

Ev.č.: 110/P

Výtisk číslo:
Počet listů: 12

Schvaluji:



Děkan-velitel FVZ

plukovník doc. MUDr. PRYMULA Roman, Ph.D.

SMĚRNICE

PRO PROVOZ PROSTŘEDKŮ INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ V SÍTI INTERNET FAKULTY VOJENSKÉHO ZDRAVOTNICTVÍ

Oddělení informačních technologií

2005

1. ZÁKLADNÍ USTANOVENÍ

1.1. Síť FVZ

Síť INTERNET Fakulty vojenského zdravotnictví (dále jen SÍŤ FVZ) je určena k pokrytí informačních a komunikačních potřeb zaměstnanců a studentů fakulty. Napomáhá při plnění studijních, vědeckovýzkumných a pracovních úkolů vyplývajících ze studijního nebo pracovního poměru na FVZ v rozsahu daném skutečnými potřebami jednotlivých aktivit při respektování níže uvedených zásad. Umožňuje centralizovanou správu uživatelských účtů a programového vybavení, bezpečný přístup k informacím, využívání služeb elektronické pošty, elektronické plánování, sdílení dokumentů a zařízení.

SÍŤ FVZ je tvořena aktivními i pasivními prvky a zařízeními k nim připojenými (pracovní stanice, účastnické zásuvky, kabeláž, servery...). Do SÍŤE FVZ smí zasahovat pouze pracovníci pověřeni správcem sítě.

1.2. Služby poskytované sítí FVZ

O rozsahu poskytovaných služeb SÍŤE FVZ rozhoduje vedení FVZ. Každý oprávněný uživatel má nárok na standardní služby, které zahrnují:

- služby elektronické pošty,
- využívání standardního programového vybavení,
- přístup k všeobecně dostupným informacím vnitřní sítě a databází,
- přístup k všeobecně přístupným zdrojům a službám sítě Internet,
- přístup ke speciálním informačním pramenům a databázím sjednaný FVZ nebo UO.

SÍŤ FVZ nelze používat k činnostem nebo podpoře činností, které jsou v rozporu se zákony ČR, interními předpisy AČR, dokumenty sdružení CESNET, či ohrožují bezpečnost a spolehlivost provozu počítačové sítě.

Služby elektronické pošty nejsou určeny pro soukromou korespondenci. Rozesílání hromadných zpráv do SÍŤE FVZ je vyhrazeno vedení FVZ a správě sítě. Ostatní mohou tento způsob komunikace používat jen pro mimořádně důležitá a neodkladná sdělení, nebo sdělení zasahující zájmy širokého okruhu uživatelů vyplývající ze vztahu k FVZ.

1.3. Účel směrnice

Tato směrnice definuje zásady provozu v SÍŤI FVZ, stanovuje pravidla používání veškerých zařízení do ní připojených, a je závazná pro všechny uživatele SÍŤE FVZ.

2. ŘÍDÍCÍ ORGÁN SÍŤE

Řídícím orgánem - správcem sítě - je Oddělení informačních technologií (OdIT), které odpovídá za administraci sítě a její bezporuchový provoz. OdIT sleduje vývoj a trendy v informačních technologiích, vyhodnocuje potřeby fakulty a předkládá vedení FVZ návrhy na modernizaci sítě a zkvalitňování informačních služeb.

Správce sítě (OdIT) provádí:

- Centrální správu sítě a kontrolu dodržování pravidel provozu.
- Servis aktivních i pasivních prvků sítě.
- Plánování rozvoje a modernizace sítě a koncových zařízení.
- Centrální správu programového vybavení, jeho pořizování a modernizaci.
- Technickou a odbornou podporu uživatelů.

3. ZAŘÍZENÍ V SÍTI FVZ

SÍŤ FVZ umožňuje připojení technických zařízení určených ke komunikaci či pro práci s daty, jako jsou počítače, tiskárny, datová úložiště, zařízení pro zpracování obrazu nebo speciální laboratorní přístroje.

Za správu konkrétního prostředku informačních a komunikačních technologií (PIKT) odpovídá uživatel, kterému bylo zařízení přiděleno. Do SÍŤE FVZ nelze připojovat žádné zařízení bez vědomí správce sítě.

3.1. Tvorba a modernizace pracovišť

Správce sítě na základě podložených požadavků a s ohledem na reálné možnosti zabezpečuje vybavení pracovišť prostředky informačních a komunikačních technologií (PIKT). Vede přehled o technickém stavu zařízení v síti a dle možností provádí jeho průběžnou modernizaci.

