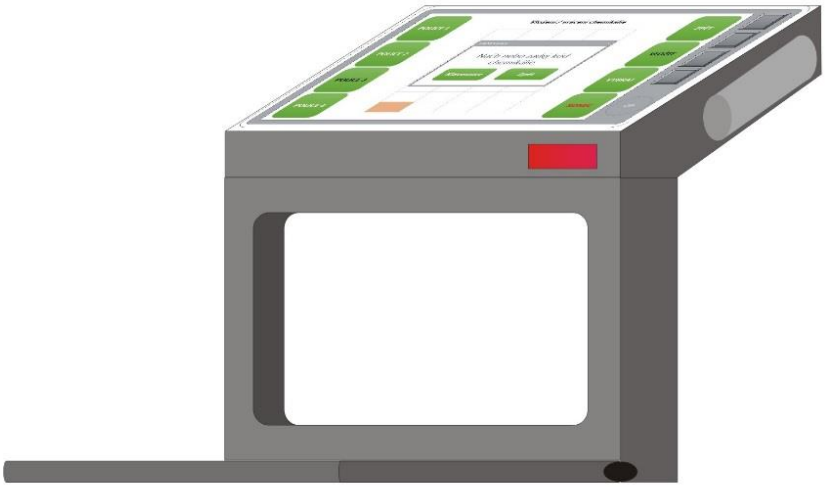
Obrázek č. 17 – Blokové schéma modulu UM s periferiemi, zdroj: vlastní

Detail napojení periferií na port GPIO je znázorněno na obrázku 18. Je zde vidět napojení digitálního teplotního 1-wire sensoru, čtečky RFID i dvou LED diod. LED1 je spřažená s bází výkonného transistoru a indikuje akceptaci požadavku otevření dveří, kdežto LED2 indikuje odmítnutí požadavku. V reálu se může jednat o jednu optoelektronickou součástku se zapouzdřením LED diod dvou barev. Do obvodu výkonového transistoru je zapojený Elektrický dveřní zámek, který uvolňuje západku dveří.



Obrázek č. 18 – Schéma zapojení pinů modulu pro ovládání elektrického zámku, zdroj: vlastní

Zařízení je tvořeno rámem jednotky, který se připevní na stěnu skříně společně s elektronickým zámkem. Horní část tvoří 7“ dotykový display, v jehož rovině se ve společném rámu vpravo nachází RFID čtečka. V přední hraně pod displejem je integrovaná čtečka čárového kódu, přičemž i tato může být nahrazena jinou s možností číst např. QR kódy. Spodní část modulu pak tvoří výklopná deska s integrovanou váhou, která může být osazena i jiným systémem pro měření množství skladovaných látek. Z důvodu možného nasazení v prostoru, který může pro manipulaci s nebezpečnými látkami vyžadovat použití rukavic, je na boku připevněný a snadno vyjmutelný stylus pro ovládání dotykového panelu (obrázek č. 19).

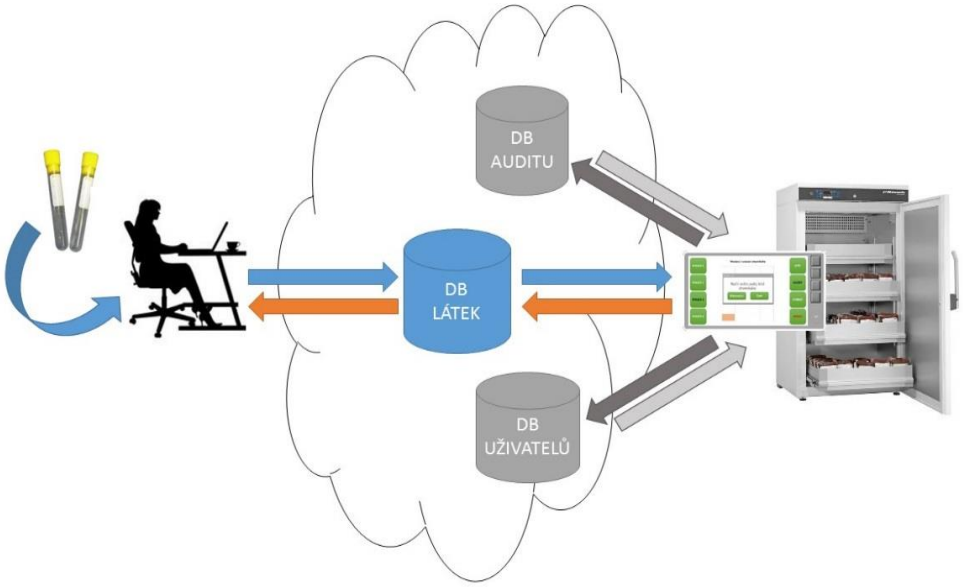


Obrázek č. 19 - Návrh designu modulu v poloze s vyklopenou váhou, zdroj: vlastní

Úprava samotné lednice spočívá v tom, že je pláštěm lednice zavedeno do vnitřního prostoru čidlo pro snímání teploty, na dveře připevněn elektronikou ovládaný zámek a na tělo lednice se připojí blok výkonné jednotky s displejem a tlačítky. Celek je do informačního systému připojený buď ethernetovým kabelem nebo prostřednictvím WIFI sítě. Rozhodnutí je závislé na místních podmínkách, tedy na dostupnosti a počtu volných datových zásuvek v místnosti nebo dostupnosti bezdrátové sítě. K napájení lze využít buď elektrickou zásuvku, nebo provést úpravy v rozvodu lednice a z něj napájení modulu řešit napřímo.

8.2 Napojení na LIMS

Jak je znázorněno na obrázku č. 20, programové vybavení Modulu je integrované do Laboratorního informačního systému. Zde je připojen k databázi uživatelů, kde jsou definovaná jejich oprávnění a na základě nich řídí přístup do střežené skříně. Druhý spoj je s databází auditu, do níž zapisuje informace o úspěšných i neúspěšných pokusech o přihlášení a odhlášení pracovníků. Primární spoj vede do databáze látek uložených na pracovišti, v níž je definováno, kde se daná látka nachází, tedy do místa v dané skříni včetně. Dotazy definovanými interakcí s uživatelem získává informace, které zobrazuje na dotykovém panelu, anebo provádí předdefinovanou akci. Přístup k datům databáze je aktivní, tedy nazpět ukládá aktualizované informace o doplňování a spotřebě materiálu. Obsah databáze ve smyslu zadávání látek a jejího umístění ve sledovaných skříních je editován z pracovní stanice logistického pracoviště.



Obrázek č. 20 - Návaznost modulu na LIMS, zdroj: vlastní

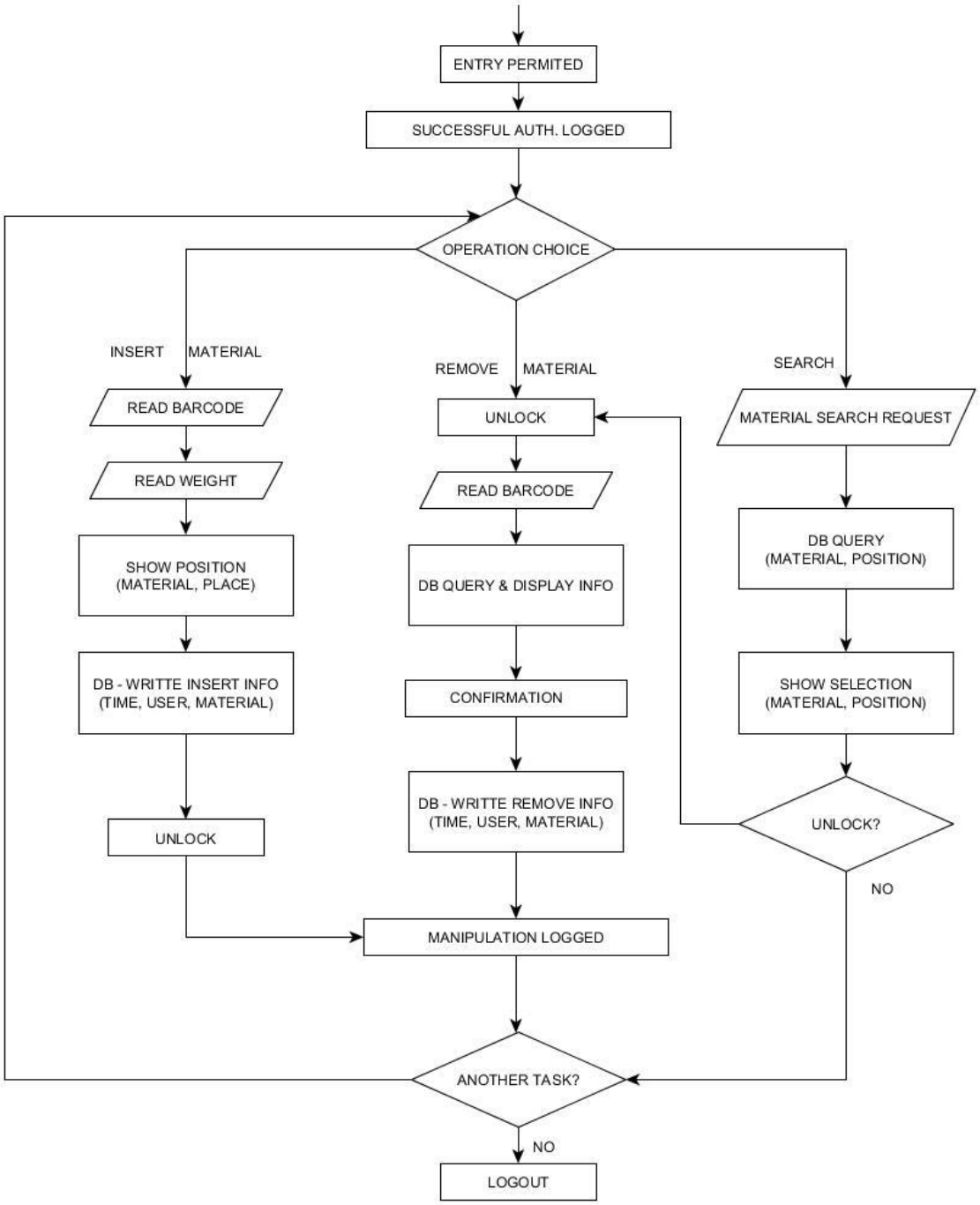
V kontextu různých procesů v laboratoři, je možné vidět možná další rozšíření modulu a propojení o další technologie. Výše popsané nasazení vychází z ideálního modelu, který neobsahuje detailnější popisy pohybu materiálu a aspekty, které mohou popsané postupy v určitých situacích eliminovat. Častý problém je, že vzorky a látky, s nimiž se v laboratořích manipuluje, se smí otevírat jen v chráněné oblasti laboratorní digestoře. Důvodem jsou různé fyzikální vlastnosti nebo toxicita. Aby nedocházelo k nechtěné evaporaci v průběhu skladování, jsou přechody víček dózy zabezpečeny ovinutím speciální páskou, parafilmem, který je dokonale utěsní. Dle zručnosti laboranta je množství použitého parafilmu různé, tedy i výsledná hmotnost ukládané nádoby se změní nejen vlivem spotřeby či

