SNAS SLOVENSKÁ NÁRODNÁ AKREDITAČNÁ SLUŽBA

METODICKÁ SMERNICA NA SPRÁVNU LABORATÓRNU PRAX
METHODICAL GUIDELINE FOR GOOD LABORATORY PRACTICE

APLIKÁCIA ZÁSAD SLP NA POČÍTAČOVÉ SYTÉMY

APPLICATION OF GLP PRINCIPLES TO COMPUTERISED SYSTEMS

MSA – *G/09*

BRATISLAVA
August 2001

Slovenská národná akreditačná služba (ďalej len SNAS) je jedinou akreditujúcou osobou (akreditačným orgánom), určenou Ministerstvom hospodárstva Slovenskej republiky v zmysle zákona NR SR č. 264/1999 Z.z. na akreditáciu skúšania výrobkov, kalibrovania meradiel, certifikačných, inšpekčných a iných obdobných technických činností. SNAS posudzuje a osvedčuje systémy správnej laboratórnej praxe.

Základným poslaním SNAS je zabezpečiť dôveru zainteresovaných orgánov, inštitúcií a osôb doma a v zahraničí posudzovaním zhody, uskutočňovaným v Slovenskej republike a ich spôsobilosť potvrdzovať akreditáciou. Vytvárajú sa tak predpoklady na garantovanie kvality slovenskej produkcie, realizovanej na domácom i na zahraničnom trhu, kvality dovážaných výrobkov, na ochranu spotrebiteľa, ochranu životného prostredia a zdravia obyvateľov.

SNAS dbá všetkými prostriedkami na to, aby procesy posudzovania na účely akreditácie a osvedčovania SLP boli transparentné, nestranné, objektívne, na potrebnej odbornej úrovni a, aby sa rešpektovali potreby uchádzačov o akreditáciu a potreby užívateľov výsledkov práce akreditovaných subjektov.
Pri plnení svojej funkcie SNAS vychádza z medzinárodne prijatých prístupov, pravidiel a postupov obsiahnutých predovšetkým v normách radu STN EN 45000, radu STN EN ISO/IEC 17000, radu STN EN ISO 9000, v pokynoch ISO/IEC a v pokynoch a návodoch medzinárodných organizácií ILAC, IAF, EA a OECD, ktoré plne rešpektuje.

Metodické smernice na akreditáciu (ďalej MSA) bližšie špecifikujú zásady a princípy týchto dokumentov s cieľom zabezpečiť kompatibilitu procesu akreditácie v Slovenskej republike s medzinárodnou praxou.

Oznámenia o vydaní, zmenách a doplnkoch MSA sa uverejňujú vo Vestníku ÚNMS SR.

Spracoval: Pharm. Dr. Ivana Šidlíková.

Schválil: Ing. Ľubomír Šutek, CSc. - riaditeľ SNAS

Účinnosť od: 1. septembra 2001

Táto MSA neprešla jazykovou úpravou.

Dostupnosť MSA : Slovenský ústav technickej normalizácie,
Karloveská 63, P.O. BOX 246, 840 00 Bratislava 4,
Predajňa noriem - telefón: 02/654 25 055, 602 94 469, fax :02/ 654 28 845
Virtuálna predajňa - http//: www.sutn.gov.sk

OBSAH
CONTENTS

***

1. ÚVODNÉ USTANOVENIA

1.0 Úvod

MSA-***G /09*** stanovuje kritéria pre počítačové systémy, ktoré sa používajú v rámci skúšania v laboratóriách na generovanie, meranie alebo stanovenie údajov najmä v regulovanej oblasti. V laboratóriách, kde sa vykonáva skúšanie z hľadiska bezpečnosti zdravia a životného prostredia by mali byť všetky počítačové systémy validované, prevádzkované a udržiavané podľa tejto MSA.

Do tejto MSA bol v plnom rozsahu zapracovaný text medzinárodného dokumentu OECD Environment Monograph No. 116

1.2 Východiskový dokument

The Aplication of the Principles of GLP to Computerised Systems"
OECD GLP Consensus Document Number 10 (revised), Environment Monograph No.116, Paris 1995

1.3 Súvisiace dokumenty

OECD Principles of Good Laboratory Practice
ENV/MC/CHEM(98)17, IOMC, Paris 1998

Commission Directive 1999/11/EC
Commission Directive 1999/12/EC

1.0 Definície

Akceptačné kritériá **-** zdokumentované kritériá, ktoré sú potrebné pre úspešné ukončenie testovacej fázy, alebo ktoré musia vyhovieť požiadavkám.