Vedoucí pracoviště může ve zdůvodněných případech požádat o neplánovanou modernizaci přiděleného zařízení. Taková žádost musí být zpracována písemně, dostatečně zdůvodněna a potvrzena podpisem vedoucího. Správce sítě posoudí účelnost a realnost požadavku, a vyrozumí žadatele o způsobu vyřízení.

Rozsáhlé a materiálově náročné požadavky na modernizaci PIKT, případně požadavky na budování nových pracovišť, podávají vedoucí na OdIT nejpozději do měsíce prosince s výhledem na další kalendářní rok.

Pracoviště, která disponují vlastními finančními prostředky, si mohou pořizovat vybavení potřebná k zajištění své činnosti a vědeckovýzkumné práce ve vlastní režii. Pokud předpokládají zapojení takto získaných zařízení do SÍŤE FVZ, je nutné tento nákup předem konzultovat s OdIT, aby byla zabezpečena kompatibilita se systémem a ostatními zařízeními sítě. V opačném případě hrozí nebezpečí, že koupené zařízení nebude možno do sítě připojit.

Výpočetní techniku lze podle platných předpisů pořizovat pouze s nainstalovaným operačním systémem.

3.2. Připojení do sítě

K SÍTI FVZ nesmí být připojeno nepovolené zařízení. Nepovoleným zařízením ve smyslu této směrnice je veškeré zařízení, které nebylo správcem sítě pro provoz v SÍTI FVZ přiděleno, nebo schváleno. O připojení do SÍŤE FVZ či vyjmutí z ní, žádá vedoucí pracoviště. Obsahem žádosti je definice požadavku, jeho stručné zdůvodnění, určení zodpovědné osoby a podpis vedoucího. Žádost se podává písemně na OdIT.

V případě kladného vyřízení požadavku předá pracovník OdIT funkční zařízení určené osobě a poučí ji o pravidlech provozu v SÍTI FVZ. Přebírající podepíše zápis o provedeném poučení.

Zařízení nakoupená jinými pracovišti fakulty nesmí být připojena do SÍTĚ bez souhlasu OdIT. Písemný požadavek na připojení v takovém případě musí obsahovat přesné označení zařízení, jeho základní evidenční údaje, způsob porizení a stručné zdůvodnění. Žádost podepsanou vedoucím pracoviště zasílá uživatel na OdIT.

Správce sítě má právo zabránit připojení zařízení do SÍTĚ jestliže:

- připojení zařízení by bylo v rozporu s platnými předpisy a normami,
- zařízení nemá požadované parametry, není dostatečně zabezpečené, nebo by jinak mohlo ohrozit provoz v síti,
- připojení zařízení do sítě je nedostatečně zdůvodněné, nebo neúčelné,
- zařízení má nejasný původ, nebo má nedostatky v evidenci.

3.3. Organizace servisní činnosti

Opravy zabezpečuje OdIT na základě adresného požadavku uživatele, ze kterého musí jednoznačně vyplývat, pro které zařízení je servis vyžadován (číslo záznamníku). OdIT nezabezpečuje opravy zařízení, která nejsou ve vlastní evidenci FVZ nebo nemají přiděleno číslo záznamníku. Servis zařízení porizovaných jednotlivými složkami bez souhlasu OdIT není standardně zabezpečován. Technická a odborná podpora je poskytována jen na programové vybavení dodávané správcem sítě. Pravidla vyžádání servisního zásahu stanoví OdIT.

Změny konfigurace zařízení, jeho přemísťování, odstraňování závad a modernizaci jednotlivých prvků smí provádět jen OdIT nebo jím pověřený pracovník.

Diagnostika a drobné změny v konfiguraci se provádí dálkově pomocí systémových nástrojů, nebo v místě zasazení zařízení. Ostatní opravy a modernizace se provádí v servisních prostorách OdIT. Výjimkou jsou zařízení, jejichž povaha, funkce nebo vnější atributy neumožňují manipulaci.

3.4. Použití soukromého počítače

Soukromý počítač lze na pracovištích FVZ používat jen výjimečně, ve zvlášť zdůvodněných případech. Na základě doporučení bezpečnostního důstojníka útvaru takové použití povoluje děkan – velitel ve svém rozkaze.