doplnění obsahu. Ve vybraných případech se zpracovávají jen velmi malá množství, vážená s velmi nízkou tolerancí. Hmotnost spotřebované látky může být několik miligramů. Z laboratorní praxe je známé, že ke zkreslení údajů stačí, aby na dóze ulpěl pot z prstů rukou laboranta nebo byl na dózu doplněn popis lihovým fixem. Po ochraně zdraví operátora je toto hned dalším důvodem, proč se manipulace s látkou odehrává v rukavicích. Použití parafilmu na dokonalé utěsnění dózy s sebou nese variabilitu její délky, což také znamená variabilitu hmotnosti. Výsledkem může být mylné vyhodnocení hmotnosti ukládaného celku jako vyšší spotřeba, než byla reálně anebo doplnění látky.

Než kombinovat vážení ukládané dózy s váhou kotoučku parafilmu před a po odmotání množství potřebného k hermetizaci, provádět výpočty a po té je ukládat, je snazší a již v běžné praxi prováděné, vážení v digestoři ještě před jejím uzavřením. K tomu je třeba systém modifikovat jak po HW tak SW stránce. Systém čtečky kódu a váhy bude třeba osadit do digestoře a napojit je na modul CAM. Laborant po zvážení vracené dózy provede její hermetizaci, dojde k lednici, identifikuje sebe a ukládanou dózu a materiál uloží. Systémem lze sledovat a omezit tolerovaný interval procesu od zvážení po vložení do lednice a definovat jej obsluze.

8.3 Návrh grafického uživatelského rozhraní

Navrhované grafické rozhraní Modulu musí být maximálně jednoduché, intuitivní. Činnost obsluhy nesmí nijak omezovat a nevyžadovat nadbytečné úkony [44]. Návrh rozložení prvků jednotlivých obrazovek vychází z blokového diagramu (Obrázek č. 21), který popisuje základní funkce ovládání panelu, tedy přihlášení a odhlášení uživatele k Modulu, zjištění stavu a místa uloženého materiálu, možnost jeho vyzvednutí a uložení nazpět na správnou pozici.



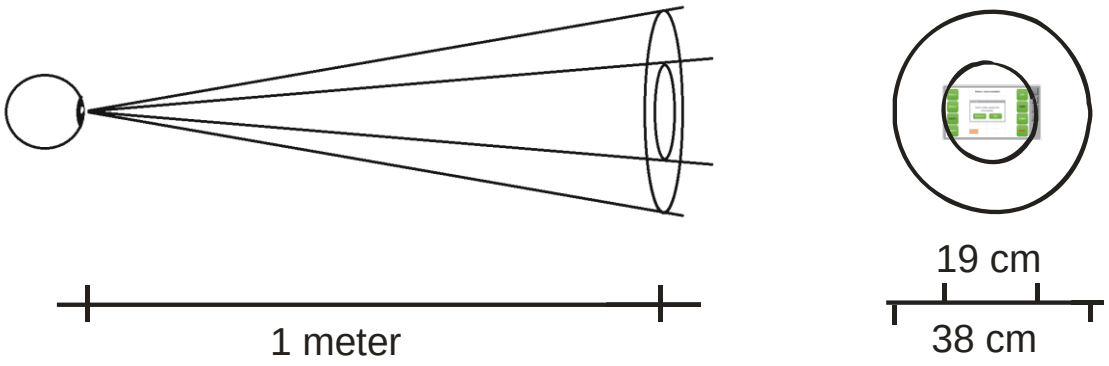
Obrázek č. 21 - Blokový diagram základních funkcí Modulu, zdroj: vlastní

Ovládání Modulu musí být pro obsluhu rychlé a intuitivní. Z toho důvodu je třeba eliminovat maximum ovládacích prvků (tlačítek) a periferií (myš). Jasnou volbou je proto využít dotykovou obrazovku. Aby ji uživatel efektivně, musí být na ni schopen přesně zvolit cíl a vyhnout se nechtěnému výběru cílů přilehlých. Design aplikace musí zohlednit jak technické možnosti zařízení, tak i ergonomii [V.6], [46], fyziologii člověka a poznatky kognitivní psychologie [I.33].

Velikost displeje 7“ vychází z poznatků o zorném úhlu akomodovaného pohledu, uvažované vzdálenosti displeje od hlavy operátora, množství informací zobrazovaných na ploše displeje, jemné motoriky a také je dána prostorem potřebným pro montáž integrovaných snímačů. Navíc, větší jednotka by již neúměrně zabírala prostor při montáži.

Zorné pole akomodovaného pohledu na text je v rozsahu 5°-10°. Na uvažované vzdálenosti 1 metr od očí operátora jde o kruhovou plochu o průměru minimálně 19 cm a maximálně 38 cm. Dotyková obrazovka plní funkci jak zobrazovací jednotky, tak i ovládacího panelu. Vzdálenost Modulu od hlavy je stanovena tak, aby zobrazovaná informace byla čitelná a zároveň ovládání bylo pohodlné pro běžné výšky dospělých osob. Umístění Modulu na povrch skříně o běžné výšce 120 – 180 cm je realizovaná do výšky 100cm jeho horní hrany od podlahy, přičemž sklon displeje je pevně daný konstrukcí Modulu na 40° od horizontální roviny.

Množství zobrazované informace grafické a textové, zvlášť pak velikost písma a detaily použité grafiky, směrem k drobným detailům a menší velikosti použitého fontu písma vedou k zúžení pohledu k uvedené dolní hranici. Z obrázku č. 22, který je publikován v článku [V.7], je patrný rozdíl maximální a minimální plochy.



Obrázek 22. - Zobrazení změny proporcí ploch pro různou úroveň detailů, zdroj: vlastní

Nemalou roli sehrává i jemná motorika. Soustředění na ovládání malé dotykové plochy a nižší přehlednost daná velkosti písma a množství zobrazované informace vede k snížení pracovní použitelnosti. Přesnost, s níž je člověk schopen vybrat cíl na pomoci prstu nebo stylusu, závisí na jeho poloze na obrazovce. Nejvyšší přesnost je deklarována v jejím středu, o něco nižší v levém a pravém okraji. Nejnižší přesnost zacílení je na horním, zejména pak na dolním okraji obrazovky. Pro udání přesnosti v souřadném systému se používají různé metody. Výpočty metody CEP se opírají o pravděpodobnou kruhovou chybu a vycházejí z vojenských statistických výpočtů vyhodnocování přesnosti zásahu cíle.

Metoda R95 používá 95% přesnost [I.34]. Pro dosažení cíle v centru potřebujeme plochu o 7 mm, zatímco v dolních rozích 12 mm [V.6], [I.35,] [47]-[49]. Uživatelé si jsou podvědomě toho vědomi, z čehož vyplývá mírně pomalejší výběr menších cílů v rozích a na hranách obrazovky. Naproti tomu, pokud je prst již v kontaktu s obrazovkou, přesnost pohybu je 0,1 mm [50], [I.36].

Podle laboratorní studie MIT [51], [52] je průměr průměrná šířka prstu dospělé osoby 16 – 20 mm, což je více, než uvádějí doporučení pro vývoj mobilních aplikací. Shrnutí lze najít na oficiálních stránkách Ubuntu [I.37], kde je shrnutí poznatků a doporučení pro vývoj GUI pro dotykové displeje. Dotykové plochy špičky prstu jsou 8 – 10 mm, zatímco u polštářků prstů jde o průměrnou 10 – 14 mm. Na rozdíl od doporučení firmy Apple a Microsoft [I.38]-[I.40], které uvádějí, že velikost dotykové plochy ovládacího prvku by neměla být menší než 9 mm se vzájemným rozestupem 2 mm, se zde uvádí minimální velikost 10 mm.

Uvedený rozměr se týká prvků:

- často používaných
- umístěných blízko hrany obrazovky
- používaných v sekvenci (vytáčení čísel telefonu)

Pro méně frekventované prvky postačuje čtverec o hraně 7 mm se vzájemným rozestupem 1 mm od sousedních prvků.

Snadná obsluha je navíc ovlivněná těmito faktory:

- mladí uživatelé mají menší prsty
- osoby starší a korpulentnější mají prsty silné
- na rozdíl od kurzoru myši se při ovládání dotykem část displeje zakryje

Podle norem [V.6] jsou uváděné optimální plochy pro dotykové ovládání rozměrů vyšší. Zatímco výše uvedená doporučení budou nuceně implementovaná na displeje s úhlopříčkou 5,5“ a menší, pro větší plochy již tak striktně neplatí.