Akceptačný test - formálne testovanie počítačového systému v jeho predpokladanom operačnom prostredí, aby sa zistilo, či všetky akceptačné kritériá testovacieho zariadenia boli dosiahnuté a či je systém vhodný pre operačné použitie.

Záloha - Opatrenia urobené pre znovunadobudnutie dátových súborov alebo softvéru, pre reštartovanie spracovania údajov, alebo pre neskoršie použitie alternatívneho počítačového zariadenia po prípadnom zlyhaní systému alebo pri katastrofe.

Kontrola zmien - neustále hodnotenie a dokumentácia činnosti systému a jeho zmien z dôvodu zistenia, či validačný proces sleduje každú zmenu, ktorú je potrebné zaznamenať do počítačového systému.

Počítačový systém - skupina hardvérových zložiek a pridruženého softvéru, ktorý je navrhnutý a zostavený tak, aby vykonával špecifickú funkciu alebo skupinu funkcií.

Elektronický podpis_- vstup vo forme magnetických impulzov alebo kompilácie počítačových údajov zložených z rôznych symbolov alebo série symbolov, zrealizovaných, adaptovaných alebo autorizovaných osobou, ktorý je zhodný s jej rukopisným podpisom.

Hardvér - fyzické komponenty počítačového systému, zahŕňajúce vlastnú počítačovú jednotku a jej periférne komponenty.

Periférne komponenty - každé pripojené prístrojové vybavenie, prídavné alebo vzdialené komponenty ako sú tlačiarne, modemy, terminály, a pod.

Uznané technické štandardy - štandardy vyhlásené národnými, alebo medzinárodnými orgánmi, ktoré stanovujú štandardy (ISO, IEEE, ANSI, atď).

Bezpečnosť - ochrana hardvéru a softvéru počítača pred náhodným alebo zlomyseľným prístupom, použitím, modifikáciou, deštrukciou alebo odhalením. Ochrana sa tiež týka, personálu, údajov, komunikácie a fyzickej a logickej ochrany počítačových inštalácií.

Softvér **(aplikácia)** - program, ktorý je získaný, vyvinutý, adaptovaný a/alebo prispôsobený požiadavkám testovacieho zariadenia pre účely riadenia procesov, zberu údajov, manipulácie s údajmi, zaznamenávania údajov a/alebo archivácie.

Softvér **(operačný systém)** - program alebo súbor programov, štandardných programov alebo podprogramov, ktoré kontrolujú činnosť počítača. Operačný systém vykonáva napr. alokáciu zdrojov, plánovanie, vstupnú/výstupnú kontrolu a riadenie údajov.

Zdrojový kód - pôvodný počítačový program vyjadrený pre človeka v čitateľnej forme (programovacom jazyku), ktorý musí byť preložený do čitateľnej formy pre počítač predtým ako je ním spracovaný.

Validácia počítačového systému - ukážka, že počítačový systém je vhodný pre určené účely.

1.5 Použité skratky

OECD	Organisation for Economic Co-operation and Development
QA	Quality Assurance - Zabezpečenie kvality
SLP	Správna laboratórna prax
SNAS	Slovenská národná akreditačná služba
ŠPP	Štandardný pracovný postup
ÚNMS SR	Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky

1.6 PREDHOVOR

V rámci tretieho pracovného zasadnutia OECD skupiny pre oblasť Správnej laboratórnej praxe, ktorý sa konal 5.-8. októbra 1992 v Interlakene (Švajčiarsko), pracovná skupina odborníkov diskutovala o interpretácii zásad SLP na počítačové systémy. Pracovnú skupinu viedol Dr. Theo Helder z holandského úradu SLP; zapisovateľom bol Bryan Doherty (predseda počítačového výboru Britskej asociácie pre výskum zabezpečenia kvality). Účastníkmi pracovnej skupiny boli zástupcovia z oboch národných Úradov kontroly pre dodržiavanie SLP a z testovacích laboratórií nasledovných krajín: Rakúsko, Belgicko, Dánsko, Fínsko, Francúzsko, Nemecko, Japonsko, Holandsko, Švajčiarsko, Spojené kráľovstvo a Spojené štáty americké. Pracovná skupina sa na tomto zasadnutí nedokázala dohodnúť na presnom znení dokumentu. Vytvorila však dokument nazvaný „*Pojmy vzťahujúce sa k počítačovým systémom v prostredí SLP*“, ktorý určuje a opisuje všeobecné zásady. Návrh dokumentu, ktorý vznikol v tejto pracovnej skupine, dali členským krajinám na pripomienkovanie.