Zařízení musí být viditelně označeno: „SOUKROMÉ PC" s uvedením čísla rozkazu, ve kterém byl jeho provoz na pracovišti povolen, a se jménem zodpovědné osoby. Uživatel soukromého počítače je povinen řídit se touto směrnici a zodpovídá za dodržování zásad OUS.

Do sítě smí být připojen jen soukromý počítač s operačním systémem Windows 2000 a vyšším. Operační systém musí obsahovat všechny výrobcem vydané bezpečnostní záplaty, a počítač musí mít zapnutou aktualizovanou antivirovou ochranu.

U soupravy musí být:

- seznam předmětů a úplná technická specifikace;
- složka s nákupními a licenčními doklady k nainstalovanému programovému vybavení.

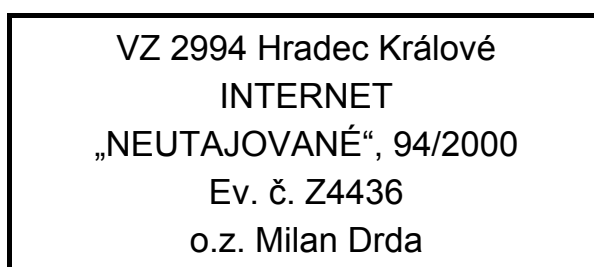
3.5. Jmenná konvence

Všechny pracovní stanice v SÍTI FVZ se musí přihlašovat do domény a používat jednotnou jmennou konvenci. Název pracovní stanice definuje správce sítě. Uživatel nemá právo svévolně přidělovat názvy pracovním stanicím, ani je měnit, nebo vytvářet nové pracovní skupiny.

3.6. Označení zařízení

Každá souprava musí být viditelně označena identifikačním štítkem. Identifikační štítek se umísťuje na čelní panel základní jednotky, monitoru a samostatných periférií kromě klávesnice a myši. Za správné označení a neporušenost pečete u přidělené soupravy zodpovídá uživatel, na pracovišti bezpečnostní správce pracoviště.

Vzor identifikačního štítku:



4. UŽIVATELÉ SÍTĚ FVZ

SÍŤ FVZ smí používat jen oprávnění uživatelé. Oprávněným uživatelem SÍTĚ FVZ je ten, kdo přistupuje do SÍTĚ FVZ na základě přihlašovacích údajů přidělených mu správcem sítě. Osoba, která využívá služeb SÍTĚ FVZ bez vědomí jejího správce, nebo připojuje do SÍTĚ FVZ nepovolené zařízení je neoprávněným uživatelem. Při zjištění neoprávněného uživatele přijímá správce sítě účinná opatření k ukončení jeho činnosti a navrhuje řešení dle platných předpisů.

4.1. Zásady používání hesla

Uživatel se přihlašuje do systému pomocí specifického přístupového jména a hesla, které musí uchovávat v tajnosti. Přihlašovací údaje jsou vázány na konkrétní osobu a jsou nepřenositelné. Při prvním přihlášení je uživatel povinen změnit inicializační heslo a vytvořit heslo nové.

Heslo musí mít minimálně pět znaků. Nedoporučuje se používat vlastní jména, nebo lehce odhadnutelné údaje (datum narození ...). Nejvhodnější je kombinace malých a velkých písmen, čísel a speciálních znaků. (Příklad správného hesla - **spR@vnEhesl0**).

4.2. Založení uživatelského účtu:

O založení nového uživatelského účtu žádá přímý nadřízený pracovníka, pro něhož je účet zřizován. Žádost se podává písemně na OdIT.

Každému uživateli je přiděleno unikátní přihlašovací jméno, inicializační heslo a poštovní schránka. Jeden uživatel sítě může mít pouze jeden uživatelský účet. Správce před zavedením účtu kontaktuje osobu, které se nový účet zřizuje a poučí ji o pravidlech

provozu v síti. Poučená osoba na závěr podepíše „Zápis o proškolení uživatele“, který se založí u OdIT.

4.3. Zrušení uživatelského účtu

Při ukončení zaměstnaneckého nebo studijního vztahu k FVZ zaniká uživateli nárok na využívání síťových služeb včetně elektronické pošty. Jeho nejbližší nadřízený je povinen zaslat na OdIT žádost o zrušení uživatelského účtu.

4.4. Uživatel zodpovídá za:

- úplnost přiděleného zařízení a jeho správné používání,
- dodržování bezpečnostních zásad práce v SÍTI FVZ a na přiděleném zařízení,
- dodržování zásad OUS při zpracovávání, ukládání a manipulaci s daty,
- používání legálního a řádně evidovaného software,
- zálohování lokálně uložených uživatelských dat,
- škody způsobené úmyslně či z nedbalosti.