Při dodržení výše uvedených poznatků byla velikost základní sady ovládacích prvků určených pro pohyb v GUI v krajích displeje stanovena na 20 x 20 mm se vzájemným rozestupem 1 mm. Podle studie [53] by větší zobrazovaná tlačítka než 22x22 mm nepřinesla vyšší efekt v přesnosti zásahu, zatímco snížením velikosti na 13 x 13 mm by poklesla rychlost obsluhy panelu o více než 18%. Tomu se nelze vyhnout v případě zadávání textu ze zobrazené klávesnice při vyhledávání položek. Tato funkce je však

pro obsluhu minoritní, neboť informace o manipulovaném materiálu pochází z databáze na základě načteného kódu z jeho obalu.

Návrh, rozložení a velikost ovládacích prvků vychází jednak z výše uvedených poznatků, z požadavku na minimalizaci časové náročnosti při interakci uživatele s modulem a 7“ displeje. Rozměr jeho reálné zobrazovací plochy je 86 x 154 mm při rozlišení 800x480. Dané parametry se jeví jako dostatečné, aby se daly zobrazit jak potřebné textové, tak i grafické informace a ovládací prvky. Studií provedenou nad různými velikostmi dotykových displejů [54] lze zvolený rozměr pro dané použití potvrdit.

Velikost buněk středového rastru, které znázorňují souřadnice uloženého materiálu v policích, je pak možné zvolit až do minimální velikosti 7 x 7 mm. Aby se dala plocha police bez problému zobrazit, neměla by mít více než 10 řad a 10 sloupců, což je technicky přijatelné a s navrhovaným rozhraním kompatibilní.

Plocha ovládacích prvků je dostatečná, aby vzhledem k jejich umístění po stranách obrazovky nedocházelo při dotyku k chybám. Počet současně zobrazených prvků nikdy nevyžaduje zmenšení jejich velikost pod mez, která by znamenala nárůst chybovosti zásahu cíle prstem nebo stylusem. Z důvodu předpokládaného nasazení v kontaminovaném prostředí, kde je obsluha nucena používat ochranné pomůcky, tedy i rukavice, je uvažován stylus jako primární pointer. Průměr jeho dotykové plochy koresponduje s polštářkem prstu.

Grafický návrh vybraných oken je možné vidět na následujících obrázcích. Na obrázku č. 23 je vyobrazena základní obrazovka, kterou vidí uživatel po přihlášení. Obsahuje vyobrazení obsluhovaného objektu, jméno autentizované osoby, místo, datum a čas a trojici aktivních tlačítek pro vstup do požadované části systému.

Obrázek č. 23 - Úvodní obrazovka, zdroj: vlastní

Pokud dojde k aktivaci obrazovky dotykem, objeví se varování, že k další práci na zařízení je třeba ověření personálním čipem, viz obrázek číslo 24.

Obrázek č. 24 - Výzva k přihlášení, zdroj: vlastní

Pokud dojde k přiložení čipu, jenž není v systému neevidovaný nebo patří osobě, která k zařízení nemá definovaná příslušná oprávnění v politikách LIMS, objeví se varování vyobrazené na obrázku č. 25, s informací, že byl přístup zamítnut a proveden záznam kvalifikovaný jako incident.

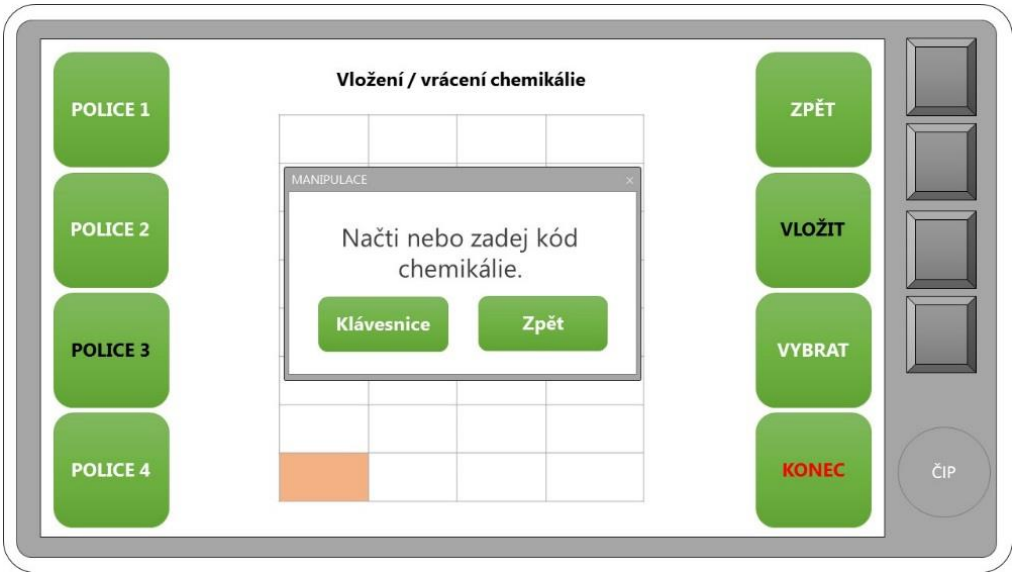
Obrázek č. 25 - Přístup odmítnut, zdroj: vlastní

Pokud byl přístup povolen, na obrazovce se objeví trojice tlačítek, která dovolí provést příslušnou akci, tedy vyzvednout nebo vložit materiál do zabezpečené oblasti. Návrh rozložení prvků je zřejmý z obrázku č. 26.

Obrázek č. 26 - Hlavní obrazovka autorizovaného přístupu, zdroj: vlastní

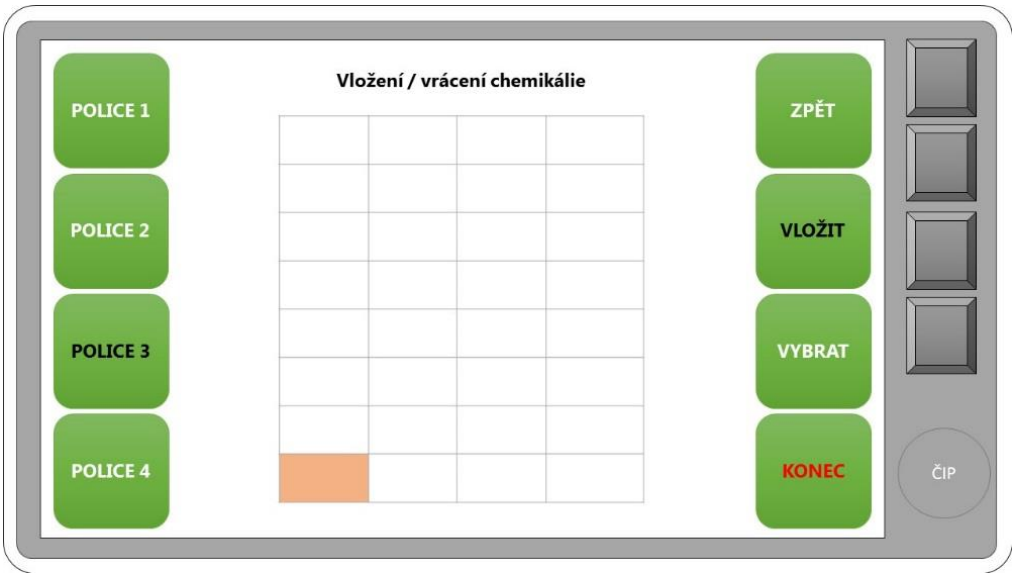
Na obrázku č. 27 je vidět, že při volbě vracení materiálu přes tlačítko „VLOŽIT“ se na obrazovce objeví výzva k načtení čarového kódu nebo jeho zadání prostřednictvím klávesnice (obrázek č. 28) pro případ, že by došlo k poškození čar např. působením chemikálií.

Po načtení kódu se zobrazí mapa s pozicí, kde má být nádoba uložena. V levém sloupci je zvýrazněno číslo police, ve středu plochy pak její souřadná síť se zvýrazněným místem tak, jako je tomu na obrázku č. 29.



Obrázek č. 27 - Obrazovka s výzvou volby identifikace předmětu, zdroj: vlastní

Obrázek č. 28 - Obrazovka manuální identifikace manipulovaného předmětu, zdroj: vlastní



Obrázek č. 29 - Obrazovka režimu vkládání předmětů do skříně, zdroj: vlastní

Před vložením nádoby je třeba zanést do systému jeho aktualizovaný stav. Primárně se provede jejím zvážením na integrované váze. Na obrázku č. 30 je vyobrazeno rozhraní pro případ manuálního zadání, kdy nádobu nelze z na tomto místě zvážit z důvodu velikosti nebo převýšení maximálního váhového limitu.

Obrázek č. 30 - Obrazovka provedení změn vlastností vkládaného předmětu, zdroj: vlastní

Při ukončení manipulace s materiálem a odchodu obsluhy, nebo po uplynutí nastaveného časového limitu, kdy je obrazovka bez interakce s obsluhou, je uživatel odhlášen. Čidlo otevření dveří způsobí, že se zobrazí pokyn k jejich zavření a spustí odpočítávání. V okamžiku, kdy je skříň uzavřena se spínač odpojí, odpočítávání je zastaveno a oznámení z obrazovky zmizí. Zůstanou-li dveře otevřené a časovač dospěje k nule, spustí se akustický signál, který na vzniklý stav upozorní. Obrazovka s varováním a odpočítáváním je na obrázku č. 31.

Obrázek č. 31 - Obrazovka odhlášení, zdroj: vlastní

Navrhovaný zabezpečený LIMS ve spojení s prvky podobnými popsanému Modulu je pro ochranu biomedicínských dat, výsledků vědecké práce i fyzického zabezpečení přínosný, pokud se jeho ovládání nestane pro uživatele přítěží. Návrh jednoduchého a přitom funkčního designu GUI je proto nezbytným krokem stejně jako návrh struktury databází a zabezpečeného propojení jednotlivých prvků v síti.