Na základe obdržaných komentárov, Panel pre Správnu laboratórnu prax na 5. zasadaní v marci 1993 rozhodol, že je potrebné vykonať ďalšie úpravy a zvolať druhé stretnutie pracovnej skupiny. Pod vedením Dr. Heldera a pána Dohertyho ako zapisovateľa sa skupina stretla 14. – 16. decembra 1994 v Paríži. Účastníkmi boli zástupcovia z Kanady, Dánska, Francúzska, Nemecka, Japonska, Holandska, Švédska, Spojeného kráľovstva a Spojených štátov amerických.

Návrh konsenzného dokumentu vytvoreného pracovnou skupinou bol založený na dokumente vychádzajúceho zo zasadnutia v Interlakene, z komentárov členských krajín a dokumentu vytvoreného Pracovnou skupinou zo Spojeného kráľovstva. Text bol následne skontrolovaný, modifikovaný a odsúhlasený Panelom a Spoločným zasadnutím Výboru pre chemikálie a Pracovnej skupiny pre chemikálie OECD. Výbor životného prostredia odporučil, aby tento dokument bol sprístupnený úradom generálneho sekretariátu.

1. VECNÁ ČASŤ

2.1 APLIKÁCIA ZÁSAD SLP NA POČÍTAČOVÉ SYSTÉMY

Za posledné roky stúplo používanie počítačových systémov pre testovanie látok z hľadiska bezpečnosti zdravia a životného prostredia. Tieto počítačové systémy zahŕňajú priamy a nepriamy zber dát, spracovanie, zaznamenávanie a uloženie dát a čoraz viac tvoria integrálnu časť automatizovaného vybavenia. Tam, kde sú počítačové systémy pridružené k vykonávaniu štúdií zameraných pre regulované oblasti, je dôležité, aby boli vyvíjané, validované (platné), riadené a udržiavané v súlade so zásadami SLP OECD.

Nasledujúce stanovisko by malo slúžiť pri aplikácii zásad SLP pre už vyššie spomínané počítačové systémy:

2.1.1 Rozsah

Všetky počítačové systémy, ktoré sa používajú na generovanie, meranie alebo stanovenie údajov a s ktorými sa uvažuje v regulovanej oblasti, by mali byť zdokonaľované, validované, prevádzkované a udržiavané v súlade so zásadami SLP.

Počas plánovania, vypracovania a zaznamenávania štúdií, môže byť súčasne používaných niekoľko počítačových systémov na rozličné účely. Takéto účely by mohli zahŕňať priamy a nepriamy zber dát z automatizovaných prístrojov, činnosť/riadenie automatizovaného zariadenia a spracovanie, zaznamenávanie a uchovávanie dát. Kvôli rôznym aktivitám, je možné počítačovým systémom obmeňovať programovateľný analytický nástroj alebo osobný počítač na riadiaci systém laboratórnych informácií (LIMS) s viacnásobnými funkciami. Zásady SLP by sa mali používať pri akomkoľvek rozsahu zapojenia.

2.1.2 Prístup

Počítačové systémy spojené s vedením štúdie, ktoré sú určené pre regulovanú oblasť, by mali mať primeraný dizajn, primeranú kapacitu a mali by byť vyhovujúce pre zamýšľané účely. Taktiež by mali byť vytvorené príslušné postupy na riadenie a údržbu týchto systémov a tieto systémy by mali byť vyvíjané, validované a prevádzkované v súlade so zásadami SLP.

Podstatný význam má ukážka, ktorá dokazuje, že daný počítačový systém je vhodný pre určené zámery. Tento postup sa vysvetľuje ako počítačová validácia.