4.5. Uživatel je povinen:

- pro přístup do SÍTĚ FVZ používat pouze povolené zařízení a přidělené přihlašovací údaje;
- se stolní pracovní stanicí se vždy přihlašovat do domény;
- dodržovat tato pravidla provozu v síti, související odborné normy a předpisy;
- umožnit správci sítě vzdálenou správu přiděleného počítače a na požádání spolupracovat při obnovení standardního stavu pracovní stanice;
- nosiče informací používané při práci v síti Internet nepoužívat v jiných armádních informačních systémech a naopak;
- antivirovým programem testovat stahované soubory, pravidelně spouštět testy pevných disků a kontrolovat používané nosiče informací při jejich vkládání a vyjímání;
- používat pouze legální a řádně evidované programové vybavení instalované oprávněným pracovníkem;
- při virové nákaze nebo neobvyklém chování zařízení jej okamžitě odpojit od sítě, a tuto skutečnost neprodleně nahlásit správci sítě;
- při zjištění porušení zásad OUS, nebo podezření na zneužívání SÍTĚ FVZ, okamžitě informovat bezpečnostního správce pracoviště.

4.6. Uživatel nesmí:

- používat k provozu v SÍTI FVZ nepovolené zařízení, nebo zařízení nedostatečně zabezpečené (bez aktualizací operačního systému nebo antivirového programu...);
- pracovat s uživatelským jménem nebo heslem, které mu nebylo přiděleno;
- bránit systému v aplikaci doménové bezpečnostní politiky, obcházet bezpečnostní funkce nebo používat účet administrátora;
- modifikovat programy, přistupovat do oblastí, pro které nemá oprávnění, nebo se o tyto akce pokoušet;

- používat v síti počítač nakažený viry nebo jinými škodlivými kódy;
- bránit operačnímu systému nebo antivirovému programu v provádění automatických aktualizací;
- instalovat programy nebo technická zařízení, která monitorují činnost jiných uživatelů nebo serverů, případně jinak zasahují do oblasti správy sítě;
- provádět technické zásahy do konfigurace zařízení sítě a pracovních stanic, nebo zaměňovat jejich jednotlivé komponenty;
- svévolně instalovat a používat nevidované programové vybavení, nebo instalační soubory nevidovaných programů ukládat na pevném disku;
- šířit nebo se snažit získat nelegální software;
- přetěžovat síť bezdůvodným přenášením dat o velkém objemu;
- stahovat, ukládat nebo distribuovat soubory, které nesouvisí s funkčním zařazením uživatele;
- na počítači v SÍTI FVZ pracovat s daty nebo informacemi podléhajícími režimu utajení;
- provádět jakoukoliv činnost, která by mohla ohrozit provozuschopnost nebo bezpečnost pracovní stanice nebo počítačové sítě;
- využívat SÍŤ FVZ ke komerčním účelům, nebo rozesílat „nevyžádanou“ poštu (SPAM).

5. PROGRAMOVÉ VYBAVENÍ

V SÍTI FVZ lze provozovat jen počítače s legálním programovým vybavením. Legální programové vybavení je takové, které bylo uživateli přiděleno správcem sítě či správcem programového vybavení, nebo jehož nabytí může uživatel doložit nákupním dokladem (fakturou) a licenčním osvědčením.

Veškeré programové vybavení používané v rezortu obrany musí být evidované, tzn. musí mít přiděleno evidenční číslo centrálním orgánem logistiky. Evidenci programů z vlastního nákupu vyžaduje OdIT, evidenci programů pořízených složkami FVZ vyžadují složky s odbornou pomocí OdIT.

5.1. Standardní programové vybavení

Síť FVZ je optimalizována pro toto standardní programové vybavení:

- Operační systém - Windows 2000 a vyšší
- Prolížeč Internetu - Internet Explorer
- Klient elektronické pošty - MS Outlook
- Kancelářský software - MS Office
- Antivirový program
- Adobe Acrobat Reader

Veškeré instalace a zásadní konfigurace programového vybavení pracovních stanic smí provádět jen určení administrátoři. Uživatel, který k výkonu funkce potřebuje přidělit nové nebo modernizovat stávající programové vybavení, podá písemnou žádost na OdIT, kde je

zaevidována a po vyřízení archivována. Žádost musí obsahovat přesné označení počítače (číslo záznamníku), stručné zdůvodnění potřeby a podpis vedoucího pracoviště.