8.4 Bezpečnost CAM

Popsané zařízení je součástí koncepce systému zabezpečení citlivých dat. V kontextu systému je nutné brát zřetel na způsob jeho zařazení do struktury informačního systému laboratoře. Nelze připustit, aby se tento článek stal kritickým. Z toho důvodu bylo zvoleno za komunikační a aplikační rozhraní mezi sensory a databází AUDITDB zařízení Raspberry Pi 3. Z designu vyplývá, že sensory jsou umístěny v jeho blízkosti, aby mohly být připojené bezprostředně na jeho sběrnici ve společném pouzdře. Informace z nich získané a kódy informací vložené uživateli se v aplikační vrstvě formátují do požadovaného tvaru a zašifrovaným kanálem přenášejí na server. Pokud by se měla tato vrstva rozhraní přesunout na server a data sbírat z jednotlivých čidel, byl by síťový provoz náchylný na výpadky dat.

Aby nedocházelo ke ztrátě kontinuity dat, je CAM vybaven pamětí USB flash, na níž se ukládají logy událostí za posledních 24h. Díky tomu není primární SD karta se systémem zatěžována zápisem a čtením dat. Data ukládaná na USB flash disk se paralelně přenášejí na databázový server. Pokud dojde k výpadku datové komunikace, je systém schopen uchovávat data až za období 72h. Po navázání konektivity se nashromážděná data přenesou do databáze a systém opět přechází na mechanismus 24h zálohy dat. Podobný mechanismus byl popsán v [45] pro odesílání dat z mobilního přístroje pro monitorování zdravotního stavu osob.

Ověření identity osoby a oprávnění vstupu do chladicího boxu je realizováno online s databází účtů. Pro případ dlouhodobého výpadku síťové konektivity je Raspberry Pi 3 vybaveno lokálním účtem, kterým lze ovládat elektrický zámek. Procesně je potřeba tento stav ošetřit v manuálu laboratoře. Záznam bude obsahovat minimálně následující informace:

- způsob přechodu do offline režimu
- místo, kde lze získat přihlašovací údaje
- pokyny k vedení evidence vstupu do chladicího boxu
- způsob přechodu zpět do online režimu

Dále může být jednotka vybavena BT komunikačním kanálem, přes který se lze dostat na rozhraní nouzového ovládání elektrického zámku. Tato možnost je dána libovolnému Smart zařízení s předinstalovanou aplikací, které je schopné se spárovat a jehož operátor zná přístupový kód pro nouzový přístup. Daná funkcionalita je méně nápadná z hlediska použití a měla by zůstat pod kontrolou administrátorů laboratoře.

Pro časově omezený offline provoz způsobený výpadkem konektivity je možné zvážit doplnění aplikačního vybavení o blok pro dočasné uložení přihlašovacích údajů již dříve přihlášených osob, která by se aktualizovala s každým online přihlášením. Platnost uložených údajů by byla časově limitována a exspirované záznamy by se automaticky mazaly. V případě výpadku síťové konektivity by pro běžného uživatele tak zůstal přístup do chladicího boxu bez omezení. Pro případ ztráty síťové konektivity z důvodu výpadku elektrické energie by stačilo doplnit napájení o zdroj záložní energie, který by byl schopný po omezenou dobu napájet jak elektroniku, tak i elektrický zámek. Neboť většina laboratoří má záložní zdroj napájení řešený např. dieselagregátem, byl by časový rámec definován časem jeho naběhnutí. Výpadek elektrické energie má jiný koeficient dopadu na činnost laboratoře a nelze jej proto řešit podle postupu pro samostatnou ztrátu síťové konektivity. Bude-li modul ve spojení s mrazákem hlubokých teplot, je třeba zajistit, aby byl otevřen jen krátkodobě, jen pro navrácení materiálu, u kterého hrozí jeho znehodnocení. I tak je třeba zvážit, zda je, vzhledem k ceně obsahu mrazničky a vzniklé situaci, třeba materiál vracet, zvýšit tím teplotu a potenciálně ohrozit životnost uloženého materiálu.

Pečlivým výběrem HW komponent lze dosáhnout velmi dobrých výsledků. Zařízení jako celek je stabilní a údaje, které poskytuje, jsou pro sledování provozu dostatečně přesné.

Do informačního systému v části pro zpracování dat v rámci laboratorního experimentu je vložena bezpečnostní funkce sledování uložení citlivého materiálu a výsledků experimentů. Lze tak snadno odhalit neoprávněnou manipulaci s nimi, což byl primární cíl. Další analýzou dat se dají zjistit např. možná pochybení v uložení vzorků, která vedou ke snížení kvality nebo jejich znehodnocení.

Aby bylo možné plně důvěřovat kolekci sesbíraných dat systému logování, musí být zabezpečena jejich integrita. Systém ukládání je nutné navrhnout tak, aby umožňoval ověření zdroje dat a následně jednosměrnou komunikaci od něj pro provedení zápisu. Dále je třeba zamezit možnost editace zaznamenaných dat. Po verifikaci zdroje informace, přenesení dat vygenerovat kontrolní součet daného záznamu.

Jak již bylo v kapitole 5.4 popsáno, integrace bezpečnostních prvků do navrhovaného systému dovoluje regulovat pohyb na základě oprávnění ke vstupu do jednotlivých zón. Ve spojením s informacemi získanými z HW modulu lze osobám, které si odebraly sledovaný materiál z lednice, zamezit opustit prostor místnosti, kde se vykonává experiment nebo prostory laboratoře. Mohou nastat mimořádné situace, kdy bude nutné například pro záchranu života laboranta, který s toxickou látkou nezacházel v souladu s bezpečnostními pokyny. Tyto lze však ošetřit v provozních směrnicích laboratoře.

9 MOŽNOSTI DALŠÍHO ROZŠÍŘENÍ LIMS

Následující část obsahuje diskutované problémy, které nepatří bezprostředně do diskutované oblasti zabezpečení duševního vlastnictví osob a organizace, avšak jsou součástí workflow. Byly definovány v rámci úvodní studie zmíněné v kapitole 6.1, při definování rizik a jejich dopadu. Sledováním dále diskutovaných parametrů jde spíše o vytvoření podpory činností a organizace a tím ulehčení a omezení chyb lidského faktoru. Studiem kolekce hodnot je však možné odhalit nekalé činnosti v laboratoři a pomoci objasnit bezpečnostní incidenty.

Provázanost navrhovaného LIMS s dalšími systémy je třeba brát jako nevyřčený požadavek uživatele, zadavatele. Mimo rozhraní přístrojů zavedených v laboratoři je možné databázi IS primárně propojit se dalšími kategoriemi rozhraní, jejichž náplň bude objasněný dále v textu:

- SW pro zpracování a vyhodnocování kolekce dat z experimentů
- Rozhraní podnikového informačního systému (modul logistiky, personálního systému,...)
- Rozhraní centrálního systému sběru klinických dat
- Rozhraní SMART technologií

Rozhraním pro SW pro zpracování a vyhodnocování kolekce dat z experimentů je myšlen konektor pro řízené napojení databáze s daty definovaného experimentu na statistický SW, s jehož pomocí lze provést jejich vyhodnocení a vytvoření výstupů pro následnou prezentaci. Oprávnění definované jen skupině managementu jí umožní rozkrýt blok dat, který by jinak přístupný nebyl. IBM SPSS Statistic je SW, který je na takovou variantu připravený.

Rozhraní podnikového informačního systému je možné vnímat jako část, v níž bude zapojený SW interface umožňující načíst z personální databáze osoby zaměstnané v laboratoři a podle pozice jim předpřipravit uživatelský účet a iniciační balíček oprávnění. Může jím být také napojení na logistický modul a propojení s databází majetku, který je v inventurní sestavě laboratoře nebo na systém tvorby objednávek spotřebního materiálu pro činnost laboratoře.

Rozhraní centrálního systému sběru klinických dat lze chápat spíše jako vizi, která má základ v projektu eHealth a ve vizi rodícího se oboru pracujícího nad kolekcí klinických dat získaných z pracovišť praktických a odborných lékařů. Pro potřeby vědy není třeba znát osobní údaje pacientů. Systémy vytvářející kolekcí dat jsou zodpovědné za předání jen nezbytných, avšak pro potřeby výzkumu použitel-

ných dat. Starají se o deidentifikaci citlivých údajů. Koncept byl popsán v [V.1] a [V.2]. Dostatek aktuálních klinických dat je pro epidemiologické studie neocenitelným zdrojem informací pro sledování a popis postupu různých druhů onemocnění [D.1], [D.4], [D.5] a [D.7].

Rozhraní SMART technologií má obrovský potenciál. Směrování modernizace moderních provozů je ovlivněno trendem digitalizace označovaným Průmysl 4.0. Vize robotizace a automatizace se postupně uplatňují i mimo hlavní průmyslová odvětví a nacházejí reálná uplatnění mimo jiné v projektech automatizovaných laboratoří. Může jít o podporu rutinních činností v průběhu experimentů, ale také jím může být podpora řízení laboratoře a logistiky. Lze monitorovat zvolené laboratorní vybavení, dodržování bezpečnostních postupů nebo pracovní podmínky v laboratořích.

Existuje mnoho situací, které doposud nejsou zcela pokryty technologickým vybavením. Prvky automatizace by mnohé z nich elegantně vyřešily. Dominantně jde o sledování a doplňování spotřebního materiálu, avšak jsou zde jistá omezení. Materiál spotřebovávaný v laboratořích lze rozdělit do tří hlavních kategorií:

1, Materiál pro podporu a přípravu experimentů vycházející z rutinních postupů provádění experimentů. Jde o periodicky nakupované chemikálie a pomůcky potřebné pro realizaci rutinních metod a diagnostických postupů, směsi pro práci s buněčnými médii. Ta vychází z reality posledních let, kdy se testy neprovádí na zvířatech ale jen na tkáních. Do této kategorie patří mezi ně ochranné pomůcky, rozpouštědla (voda, organická rozpouštědla), chemikálie pro nastavení pH roztoků (pufrů), plyny, jednorázové plastové pomůcky,...

2, Materiály pro přípravu biologických preparátů a pro realizaci vybraných laboratorních metod. Jsou vázané ke konkrétním postupům, které se neprovádí často. Díky fyzikálně-chemickým vlastnostem je třeba je doplňovat na základě plánů činností laboratoře. Příkladem mohou být tzv. kity, jejichž cena je vysoká a exspirace krátká.