Proces validácie poskytuje vysoký stupeň záruky, že počítačový systém vyhovuje jeho vopred určenej špecifikácii. Validácia by mala byť garantovaná pomocou formálneho plánu validácie a mala by byť prevedená pred spustením prevádzky.

2.1.3 Zodpovednosti

a) *Manažment* skúšobného zariadenia má celkovú zodpovednosť za dodržiavanie zásad SLP. Táto zodpovednosť zahŕňa menovanie a efektívne usporiadanie adekvátneho počtu kvalifikovaného a skúseného personálu ako aj povinnosť zabezpečiť, že zariadenia, vybavenie a postupy týkajúce sa spracovania údajov sú v súlade s predpísanou normou.

Jednou z úloh manažmentu je zabezpečiť, aby počítačové systémy boli vyhovujúce na určené účely. Manažment by mal tiež vytvoriť zásady a metodiku, ktorá by zaistila, že vyvinuté systémy sú validované, prevádzkované a udržiavané v súlade so zásadami SLP. Dodržiavanie týchto postupov a zásad by malo byť efektívne monitorované.

Manažment určuje personál, ktorý bude zodpovedný za vývoj, validitu, prevádzku a údržbu počítačových systémov. Tento personál by mal byť primerane kvalifikovaný s dostatočnými skúsenosťami a vhodným tréningom, aby mohol vykonávať svoje úlohy v súlade so zásadami SLP.

b) *Vedúci štúdií* sú zodpovední za celkové vedenie štúdií v súlade so zásadami SLP. Keďže veľa štúdií bude využívať počítačové systémy, je nevyhnutné, aby si títo vedúci pracovníci boli plne vedomí zainteresovanosti počítačových systémov používaných v štúdiách pod ich vedením.

Zodpovednosť vedúceho štúdie za zaprotokolovanie údajov v elektronickej forme je taká istá ako vo forme papierovej a iba oprávnené systémy môžu byť použité v SLP štúdiách.

c) *Personál.* Personál, ktorý využíva počítačové systémy je zodpovedný za činnosť týchto systémov v súlade so Zásadami SLP. Personál, ktorý zodpovedá za vývoj, validitu, činnosť a údržbu počítačových systémov je zodpovedný za vykonávanie týchto činností v súlade so zásadami SLP a uznávanými technickými štandardami.

d) *Zabezpečenie kvality (QA).* Zásady a postupy pracovníkov pre zabezpečenie kvality týkajúcich sa počítačových systémov musia byť definované manažmentom a zaznamenané v písomnej forme. Program zabezpečenia kvality by mal zahŕňať postupy a pokyny, ktoré zaistia, že zavedené štandardy zodpovedajú všetkým fázam validácie, činnosti a údržby počítačových systémov. V postupoch a pokynoch by mali byť zaznamenané informácie o zavádzaní kúpených a vývoj nových počítačových systémov.

Personál pre zabezpečenie kvality je povinný sledovať, či práca s počítačovými systémami prebieha v súlade so zásadami SLP. V prípade nevyhnutnosti tréningu v tejto oblasti, je potrebné zabezpečiť školenie v rôznych špeciálnych technikách. Personál by mal byť dostatočne erudovaný v oblasti počítačových systémov, v niektorých prípadoch je však potrebné zabezpečiť audit špecialistov.

Personál pre zabezpečenie kvality by mal mať priamy prístup k údajom uloženým v počítačovom systéme.

1.0.0 Školenia

Zásady SLP vyžadujú, aby skúšobné zariadenie malo primerane kvalifikovaný a skúsený personál. Skúšobné programy a školenia pri práci, alebo účasť na externých kurzoch, musia byť zaznamenávané a dokumentácia archivovaná.
Vyššie spomenuté nariadenia sa týkajú všetkých pracovníkov zainteresovaných vo využívaní počítačových systémov.

2.1.5 Zariadenia a vybavenie

Z dôvodu vedenia štúdie v súlade so zásadami SLP je potrebné zabezpečiť primerané zariadenie a vybavenie. Uvádzame niekoľko návodov pre správne používanie počítačových systémov:

a) ***Zariadenia***

Dôležitým aspektom je správne umiestnenie hardvéru, periférnych zložiek (modemy, tlačiarne, terminály) a elektronického pamäťového média. Pri inštalácii sa odporúča vyhnúť sa extrémnym teplotám, vlhkosti a prachu, elektromagnetickému rušeniu a tesnej blízkosti káblov vysokého napätia.