Operační systém je dodáván pouze jako „upgrade“ stávajícího! Nová výpočetní technika se nesmí nakupovat bez operačního systému.

5.2. Pořizování programového vybavení

Pořizování programového vybavení pro všechna zařízení v SÍTI FVZ zajišťuje OdIT na základě písemné žádosti podepsané vedoucím pracoviště. OdIT provádí rovněž centrální evidenci veškerého programového vybavení používaného v síti FVZ.

OdIT má právo nepřidělit pracovní stanici licenci programu jestliže:

- cílové zařízení není v materiálové evidenci fakulty;
- přidělení licence by bylo v rozporu s platnými normami, nebo licenčními podmínkami;
- počet licencí u fakulty byl vyčerpán a na nákup nových licencí není dostatek finančních prostředků;
- požadavek není dostatečně zdůvodněný nebo je neúčelný;
- cílové zařízení nesplňuje minimální technické parametry definované výrobcem software.

Individuálně získané programy mohou být na zařízení připojeném do SÍTĚ FVZ instalovány a provozovány jen v souladu se zájmy FVZ, a při respektování této směrnice.

5.3. Evidence programového vybavení

Pracoviště fakulty, která nakoupila software z vlastních prostředků, vyžadují přidělení evidenčního čísla cestou OdIT. K tomu musí uvést zejména tyto údaje:

- přesné označení software včetně čísla verze,
- přesné označení výrobce a dodavatele software,
- kopii faktury a licenčního osvědčení,
- fotokopii potištěné strany instalačního média.

U programového vybavení, které nebylo pořízeno nebo nainstalováno OdIT a není v jeho evidenci, musí uživatel na požádání kontrolních orgánů předložit licenční osvědčení a nabývací doklady (fakturu, dodací list,...). Není-li uživatel schopen tyto doklady předložit, je používání daného software považováno za nelegální se všemi trestněprávními důsledky.

V případě zjištění nelegálního software přijímá pověřený pracovník OdIT účinná opatření k nastolení právního stavu, přičemž má povinnost používání takového software technicky zabránit, nebo jej odinstalovat.

5.4. Správce programového vybavení

Centrální správu programového vybavení u FVZ zabezpečuje OdIT. Ve zvláštních případech může být pro potřeby provádění instalací základního programového vybavení určen lokální správce programového vybavení (dále jen „lokální správce“). Lokální správce může být ustanoven na základě žádosti vedoucího pracoviště, a může jím být jen osoba, která má znalosti a zkušenosti s instalováním programů.

Lokální správce je po proškolení a podpisu „Záznamu o poučení...“ oprávněn provádět instalace a konfigurace základního programového vybavení a ovladačů na přesně vymezeném okruhu pracovních stanic.

Při své činnosti se řídí platnými právními normami, touto směrnicí, licenčními podmínkami výrobců software a pokyny OdIT. Svou činnost může provádět jen na pracovních stanicích v materiálové evidenci příslušného pracoviště. Podmínky instalace určuje a počty licencí přiděluje OdIT.

Lokální správce odpovídá za to, že programové vybavení pracovních stanic pracoviště, pro které je určen správcem, je nainstalováno a používáno v souladu s platnými zákony a licenčními podmínkami.

Provedením instalace přebírá odpovědnost za systémovou funkčnost instalovaného prostředku a k němu připojených periférií včetně použitých ovladačů.

Lokální správce je povinen:

- dodržovat platné právní normy a licenční podmínky výrobců software,
- sledovat změny v licenční politice výrobců software, a v platné legislativě
- dodržovat počty přidělených licencí,
- zpracovávat měsíční souhrny nových instalací a předávat je na OdIT,
- při instalaci operačního systému nastavit dohodnuté heslo lokálního administrátora a toto nikomu nesdělovat,
- instalovaný prostředek připojit do domény a umožnit prosazení doménové, bezpečnostní politiky.

Lokálnímu správci je zakázáno:

- provádět instalace na počítače, které nejsou v materiálové evidenci příslušného pracoviště,
- překračovat počty přidělených licencí,
- vytvářet kopie instalačních souborů,
- sdělovat instalační údaje a poskytovat instalační média jiným osobám, nebo tato média vynášet mimo pracoviště,
- při zřizování uživatelských účtů přidělovat uživateli práva lokálního administrátora.