3, Nebezpečný materiál, jehož nákup podléhá povolením, neboť je životu nebezpečný. Může jít o toxiny, omamné a psychotropní látky apod. Ty jsou pak uložené ve skladech s režimovým přístupem. Jde o sklady vysoce nebezpečných látek, sklad omamných a psychotropních látek, které bývají v zónách, kde se tyto látky jednak uchovávají, ale také připravují na experimenty např. ředěním. Do skladů s omezeným přístupem osob se dále ukládají látky testované v rámci patentových řízení.

Autonomní systémy mohou v plném rozsahu obsloužit pouze pořízení materiálu uvedeného v první kategorii, neboť nehrozí riziko zmaření investic do nákladů na jejich pořízení. Většinou jde o materiál, jehož cena je v porovnání s kategorií druhou nízká a jeho spotřeba je kontinuální. Pro druhou

kategorii lze použít jen automatizované sledování množství materiálu s možností přípravy jeho objednávky. V rámci zavedených laboratoří jsou již pro uvedené zažité a praxí potvrzené postupy. Pokud je nový informační systém převezme korektně, nedojde k narušení plynulosti provozu.

Do kategorie autonomních systémů nemusí patřit jen objednávání materiálu, ale také servisní činnost. Pro ilustraci jsou dále uvedeny tři příklady s navrhovaným řešením.

Případ 1: Střežení teploty v lednicích a skladových prostorech

Definice problému: Zmíněna byla lednice a stav odpojení od napájení. Pokud jde o lednici s hluboce zamraženými biologickými vzorky na teplotu -80°C, je zakolísání teploty nad určitou mez kritické. Přes všechna opatření se stává, že dojde k dlouhodobějšímu výpadku napájení. Pokud jde o pracovní dny, nebývá to problém. Ten nastává ve dnech volna. Teplota uvnitř mrazáku přesáhne kritickou mez a po obnově napájení se zas vrátí do provozního normálu. Obsluha nemá jak vyhodnotit, že k incidentu došlo. U biologicky aktivních vzorků může dojít k nevratnému znehodnocení. Pokud se vzorek bez znalosti události použije, nevykazuje požadované vlastnosti a experiment končí neobjasnitelným neúspěchem.

Řešení: Pokud má modul střežení teploty dostatečné vlastní záložní napájení a GSM modul, je schopen sledovat a zaznamenávat hodnoty z čidel, případně odeslat varovnou zprávu. Po obnově napájení a síťové konektivity může informaci o incidentu zapsat k dalšímu vyhodnocení do DB logů. Pokud záložní napájení dostatečné není, lze předpokládat, že než bude modul vypnut, bude schopný trend stoupání teploty zachytit. V záznamech systému by se měl pak objevit nejen ten, ale také časový úsek bez kontinuálního ukládání hodnot, což může být použito ke zhodnocení závažnosti stavu incidentu.

Případ 2: Střežení technických plynů

Definice problému: Experimenty stojí na materiálu, který je k jejich provedení v definovaném množství nezbytný. Lidský faktor může způsobit, že podmínky před jeho zahájením nejsou dodrženy ve smyslu logistického zabezpečení. Problémem může být nedostatek plynu, který je uskladněný v tlakové láhvi.

Řešení: Zařazením inteligentního snímače tlaku do cesty před ventil můžeme mít periodicky hlášený přehled o stavu zásob doplněný vysláním varovné zprávy v případě

- rychlého úniku obsahu lahve (neodborná manipulace, závada, prasklá hadice)
- nečekaného navýšení tlaku v lahvi (vystavení tlakové nádoby žáru)
- poklesu tlaku pod definovanou mez (ohrožení dalších experimentů)

Provozní plyny patří do první kategorie spotřebního materiálu, propojením na systém logistiky lze zautomatizovat vytvoření a odeslání objednávky.

Případ 3: Střežení kvality deionizované vody

Definice problému: Stav výrobníku deionizované vody. Jeho provoz je limitovaný životností komponenty, jež funkci deionizace zabezpečuje. Stav kapaliny na výstupu se kontroluje pomocí testu vodivosti. Snižováním účinnosti filtru dochází k průniku iontů na výstup. Od překročení určitého limitu již nelze takto upravenou vodu v experimentech používat. Pokud se včas nezachytí ztráta účinnosti a nezabezpečí servis, který nelze provést svépomocí, experimenty se zastaví se všemi důsledky z toho vyplývajícími. Interval životnosti komponenty je závislý na množství zpracované vody a její vstupní kvalitě, což vylučuje řídit servis jako periodicky se v čase opakující akci.

Řešení: Pokud by se ve výstupním zásobníku v pravidelných intervalech sondou kontrolovala vodivost a data zaznamenávala v informačním systému, mohl by jím být v předstihu vygenerovaný požadavek, který by osoba zodpovědná za logistiku v laboratoři zpracovala. Vzhledem k ceně servisního zásahu jde o druhou kategorii materiálů a služeb, proto zde nelze použít mechanismus automatického objednání servisního zásahu.

Výčet není pochopitelně úplný. Souhrn poznatků o provozu biomedicínské laboratoře, o mechanismech fungování a návazností rutinních činností je podnětem k hlubší analýze. Již jen z uvedených příkladů, které vzešly z předběžného prozkoumání, se jeví přínosné pokryt oblast inteligentními systémy. Našly by zde uplatnění konkrétně multiagentní systémy, které by zpracovávaly informace z gridu sdílených agentů. I tato oblast je pro prostředí laboratoří specifická, vychází z přesnosti měření. Pro mnoho systémů je postačující tolerance naměřených hodnot vyšší, než tomu bude v laboratořích. S tím a také s poznatky o akreditacích pak souvisí i mechanismus provádění periodických kalibrací čidel a vedení souvisejících záznamů. Řešením by se mohla zabývat práce s návrhem na automatizaci a zefektivnění procesů za použití SMART technologií.

10 DISKUZE VÝSLEDKŮ

Části práce definované v zadání jako cíle jsou mnohdy rozpracovány ve více blocích, neboť navazují na jednotlivé etapy vývoje nebo se prolínají jednotlivými stavebními bloky navrhovaného informačního systému. Jako příklad lze uvést pojem/termín „bezpečnost“. Nachází se v různých etapách v různém kontextu. Přibyly k nim také poznatky, které se prolínají etapami a také ty, které se v průběhu tvorby návrhu objevily a jsou pro realizaci přínosné.

Základní cíle této disertační práce jsou uvedené v kapitole 3. Jejich naplnění je shrnuto v následující části, kde jsou diskutovány výsledky a uvedeny výstupy použité v příspěvcích na konferencích či v časopisech.

Analýza stávajícího workflow a jeho porovnání se standardy

Jako první byla v kapitole 4.1 provedena analýza organizačních struktur a stávajícího workflow laboratoří. Byly vzájemně porovnány organizační struktury tří fyzických subjektů a modelů daných normami. Vzhledem k zákonem stanoveným podmínkám pro provoz laboratoří, skladování a nakládání s chemickými, biologickými látkami nelze očekávat, že by se organizační struktura laboratoří významně lišila. Nebylo tedy složité sestavit vlastní model, který splňuje bezpečnostní požadavky vycházející z požadavků nejnáročnější z nich, tedy katedrou toxikologie. Od nich se odvíjí další postup.

Analýza systémů podpory laboratoří vycházející z doporučení a norem pro výstavbu laboratoří
Na základě postupů definovaných normami a dobré laboratorní praxe byly definovány funkce, které nejsou obvykle zahrnuty do informačních systémů laboratoří. Především se dotýkalo systémů zabezpečení vstupu. Výsledky posloužily pro kategorizaci dat a následně pro návrh frameworku LIMS. Daná etapa je popsána v kapitole 5, výsledky analýzy a návrhu byly popsány v konferenčních příspěvcích [V.4], [V.5] a prezentovány na mezinárodních konferencích ICCCI 2016. Z materiálů vzešel článek uvedený v IF Journal of Intelligent and Fuzzy Systems v roce 2017 [V.3]

Analýza rizik kompromitace dat

Analýzou rizik zpracovanou v kapitole 6.1 bylo potvrzeno, že stav neodpovídá bezpečnostním požadavkům, a že je třeba klást vyšší důraz na ochranu duševního vlastnictví a na efektivnější nakládání s monitorovaným materiálem. Obojí má dopad na všeobecnou úsporu finančních prostředků.

Z toho důvodu byly v kapitole 5.3 stanoveny parametry pro úroveň autentizace uživatelů přistupujících nejen do elektronického informačního systému laboratoře, ale také do jejích prostor. V této

fázi byly definovány zóny, které odrážení nejen oblasti dle nebezpečnosti, ale také dle citlivosti informací s daným prostorem svázaných. K dané problematice byl prezentován článek [V.8] na mezinárodní konferenci HED 2018.

Návrh úpravy workflow

Na základě analýzy organizační struktury a stávajícího workflow laboratoří byl vytvořen vlastní model, popsaný v kapitole 7.2. Opírá se o elektronický laboratorní deník, jehož funkce podpořené bezpečnostními prvky jsou v modulu LabApp, což není jediný a zásadní rozdíl. Zatímco v na výstupu informačního systému klinické laboratoře očekáváme výstup hodnot z předdefinovaného rozsahu s případným automatickým vyhodnocením, v případě primárního výzkumu jde o hodnoty, které bude třeba odůvodnit a verifikovat dalšími pokusy a měřeními. Pokud bylo použito postupů, které plně nekorespondují s běžnou praxí, je třeba také tyto validovat.

Návrh zahrnuje průběžně zpracované a vyhodnocované informace o monitorovaném, převážně chemickém a biologickém, provozním materiálu. Přínosem je zlepšení plánování jeho pořizování a realizace doplňování v souladu s požadavky na připravované nebo již prováděné experimenty. Pro podporu zmíněného procesu je využito HW modulu navrženého pro autentizaci uživatelů odebírajících materiál z boxů v laboratoři a ke sledování pohybu uloženého materiálu. Je popsaný v kapitole 8.