Do úvahy sa musí zobrať aj elektrická zásuvka pre počítačové vybavenie, zálohovanie pamäti, alebo neprerušiteľné zdroje pre počítačové systémy, ktorých náhle zlyhanie by nepriaznivo ovplyvnilo výsledky.

Primerané zariadenia by mali zabezpečiť bezpečné udržiavanie elektronického uskladnenia údajov.

b) ***Vybavenie***

i) Hardvér a softvér

Počítačový systém je definovaný ako skupina hardvérových zložiek a pridruženého softvéru, ktorý je navrhnutý a montovaný tak, aby vykonával špecifickú funkciu alebo skupinu funkcií.

Hardvér je fyzická zložka počítačového systému, ktorá zahŕňa samotné počítačové zariadenie a jeho periférne zložky.

Softvér je program alebo programy, ktoré ovládajú prevádzku počítačového systému.

Zásady SLP, ktoré sú požadované pre vybavenie, sú potrebné pre hardvér aj softvér.

ii) *Komunikácie*

Komunikácie, ktoré sa všeobecne vzťahujú na počítačové systémy, spadajú do dvoch kategórií: medzi počítačmi a medzi počítačmi a periférnymi zložkami.

Všetky komunikačné linky sú potencionálnym zdrojom chyby a môžu mať za následok stratu alebo poškodenie dát. Z týchto dôvodov je potrebné vykonávať príslušné kontroly bezpečnosti a integrity údajov počas vývoja, validácie, činnosti a údržby počítačových systémov.

2.1.6 Údržba a obnova systému po havárii

Všetky počítačové systémy by sa mali inštalovať a udržiavať takým spôsobom, aby sa zabezpečila kontinuita presného výkonu.

a) ***Údržba***

Mali by sa zaznamenávať postupy údržby a postupy pre odstránenie závad. Postupy by taktiež mali zahŕňať presný popis úloh a povinností zainteresovaného personálu.

V prípade, že boli vykonané počas údržby nevyhnutné zásahy do hardvéru a softvéru, mala by sa prekontrolovať validitu systému.

Počas dennej prevádzky sa musia uschovávať záznamy o každom probléme, zistenej nezhode a každej uskutočnenej nápravnej činnosti.

b) ***Obnova systému po havárii***

Musia byť vypracované presné postupy pre prípad havárie, to znamená čiastočného alebo celkového zlyhania počítačového systému. Opatrenia sa môžu usporiadať od hardvérových plánovaných rezerv k spätnému systému papierovej dokumentácie.

Všetky rezervné plány musia byť náležite zdokumentované, validované, v každom prípade by mali zaistiť nepretržitú integritu údajov a štúdie. Personál, ktorý je zainteresovaný do vedenia štúdie, by mal vedieť o existencii rezervných plánov.

Postupy na obnovu počítačového systému záležia na kritickom stave systému, je však podstatné, aby boli zálohované kópie celého softvéru.

Tam, kde si činnosti pre obnovu počítačového systému vyžiadali nevyhnutné zásahy do hardvéru a softvéru, môže vzniknúť potreba opätovnej kontroly validity systému.

2.1.7 Údaje

Zásady správnej laboratórnej praxe definujú prvotné údaje ako všetky pôvodné laboratórne záznamy a dokumentácie vrátane údajov, priamo vložených do počítača cez prístrojové prepojenie, ktoré sú výsledkom pôvodných pozorovaní a ktoré sú potrebné pre rekonštrukciu a vyhodnotenie výsledkov štúdie.

Počítačové systémy, ktoré pracujú v zhode so zásadami SLP môžu uvádzať prvotné údaje v rôznych formách (elektronické pamäťové médium, počítačové alebo prístrojové výpisy, mikrofilmové/mikrofišové kópie). Je potrebné, aby prvotné údaje boli definované pre každý počítačový systém.

Tam, kde je počítačový systém používaný na zber, spracovanie alebo uloženie prvotných údajov v elektronickej podobe, je potrebné zabezpečiť uchovávanie úplných preverovacích záznamov. V týchto záznamoch musia byť uvedené všetky zmeny údajov spolu s menami osôb, ktoré zmenu vykonali, s použitím časových a dátových (elektronických) podpisov. Samozrejme musí byť uvedený dôvod každej zmeny.