Na tuto část navazuje kapitolou 8.3 pojednání o vhodném sjednoceném a uživatelsky vstřícném grafickém rozhraní pro celý informační systém. K úkolům zabezpečení bezpečnosti neodmyslitelně patří proces zálohování a obnovy dat. Se vzrůstajícími útoky na infrastrukturu firem, medicínská zařízení nevyjímaje, je třeba nastavit odpovídající mechanismus ochrany v systému uložených dat. Tím se zaobírá poslední blok návrhu struktury, přičemž vychází z modelu chování útoků Ransomware.

Návrh integrace funkcí a komponent vybraných systémů do integrovaného prostředí

Podle zpracovaných metodik je třeba na začátku prozkoumat bezpečnost systému již od jeho základních stavebních bloků. Po zvážení výhod i omezení je zamýšleno systém vybudovat na základech Open Source řešení, proto byly provedeny testy nabízených funkcí a porovnání zranitelností jak u operačních systémů, tak u aplikační vrstvy, kterou zde představují CMS servery. Porovnání a výsledky se nacházejí v kapitole 6. Nebylo prokázáno, že by testované operační systémy, Open Source i komerční zástupci, měly výrazně odlišné výsledky. Naproti tomu hodnocení systémů CMS, které byly zvoleny výhradně z Open Source, tyto vykazovaly rozdílnou úroveň zabezpečení.

Návrh zabezpečené infrastruktury datového prostředí

5.6 a 7.4 Návrh modulární struktury vychází z trendu, avšak nabízí funkce, které jsou specifické pro oblast využití v laboratořích primárního výzkumu v podmínkách akademických institucí. Pro tu je specifickou i fluktuace lidí. Návrh frameworku proto přichází i s vlastním HW řešením 8, které svými funkcemi v důsledku pokrývá nejen oblast bezpečnostní, ale nabízí i podporu workflow dalších systémů. Jedná se o detailní popis a jsou v něm zapracované také poznatky z ergonomie ovládání dotykových panelů, aby byla obsluha intuitivní a nezpomalovala rutinní činnosti více než je pro dosažení zabezpečení manipulovaného materiálu nutné. Koncept byl zpracovaný v příspěvku prezentovaném na mezinárodní konferenci Radiolektronika v Brně [V.7]

V průběhu prováděné analýzy rizik v prostředí plánovaného informačního systému byly od sebe odděleny prvky plně související s vytvořením zabezpečeného frameworku od ryze provozních. Mnohé z těch, které v hlavní části této práce nebyly využity, představují podněty pro další studii návrhu a případnou realizaci automatizace některých rutinních procesů. Neboť se systém navrhovaný jako modulární, s možností vytvářet konektory pro laboratorní zařízení, bylo by jistě možné navázat takto i vlastní řešení. Stejně tak lze vidět provázání s dalšími datovými zdroji, které poskytují klinická data. V pracích prezentovaných na přelomu roku 2014 a 2015 na konferencích CINTI 2014 [V.1] a MAREW 2015 [V.2] jde o studie, avšak v projektu eHealth již podobná funkcionalita nabírá reálnou podobu. Skutečnostmi uvedenými v tomto odstavci se v závěru práce zaobírá kapitola 9 a dává nástin dalšího směrování vývoje laboratorních informačních a management systémů.

11 ZÁVĚR

Cílem disertační práce bylo navrhnout zabezpečený framework Laboratorního informačního a management systému pro biomedicínské laboratoře primárního výzkumu provozované v rámci akademických institucí. Základem problematiky jsou jednak specifičnosti, které nedovolují využití již existujících elektronických informačních systémů určených pro klinické laboratoře a rozvoj nových technologií, které lze úspěšně do prostředí laboratoří primárního výzkumu implementovat. V porovnání s ostatními typy laboratoří je zde nestabilní často měněná sestava pracovníků vyplývající kromě jiného např. z pohybu studentů pregraduálního i postgraduálního studia na praxi. Tento fakt je zdrojem rizik na mnoha úrovních.

K dosažení vytyčeného cíle byl zpracován diagram organizační struktury a od něj v následné studii odvozeno workflow, jehož základem je elektronický laboratorní deník, který svou strukturou koresponduje s kreativním prostředím tohoto typu laboratoře. S důrazem na zabezpečení duševního vlastnictví do něj byly implementovány prvky zamezující sledování globálního výsledku probíhajícího experimentu. Jako podpůrný prvek bylo detailně navrženo hardwarové řešení ve formě modulu napojeného na informační systém laboratoře. V souladu s postupy v příslušných normách byly provedeny testy potenciálních platforem.

Framework laboratorního informačního management systému navržený jako modulární řešení splňuje požadavky a sledované trendy elektronických systémů laboratoří daného typu, přičemž nabízí další rozšiřitelnost funkcí dle úzce specifických požadavků laboratoří dle jejich konkrétního zaměření, čímž naplňuje cíle této disertační práce.

12 SEZNAM POUŽITÉ LITERATURY

1. Cagınd, O., Otles, S.: Importance of laboratory information management systems (LIMS) software for food processing factories. Journal of Food Engineering, Volume 65, Issue 4, December 2004, Pages 565-568, ISSN 0260-8774, DOI: 10.1016/j.jfoodeng.2004.02.021
2. Quo C.F., Wu, B., Wang, M.D.: Development of a Laboratory Information System for Cancer Collaboration Projects. IEEE Engineering in Medicine and Biology 27th Annual Conference, 2005, DOI: 10.1109/IEMBS.2005.1617070
3. Kammergruber, R., Robold, S., Karliç, J., Durner, J.: The future of the laboratory information system – what are the requirements for a powerful system for a laboratory data management?. Clinical Chemistry and Laboratory Medicine (CCLM), 2014, vol. 52, issue 11, DOI: 10.1515/cclm-2014-0276
4. Prasad P.J., Bodhe, G.L.: Trends in laboratory information management system. Chemometrics and Intelligent Laboratory Systems, 2012, vol. 118, page 187-192, DOI: 10.1016/j.chemolab.2012.07.001
5. Ekins S.: Computer Applications in Pharmaceutical research and Development. Sean Ekins, Wiley, 2006, page 57-61, ISBN 0-471-73779-8
6. ISO/IEC 17025 - General requirements for the competence of testing and calibration laboratories
7. ISO 9001 ”Quality management”
8. ZOF 1996, United States Public Law, p.104-191
9. Personal Information Protection and Electronic Documents Act, Second Session, Thirty-six Parliament, 48-49 Elizabeth II, 1999-2000, Statutes of Canada 2000
10. Law on the Protection of Personal Information, promulgated by the Diet of Japan on May 30, 2003
11. Privacy Act of 1988, Commonwealth of Australia, Act No. 119 of 1988 as amended
12. Hansen, M., Kohntopp, K., Pfitzmann, A.: The Open Source approach - opportunities and limitations with respect to security and privacy. Computers & Security, Volume 21, Issue 5, 1 October 2002, Pages 461-471, DOI 10.1016/S0167-4048(02)00516-3
13. Delaney N. F., Echenique, J. I. R., Marx, C. J.: Clarity: An Open-Source Manager for Laboratory Automation. Journal of Laboratory Automation, 2012, vol. 18, issue 2, pages 171-177, DOI: 10.1177/2211068212460237
14. Machina, H. K., Wild, D. J.: Laboratory Informatics Tools Integration Strategies for Drug Discovery: Integration of LIMS, ELN, CDS, and SDMS. Journal of Laboratory Automation, 2012, vol. 18, issue 2, page 126-136, DOI: 10.1177/2211068212454852

15. Sahiti, M., Vimla L. P.: Organization of biomedical data for collaborative scientific research: A research information management system, International Journal of Information Management, Volume 30, Issue 3, June 2010, pp. 256-264, ISSN 0268-4012, DOI 10.1016/j.ijinfomgt.2009.09.005
16. Hu, Yu, Development of Information Management System Used in Laboratory. Advanced Materials Research, 2012, Published in: Engineering in Medicine and Biology Society, 2005, IEEE-EMBS 2005. 27th Annual International Conference, page 2859-2862, Conference Location: Shanghai, Publisher: IEEE, ISBN: 0-7803-8741-4, DOI: 10.4028/www.scientific.net/AMR.605-607.2518
17. Stephan, Ch., Kohl, M., Turewicz, M., Podwojski, K., Meyer, H. E., Eisenacher, M.: Using Laboratory Information Management Systems as central part of a proteomics data workflow. PROTEOMICS. 2010, vol. 10, issue 6, pages. 1230-1249, DOI: 10.1002/pmic.200900420
18. Piho, G., Tepandi, J. , Parman, M.: "Towards LIMS (Laboratory Information Management Systems) software in global context," 2012 Proceedings of the 35th International Convention MIPRO, Opatija, 2012, pp. 721-726, ISBN: 978-953-233-072-4
19. Drobník, J.: Mezinárodní pravidla pro práci v chemických a biologických laboratořích. Praha: Karolinum, 1995. ISBN 80-7184-059-9.
20. G. Piho, J: Tepandi, M. Roost, M. Parman and V. Puusep, "From archetypes based domain model via requirements to software: Exemplified by LIMS Software Factory," 2011 Proceedings of the 34th International Convention MIPRO, Opatija, 2011, pp. 570-575
21. Greenfield, J., Short, K.: Software factories: assembling applications with patterns, models, frameworks, and tools. Indianapolis, IN: Wiley Pub., 2004, ISBN: 978-0471202844
22. Mezinárodní akreditační standardy pro klinické laboratoře: komentovaný oficiální překlad. Praha: Grada, 2005. Zlepšování kvality a bezpečí zdravotní péče. ISBN isbn:80-247-1003-x.
23. Pešek, J.: Tvorba systému jakosti ve zdravotnictví a lékárenství s využitím norem ISO. Praha: Grada, 2003. ISBN 80-247-0551-6.
24. Honsa J.D., McIntyre D.A.: ISO 17025: practical benefits of implementing a quality systém, Journak of AOAC Internationat, 2003 Sep-Oct, 86 (5), pp.1038-44
25. Taina, A.: Software validation with respect to requirements specified by SR EN 15189: 2013 and SR EN 17025. In: 2015 9th International Symposium on Advanced Topics in Electrical Engineering (ATEE) IEEE, 2015, 2015, s. 720-724, ISBN 978-1-4799-7514-3, DOI:10.1109/ATEE.2015.7133899
26. Steinberg, R.A.: Architecting ITIL: a reference for architecting the complete enterprise architecture and configuration items needed to operate an IT service management infrastructure. Victoria, B.C: Trafford, 2005. ISBN 142518034-5.
27. TSO (THE STATIONARY OFFICE): ITIL foundation handbook. 3rd ed. London: TSO, 2012. ISBN: 978-0-11-331349-5