V prípade, že sa údaje uchovávajú v elektronickej podobe, je potrebné zabezpečiť požiadavky dlhodobého uchovávania pre každý typ archivovaných údajov vzhľadom k predpokladanej životnosti počítačových systémov. Zmeny hardvéru a softvéru musia umožniť kontinuálny prístup a uchovanie prvotných údajov bez rizika prerušenia integrity.

Podporné informácie (napr. uchovávanie záznamov, kalibrovanie), ktoré sú potrebné na overenie validity prvotných údajov, alebo na prípadnú rekonštrukciu postupu, by sa mali uchovávať v archívoch.

Pre prípad alternatívneho zberu údajov (v prípade zlyhania počítačového systému) je potrebné mať vypracovaný pracovný postup, ktorý bude popisovať spôsob ručne zaznamenávaných údajov,

manipuláciu s nimi ako aj uchovávanie. V týchto prípadoch by tieto náhradné údaje vložené do počítačového systému mali byť identifikované ako prvotné údaje. Ručne zálohované postupy slúžia na minimalizovanie rizika straty všetkých údajov a zabezpečujú celistvé uchovávanie všetkých potrebných údajov v pamäti.

Z dôvodu výmeny zastaralého počítačového systému a následnej potreby prenosu elektronických prvotných údajov do nového systému, musí byť tento postup prijateľne zdokumentovaný a overená integrita údajov. Tam, kde nie je možné vykonať takýto presun, musia byť prvotné údaje transferované na iné elektronické médium. Toto médium je potom overené a označené ako presná kópia prvotných údajov pred deštrukciou pôvodných elektronických údajov.

2.1.8 Bezpečnosť

Na ochranu hardvéru, softvéru a údajov pred neoprávneným prístupom, vykonaním nežiadúcich zmien, stratou údajov v rámci systému, je potrebné mať vypracované presné bezpečnostné postupy. Taktiež treba zahrnúť prípad napadnutia údajov vírusmi alebo inými činiteľmi. Je žiadúce uskutočniť bezpečnostné opatrenia na ochranu integrity v prípade krátkodobého, alebo dlhodobého zlyhania pamäti.

a) Fyzická bezpečnosť

Na obmedzenie prístupu k hardvéru počítača, komunikačnému zariadeniu, periférnym zložkám a elektronickým pamäťovým médiám neoprávneným osobám, sú potrebné opatrenia fyzickej bezpečnosti. Na zariadenie, ktoré sa nenachádza v špecifických "počítačových miestnostiach" (napr. osobné počítače, terminály) sú potrebné bežné riadenia prístupu k skúšobnému zariadeniu. Avšak tam, kde sú takéto zariadenia umiestnené dislokovane (napr. prenosné zložky, modemové linky), je potrebné uskutočniť dodatočné opatrenia, ktorých úlohou je minimalizovať akékoľvek nežiadúce zásahy.

b) Logická bezpečnosť

Pre každý počítačový systém alebo aplikáciu musia byť vytvorené logické bezpečnostné opatrenia, ktoré majú uchrániť neoprávnený prístup k počítačovému systému, aplikáciám a údajom. To znamená, že je potrebné zabezpečiť používanie len schválených verzií a validovaného (platného) softvéru. Logická bezpečnosť môže zahŕňať potrebu unikátnej identifikácie používateľa pomocou vstupného hesla. Je potrebná kontrola všetkých úvodných dát alebo softvéru z vonkajších zdrojov. Tieto kontroly sa môžu vykonávať pomocou počítačového riadiaceho systému softvéru, špeciálnymi bezpečnostnými postupmi, a/alebo postupmi vloženými do aplikácií, alebo ich kombináciou.

c) Integrita údajov

Integrita uchovávania údajov je primárnym cieľom zásad SLP. Z týchto dôvodu je potrebné zabezpečiť, aby každá osoba, ktorá manipuluje s počítačovým systémom, ovládala a dodržiavala bezpečnostné postupy. Manažment je povinný zabezpečiť, aby si personál uvedomil dôležitosť zaistenia bezpečnosti údajov, postupov a funkcií systémov, ktoré sú dostupné poskytnúť primeranú ochranu a následky jej porušenia. Tieto systémy by mali poskytovať pravidelnú kontrolu prístupu k systému, realizáciu postupov na overenie súboru a vývoj záznamov.

d) Zálohovanie

Pri manipulácii s počítačovými systémami sa odporúča vyrobiť kópie celého softvéru a údajov, aby mohla byť vykonaná obnova systému v prípade jeho zlyhania (napr. poškodenie disku). Zálohovaná kópia môže zastúpiť prvotné údaje a musí sa ako taká ošetriť.