28. GAMP 5: A Risk-based Approach to Compliant GxP Computerized Systems. Tampa, FL: ISPE Headquarters, 2008. ISBN ISBN 1-931879-77-X
29. Chengui, Y., Sheng, Ch., Xiaojun, W.: Research and design of LIMS based on B / S structure. In: 2010 2nd International Conference on Industrial and Information Systems, IEEE, 2010, s. 188-191, ISBN 978-1-4244-7860-6, DOI:10.1109/INDUSIS.2010.5565879
30. Hillard, M.S., Larson, D.L., Rosenberg, M.J.: LIMS: a suite of database tools for laboratory organization. In: Proceedings 14th IEEE Symposium on Computer-Based Medical Systems. CBMS 2001 IEEE Comput. Soc, 2001, s. 158-162 DOI: 10.1109/CBMS.2001.941714. ISBN 0-7695-1004-3
31. Carette, R. N., Why software fails, Software failure: IEEE Spectrum, 2005, 42(9), 42-49, ISSN:0018-9235, DOI:10.1109/MSPEC.2005.1502528
32. Ericsson, E., Gustafsson. P., Hook, D., Wurtemberg L.M., Waldo R.F.: Process improvement framework evaluation. In: 2010 International Conference on Management Science & Engineering 17th Annual Conference Proceedings, IEEE, 2010, s. 319-326, DOI:10.1109/ICMSE.2010.5719823. ISBN 978-1-4244-8116-3
33. Yusof, M. M., Arifin, A.: Towards an evaluation framework for Laboratory Information Systems. Journal of Infection and Public Health, 2016, 9(6), 766-773, ISSN 18760341, DOI:10.1016/j.jiph.2016.08.014
34. Announcing Approval of Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, and Revision of the Applicability Clause of FIPS 180-4, Secure Hash Standard
35. Hub, M., Capek, J. , Myskova, R. , Roudny, R.: Usability versus security of authentication, International Conference on Communication and Management in Technological Innovation and Academic Globalization-Proceedings, Puerto De La Cruz, SPAIN, 2010, pg.34-38, ISBN 978-960-474-254-7
36. Kasik, V. , Penhaker, M., Novak, V., Bridzik, R., Krawiec, J.: "User Interactive Biomedical Data Web Services Application," in E-Technologies and Networks for Development. vol. 171, J. J. Yonazi, E. Sedoyeka, E. Ariwa, and E. ElQawasmeh, Eds., ed, 2011, pp. 223-237. ISBN:978-3-642-22728-8, ISSN: 1865-0929
37. Dolezal, R., Sobeslav, V., Hornig, O., Balik, L., Korabecny, J., Kuca, K.: HPC Cloud Technologies for Virtual Screening in Drug Discovery. Intelligent Information and Database Systems, page 440-449, 7th Asian Conference, ACIIDS 2015 Bali, Indonesia, March 23–25, 2015 Proceedings, Part II, DOI: 10.1007/978-3-319-15705-4_43
38. Smith, R.: Deflating the Big Bang Fast and Scalable Deep Packet Inspection with Extended Finite Automata, SIGCOMM'08, August 17–22, 2008, Seattle, Washington, USA

39. Gionis, A., Tassa, T.: “k-Anonymization with Minimal Loss of Information”, Knowledge and Data Engineering, IEEE Transactions on, vol. 21, Iss 2, pp 206-219, Feb. 2009, ISSN: 1041-4347, DOI: 10.1109/TKDE.2008.129
40. Ramerazi, V.: Finite Automata Models for Anomaly Detection, The Institut for System Research Technical Reports, TR 2002-42, CISS March 2003
41. Kumar, G., Kumar, K., Sachdeva, M.: The use of artificial intelligence based techniques for intrusion detection: a review. Artificial Intelligence Review, 34 (4), Springer, 2010
42. Stančík, P.: Internet věcí útočí, SecurityWord 4/2016, IDG
43. Pavlik, J., Komarek, A., Sobeslav, V.: Security information and event management in the cloud computing infrastructure, Computational Intelligence and Informatics, 2014, pages 209-214, DOI: 10.1109/CINTI.2014.7028677
44. Behan, M., Krejcar, O.: Adaptive Graphical User Interface Solution for Modern User Devices. In 4th Asian Conference on Intelligent Information and Database Systems, ACIIDS 2012, March 19-21, 2012 Kaohsiung, Taiwan. LNCS Vol. 6592. pages 411-420
45. Morisawa H, Hirota M, Toda T.: Development of an open source laboratory information management system for 2-D gel electrophoresis-based proteomics workflow. BMC Bioinformatics. 2006; 7:430. DOI: 10.1186/1471-2105-7-430.
46. ISO 30030 "Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)–Part 9: Requirements for Non-keyboard Input Devices". International Organization for Standardization. Geneva, Switzerland. 2000.
47. Hoober, S.: Design for Fingers and Thumbs Instead of Touch. UXmatters. Retrieved 2014-08-24.
48. Hoober, S., Shank, P., Boll, S.: Making mLearning Usable: How We Use Mobile Devices. (2014), Santa Rosa, CA.
49. Henze, N., Rukzio, E., Boll, S.: 100,000,000 Taps: Analysis and Improvement of Touch Performance in the Large. Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services. (2011). New York.
50. Parhi, P.: Target Size Study for One-Handed Thumb Use on Small Touchscreen Devices, Proceedings of MobileHCI 2006. (2006) New York.
51. Potter, R., Weldon, L., Shneiderman, B.: Improving the accuracy of touch screens: an experimental evaluation of three strategies. Proc. of the Conference on Human Factors in Computing Systems, CHI '88. Washington, DC. pp. 27–32. doi:10.1145/57167.57171
52. Dankekar, K., Balasundar, I., RAJU, M., Srinivasan., A.: 3-D Finite-Element Models of Human and Monkey Fingertips to Investigate the Mechanics of Tactile Sense. Journal of Biome-chanical Engineering, (2003), 125(5). DOI: 10.1115/1.1613673. ISSN 01480731

53. Sesto, M. E., Irwin, C. B., Chen, K. B., Chourasia, A. O., Wiegmann, D. A.: Effect of Touch Screen Button Size and Spacing on Touch Characteristics of Users With and Without Disa-bilities, In Human Factors: The Journal of the Human Factors and Ergonomics Society, 54(3), pp. 425-436, (2012), doi:10.1177/0018720811433831
54. LAI, Chih-Chun a Chih-Fu WU. Display and device size effects on the usability of mini-notebooks (netbooks)/ultraportables as small form-factor Mobile PCs. Applied Ergonomics, 2014, 45(4), 1106-1115, DOI: 10.1016/j.apergo.2014.01.009. ISSN 00036870

12.1 Internetové zdroje

I.1. Biomedical Research Center, (online 3.3.16), http://eng.fnhk.cz/cbv/introduction

I.2. University of Defence. Faculty of Military Health Sciences, (online 3.3.16), http://www.unob.cz/en/fmhs/Pages/default.aspx

I.3. University of Hradec Kralove, (online 3.3.16), https://www.uhk.cz/

I.4. LIMSwiki, (online 20.3.16), http://www.limswiki.org

I.5. Vyhláška o zdravotnické dokumentaci, (online 12.4.16), https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=77217&nr=98~2F2012&rpp=15#local-content

I.6. LABWARE Result Count, (online 28.3.16), http://www.labware.com/

I.7. Lab Collector, (online 28.3.16), http://labcollector.com/

I.8. Open-KM, (online 28.3.16), https://www.openkm.com/

I.9. FDA Title 21 CFR Part 11: Electronic Records; Electronic Signatures; (online 1.3.18), https://www.accessdata.fda.gov/SCRIPTs/cdrh/cfdocs/cfcfr/CFR-Search.cfm?CFRPart=11&showFR=1

I.10. Good Laboratory Practice, (online 18.1.18), http://ec.europa.eu/growth/sectors/chemicals/good-laboratory-practice_cs

I.11. The OECD Principles of Good Laboratory Practice, (online 1.3.18), http://www.oecd-ilibrary.org/environment/good-laboratory-practice/the-oecd-principles-of-good-laboratory-practice_9789264012837-2-en

I.12. Správná laboratorní praxe, hlava III § 18 - 20 zákona č. 350/2011 Sb., (online 1.3.18), https://www.mzp.cz/www/platnalegislativa.nsf

I.13. Směrnice Evropského Parlamentu a Rady 2004/9/ES ze dne 11. února 2004 o inspekci a ověřování správné laboratorní praxe (SLP), (online 6.12.17), http://www.mzp.cz/ris/ais-risdb-ec-table.nsf/1DE2D00D7B53EE8BC1256E7B0046BCCB/$file/32004L0009Fin.pdf

I.14. Správná laboratorní praxe, (online 2.3.18), http://www.sukl.cz/leciva/spravna-laboratorni-praxe

I.15. BSI Group, BSI Group presentation: (online 28.2.18), https://commons.wikimedia.org/w/index.php?curid=12177885

I.16. Developing ISO standards, online 28.2.18), https://www.iso.org/stages-and-resources-for-standards-development.html