2.1.9 Validácia počítačových systémov

Počítačové systémy musia byť vhodné pre účel, na ktorý sú určené. Je preto potrebné brať do úvahy nasledujúce aspekty:

a) ***Akceptácia***

Počítačové systémy by mali byť navrhnuté v súlade so zásadami SLP a mali by byť zavedené plánovaným spôsobom. Každý systém musí byť vyvinutý tak, aby jeho vývoj mohol byť skontrolovaný, najlepšie v súlade s platnými technickými normami (t.j. ISO/9001). Samozrejmosťou je primeraná dokumentácia. Okrem toho musí existovať evidencia o tom, že systém bol pred pravidelným používaním primerane odskúšaný v súlade s prijímacími kritériami pomocou skúšobného zariadenia. Formálne prijímacie skúšanie si vyžaduje vypracovanie skúšok podľa vopred definovaného plánu a následného uchovania dokumentácie všetkých skúšobných postupov, skúšobných údajov a dosiahnutých výsledkov, ako aj formálnych záverov testovania a záznamu týkajúceho sa akceptácie počítačového systému.

U systémov dodávaných maloobchodným dodávateľom je pravdepodobné, že väčšina vytvorenej dokumentácie počas vývoja sa uchováva na strane dodávateľa. V takomto prípade evidencia príjmu počítačového systému a/alebo dodávateľovho preskúšania by mala byť dostupná pre skúšobné zariadenie.

b) ***Retrospektívne hodnotenie***

V prípade, že existujú systémy, ktoré nevyhovujú zásadám SLP (nepredvídala sa ich potreba alebo nebola špecifikovaná), je potrebné zaznamenať oprávnenosť na použitie týchto systémov, súčasťou ktorého je aj retrospektívne hodnotenie.

Retrospektívne hodnotenie sa začína zozbieraním všetkých historických záznamov, ktoré sa vzťahujú k počítačovému systému. Záznamy sa revidujú, urobí sa písomný súhrn hodnotenia, ktorý špecifikuje dostupnú evidenciu validácie a kroky, ktoré treba urobiť, aby sa zabezpečila potrebná validácia daného počítačového systému.

c) ***Kontrola pri zmenách***

Kontrola pri zmenách je formálne schválenie a dokumentácia každej zmeny počítačového systému počas prevádzkovej životnosti systému. Kontrola pri zmene je potrebná, ak daná zmena ovplyvní stav validácie počítačového systému. Zmenový riadiaci postup musí byť efektívny akonáhle je počítačový systém v prevádzke.

Postup by mal popisovať spôsob hodnotenia, ak sa vyskytne prípad potreby opakovania testovania z dôvodu zachovania validity systému.
Zmenový riadiaci postup by mal identifikovať osobu, ktorá by bola zodpovedná za určenie potreby kontroly pri prevedenej zmene systému a jej odsúhlasenie.
Bez ohľadu na pôvod zmeny (dodávateľ alebo interne vyvinutý systém), je potrebné poskytnúť príslušné informácie ako súčasť spôsobu pri kontrole zmeny. Zmenový riadiaci postup by nemal narušiť integritu údajov.

d) Podporný mechanizmus

Aby počítačový systém zostal vhodný pre zamýšľané ciele, je potrebné využívať podporné mechanizmy. Tieto mechanizmy zabezpečia funkčnosť systému a jeho správne používanie. Toto všetko môže zahrňovať systémové riadenie, rôzne typy školenia, údržbu, technickú podporu, preverovanie systému, hodnotenie výkonu. Hodnotenie výkonu (prevádzky) znamená pravidelnú revíziu systému, tak aby bola kontinuálne zabezpečovaná neustála zhoda s udanými kritériami výkonu napr. spoľahlivosť, zodpovednosť, kapacita.