I.17. Information technology — Security techniques — Information security management systems — Requirements, (online, 12.1.2018) https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27001:ed-1:v1:en:sec:6

I.18. Qi Analytica. LISA.lims, (online 22.3.16), http://lisa.lims.cz/

I.19. AgiLAB, (online 28.3.16), http://www.scientificcomputing.com

I.20. BIKA LIMS, (online 29.3.16), http://www.bikalabs.com/gpllicense
I.21. Open-LIMS, (online 29.3.16), http://www.open-lims.org
I.22. LABkey, (online 30.3.16), https://www.labkey.org
I.23. ILIAS LMS, (online 30.3.16), http://www.ilias.de/docu/ilias.php?baseClass=ilrepositorygui&reloadpublic=1&cmd=frameset&ref_id=1
I.24. Security policy settings reference, (online 20.8.17) https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-policy-settings-reference
I.25. The Role of Biometrics in Enterprise Security (online 5.2.18), http://www.dell.com/downloads/global/power/ps1q06-20050132-Tilton-OE.pdf
I.26. CESNET. Data Care, (online 12.3.16), https://du.cesnet.cz/en/start
I.27. ownCloud, (online 12.3.16), https://owncloud.org/
I.28. CVE details, (online 28.4.16), https://www.cvedetails.com
I.29. UCURI - test zranitelnosti CMS (online 2.2.17) https://geekflare.com/find-wordpress-vulnerabilities/
I.30. Databáze zranitelností WordPress, (online 15.3.17) https://wpvulndb.com/
I.31. Online skenování zranitelností webů založených na platformě WordPress, (online 12.1.17) https://wpscans.com
I.32. SQLworkbench, (online 24.10.17), http://www.sql-workbench.net/dbms_comparison.html
I.33. Human Factors and Ergonomics Society, (online 16.5.16), https://www.hfes.org//Web/Default.aspx
I.34. Touchscreen: Ergonomics and usage, (online 16.5.16), https://en.wikipedia.org/wiki/Touchscreen#Ergonomics_and_usage
I.35. Circular error probable, (online 16.5.16), https://en.wikipedia.org/wiki/Circular_error_probable
I.36. TapSense: Enhancing Finger Interaction on Touch Surfaces, (online 20.5.16), http://www.chrisharrison.net/index.php/Research/TapSense/
I.37. UMEGuide/DesigningForFingerUIs, (online 20.5.16), https://help.ubuntu.com/community/UMEGuide/DesigningForFingerUIs
I.38. iOS Human Interface Guidelines, Apple, , (online 3.5.16), https://developer.apple.com/ios/human-interface-guidelines/overview/design-principles/
I.39. Metrics and Grids. Google, (online 3.5.16), https://material.io/guidelines/layout/metrics-keylines.html#
I.40. Design and UI, (online 3.5.16), https://developer.microsoft.com/en-us/windows/apps/design

VLASTNÍ PUBLIKACE K TÉMATU

V.1 Blazek, P., Krenek, J., Kuca, K., Jun, D., Krejcar, O., The system of instant access to the life biomedical data (2014) CINTI 2014 - 15th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings, art. no. 7028686, pp. 261-265. DOI: 10.1109/CINTI.2014.7028686

V.2 Blazek, P., Krenek, J., Kuca, K., Krejcar, O., Jun, D., The biomedical data collecting system (2015) Proceedings of 25th International Conference Radioelektronika, RADIOELEKTRONIKA 2015, art. no. 7128996, pp. 419-422, DOI: 10.1109/RADIOELEK.2015.7128996

V.3 Blazek, P., Kuca, K., Jun, D., Krejcar, O., Development of information and management system for laboratory based on open source licensed software with security logs extension (2017) Journal of Intelligent and Fuzzy Systems, 32 (2), pp. 1497-1508. DOI: 10.3233/JIFS-169145

V.4 Blazek, P., Kuca, K., Krenek, J., Krejcar, O.; Increasing of Data Security and Workflow Optimization in Information and Management System for Laboratory (2017) IWBBIO Granada, 26. - 28. 4. 2017, Lecture Notes in Computer Science (LNCS), Vol. 10208, pp. 602-613, DOI: 10.1007/978-3-319-56148-6_54

V.5 Blazek, P., Kuca, K., Jun, D., Krejcar, O., Development of information and management system for laboratory based on open source licensed software (2015) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9330, pp. 377-387. DOI: 10.1007/978-3-319-24306-1_37

V.6 Blazek, P., Krejcar, O., Jun, D., Kuca, K., Device Security Implementation Model based on Internet of Things for a Laboratory Environment (2016) IFAC-PapersOnLine, 49 (25), pp. 419-424. DOI: 10.1016/j.ifacol.2016.12.086

V.7 Blazek, P., Krejcar, O., Kuca, K., Concept of a module for physical security of material secured by LIMS, (2018) IWBBIO Granada, 25. – 27. 4. 2018, Lecture Notes in Computer Science (LNCS), Book:Bioinformatics and Biomedical Engineering, DOI:10.1007/978-3-319-78723-7_30

V.8 Blazek, P., Ondrej Krejcar, O., Kuca, K., Deployment of New Technologies as an Integral Part of Secure Information Systems Environment, HED 2018 Hradec Kralove, 2018, Vol. 8 (1) Part I., ISBN 978-80-7435-700-8

SEZNAM DALŠÍCH PUBLIKOVANÝCH PRACÍ

D.1 Boštíková, V., Pasdiorová, M., Marek, J., Prášil, P., Salavec, M., Sleha, R., Střtítecká, H., Blažek, P., Hanovcová, I., Šošovičková, R., Špliňo, M., Smetana, J., Chlíbek, R., Hytych, V., Kuča, K., Boštík, P., Biological factors influencing infectious diseases transmitted by invasive species of mosquitoes [Biologicke factory ovlivnujici vybrane infekcni nemoci prenasené invazivnimi druhy komaru] (2016) Klinická mikrobiologie a infekční lékařství, 22 (2), pp. 75-85.

D.2 Krenek, J., Kuca, K., Blazek, P., Krejcar, O., Jun, D., Application of artificial neural networks in condition based predictive maintenance (2016) Studies in Computational Intelligence, 642, pp. 75-86. Cited 1 time. DOI: 10.1007/978-3-319-31277-4_7

D.3 Krenek, J., Kuca, K., Krejcar, O., Maresova, P., Sobeslav, V., Blazek, P., Artificial neural network tools for computerised data modeling and processing (2014) CINTI 2014 - 15th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings, art. no. 7028685, pp. 255-260. DOI: 10.1109/CINTI.2014.7028685

D.4 Bostik, V., Sleha, R., Salavec, M., Janovska, S., Chlibek, R., Blazek, P., Stritecka, H., Hytych, V., Kuca, K., Hanovcova, I., Sosovickova, R., Smetana, J., Splino, M., Marek, J., Bostik, P.; CHARACTERISTICS OF VARICELLA ZOSTER (VZV) VIRUS (2016) Mil. Med. Sci. Lett. (Voj. Zdrav. Listy) 2016, vol. 85(4), p. 164-170, ISSN 0372-7025 http://www.mmsl.cz

D.5 Salavec,M., Boštíková, V., Boštík, P., Blažek, P.; Varicela - Zoster virus - Review, Dermatovenerologie 6/2016 http://referatovyvyber.cz/dermatovenerologie/index.php?option=com_k2&view=itemlist&layout=category&task=category&id=63&Itemid=7

D.6 Bostikova, V., Kuca, K., Blazek, P., Sleha, R., Pasdiorova, M., Marek, J., Stritecka, H., Hytych, V., Bostik, P., Zika virus - a review. Mil. Med. Sci. Lett. (Voj. Zdrav. Listy), 2016, sv. 85, č. 3, s. 94-103. ISSN 0372-7025. http://www.mmsl.cz

D.7 Boštíková V., Sleha R., Janovská S., Blažek P., Střítecká H., Salavec M., Boštík P.: Dopad migrační vlny na obraz infekčních onemocnění a očkovací strategie v Evropě. Vakcinologie

ÚČAST NA GRANTECH A PROJEKTECH

Smart Solutions in Ubiquitous Computing Environments

- Excelence 2014, Principal investigator: doc. Ing. Ondřej Krejcar, Ph.D.
- Scientific focus: usability, web applications, user preference

Smart Solutions for Ubiquitous Computing Environments

- SPEV 2014, Principal investigator: doc. Ing. Ondřej Krejcar, Ph.D.
- Scientific focus: usability, web design, user interface

Chytrá řešení v prostředích všudypřítomných systémů

- Excelence 2015, Principal investigator: doc. Ing. Ondřej Krejcar, Ph.D.
- Scientific focus: : usability, web design, user interface

Smart Solutions for Ubiquitous Computing Environments

- SPEV 2015, Principal investigator: doc. Ing. Ondřej Krejcar, Ph.D.
- Scientific focus: : usability, web design, user interface

Efektivnost rozhodování a vztah firma-spotřebitel

- SPEV 2015, Principal investigator: Mgr. Jan Draessler, Ph.D.
- Scientific focus: user preference, design requirements, interaction design

Smart Solutions for Ubiquitous Computing Environments

- SPEV 2016, Principal investigator: doc. Ing. Ondřej Krejcar, Ph.D.
- Scientific focus: user preference, design requirements, interaction design

Kognitivně-behaviorální analýzy lidského chování

- SPEV 2016, Principal investigator: prof. PhDr. Marek Franěk, CSc., Ph.D.
- Scientific focus: user interface, user interaction, user experience

Smart Solutions for Ubiquitous Computing Environments

- SPEV 2017, Principal investigator: doc. Ing. Ondřej Krejcar, Ph.D.
- Scientific focus: user preference, design requirements, interaction design

Smart Solutions for Ubiquitous Computing Environments

- SPEV 2018, Principal investigator: doc. Ing. Ondřej Krejcar, Ph.D.
- Scientific focus: user preference, design requirements, interaction design