2.1.10 Dokumentácia

Nasledujúce body sú návodom pre založenie dokumentácie týkajúcej sa vývoja, validácie, prevádzky a údržby počítačových systémov:

a) Postupy

Mali by byť spísané postupy riadenia zahŕňajúce okrem iného akvizíciu, požiadavky, dizajn, validáciu, skúšanie, inštaláciu, prevádzku, údržbu, personál, monitorovanie a vyradenie počítačových systémov.

b) Popis aplikácie

Pre každú aplikáciu by mala existovať podrobná dokumentácia:

- Názov užívateľského programu (aplikačného softvéru) alebo identifikačný kód a jasný, podrobný popis účelu použitia programu.
- Hardvér (s číslami modelov), na ktorých aplikácia softvéru pracuje
- Operačný systém a iný softvérový systém použitý v spojitosti s aplikáciou
- Aplikácia programovacieho jazyka a/alebo použitá databáza
- Hlavné vykonávacie funkcie programu
- Prehľad toku a typu dizajnu údajov/databázy
- Štruktúra súborov, možné chyby a algoritmy
- Aplikácia softvérových zložiek s číslami verzií
- Konfiguračné a komunikačné linky medzi aplikačnými modulmi a zariadením a inými systémami.

c) Zdrojový kód

Niektoré členské krajiny OECD požadujú, aby bol v skúšobnom zariadení dostupný, prípadne nahraditeľný zdrojový kód pre aplikáciu softvéru.

d) Štandardné pracovné postupy (ŠPP)

Prevádzková dokumentácia by mala byť vypracovaná vo forme ŠPP. Tieto postupy by mali obsahovať minimálne tieto údaje:

- Postupy na prevádzku počítačových systémov (hardvér/softvér) a úlohy zúčastneného personálu
- Postupy pre bezpečnostné opatrenia používané na rozpoznanie a zabránenie neoprávnenému prístupu a zmien programov
- Postupy a autorizáciu programových zmien a ich záznam
- Postupy pre zmeny zariadenia (hardvér/softvér) vrátane skúšania pred použitím
- Postupy na periodické skúšanie správneho fungovania kompletného systému alebo jeho častí a zaznamenávanie týchto skúšok
- Postupy na údržbu počítačových systémov a pridružených zariadení
- Postupy pre vývoj softvéru a prijímacích zariadení
- Postupy pre zálohovanie všetkých uložených dát a rezervné plány pre prípad poruchy
- Postupy pre archiváciu a získavanie všetkých dokumentov, softvérových a počítačových dát
- Postupy pre monitorovanie a auditovanie počítačových systémov.

2.1.11 Archivácia

Princípy SLP pre archiváciu údajov musia byť aplikovateľné pre všetky typy údajov. Preto je potrebné zabezpečiť, aby elektronické údaje boli archivované na rovnakej úrovni týkajúcej sa prístupu, indexácie a účelného vyhľadávania ako iné typy údajov.

V prípade, ak sú údaje z viacerých štúdií uskladňované na jednom pamäťovom médiu, je potrebné zaistiť adekvátnu detailnú indexáciu.

Môže nastať situácia, keď bude nevyhnutné obstarať zariadenia so špecifickou kontrolou prostredia na zabezpečenie integrity uchovávaných elektronických údajov. Ak si tento postup vyžaduje dodatočné archívne zariadenie, manažment by mal určiť zodpovedný personál za vedenie archívov a tým limitovať prístup k údajom. Taktiež bude potrebné zabezpečiť postupy, aby nebola porušená dlhodobá integrita údajov. Tam, kde sa vyskytujú pravidelné problémy k prístupu údajov, alebo počítačové systémy musia byť vyradené, je potrebné zabezpečiť postupy pre kontinuálnu čitateľnosť údajov.

Tieto postupy môžu zahŕňať napr. vytváranie trvalých výtlačkov záznamov v papierovej forme, alebo prenos údajov na iný systém.

Žiadne elektronicky uchovávané údaje by nemali byť zničené bez súhlasu, autorizácie manažmentu zariadenia a relevantnej dokumentácie. Iné údaje týkajúce sa podpory počítačového systému, ako je napr. zdrojový kód, vývoj, validácia, činnosť, údržba a kontrola záznamov, by mali byť udržiavané najmenej tak dlho ako je uchovávaný záznam štúdie, ktorá bola vytvorená pomocou tohto systému.

***