5.5. Audit

V nepravidelných intervalech provádí OdIT audit nainstalovaného programového vybavení. Na základě vyhodnocení záznamů řeší OdIT zjištěné nedostatky v souladu s touto směrnicí.

6. BEZPEČNOST SÍTĚ

Bezpečnostní politika SÍTĚ FVZ vychází z platných právních norem a předpisů. Dodržování bezpečnostní politiky v SÍTI FVZ prosazuje a kontroluje správce sítě - OdIT.

6.1. Bezpečnost dat

Za bezpečnost a zálohování centrálně uložených dat odpovídá správce sítě.

Zprávy elektronické pošty jsou standardně doručovány do přihrádek na poštovním serveru, kde jsou zálohovány. Uživatel si může nastavit doručování elektronické pošty do lokálně uložených souborů, v tom případě však za ně přebírá odpovědnost. Při havárii pracovní stanice mohou být lokálně uložená data nenávratně ztracena.

Na požádání lze, při respektování technických možností sítě, vytvořit centrální úložiště dat na centrálních prvcích sítě s možností jejich sdílení jednotlivci či skupinami uživatelů. Zálohování takto uložených dat zabezpečuje správce sítě.

6.2. Uživatelská bezpečnost

Každý oprávněný uživatel má přidělený uživatelský účet s jedinečnou identifikací. Uživatel musí držet přihlašovací údaje v tajnosti a smí využívat pracovní stanici pouze k činnosti související s výkonem funkce podle služebního zařazení. Je zakázáno nechávat pracovní stanici volně přístupnou v nezabezpečené místnosti, nebo umožňovat práci v systému jiným osobám.

Uživatel se musí zdržet takového chování, které by mohlo vést k narušení provozuschopnosti nebo bezpečnosti systémů.

Při naléhavé potřebě přístupu ke služebním datům uživatele v době jeho nepřítomnosti může ve výjimečných případech přímý nadřízený uživatele požádat správce sítě o jejich zpřístupnění. Písemná žádost se archivuje na OdIT. V žádosti musí být jasně definována data požadovaná ke zpřístupnění a důvod takového přístupu. Po návratu uživatele jej nadřízený, který žádost podal, o provedeném zásahu informuje.

6.3. Komunikační bezpečnost

SÍŤ FVZ je neutajovaným systémem. Na zařízeních v SÍTI FVZ se mohou zpracovávat, ukládat a distribuovat pouze NEUTAJOVANÁ data. Uživatelům je přísně zakázáno na pracovních stanicích pracovat s daty podléhajícími jakémukoliv utajení, tato data prostřednictvím SÍŤE FVZ sdílet nebo rozesílat.

6.4. Monitorování provozu

Provoz SÍŤE FVZ je monitorován za účelem optimalizace využívání prostředků výpočetní techniky, prevence a detekce poruchových stavů a zamezení neoprávněným přístupům. Všechny pokusy o nepovolenou činnost jsou adresně zadokumentovány a následně řešeny v souladu s touto směrnicí.

6.5. Antivirová ochrana

Každé zařízení v síti je standardně vybaveno předinstalovaným antivirovým programem, který musí být pravidelně aktualizován. Za antivirovou ochranu řídicích prvků sítě a centrálně uložených dat odpovídá OdIT, za antivirovou ochranu pracovní stanice odpovídá uživatel.

Aktivní antivirový program je základní podmínkou připojení zařízení do sítě. Uživatel nesmí antivirovou ochranu svévolně vypínat, omezovat nebo jinak nahrazovat. Rovněž nesmí bránit provádění automatických aktualizací operačního systému.

Instalace a používání nepřidělených, neschválených nebo nevidovaných programů a utilit je **ZAKÁZÁNA!**

Při zjištění virové nákazy musí uživatel okamžitě odpojit počítač od SÍTĚ FVZ. Nepodaří-li se nákazu odstranit antivirovým programem, vypne uživatel počítač a vyžádá standardním způsobem servisní zásah u OdIT.

Je zakázáno provozovat v SÍTĚ FVZ počítače, vykazující znaky virové nákazy. Porušení této zásady může způsobit živelné rozšíření virů na celé segmenty sítě, a proto je kvalifikováno a šetřeno jako bezpečnostní incident.

6.6. Bezpečnostní správci pracovišť

Na jednotlivých pracovištích fakulty jsou, jako pomocný orgán OdIT, ustanovováni bezpečnostní správci. Bezpečnostní správci vedou přehled o používaných pracovních stanicích a dbají o jejich řádnou evidenci a označení. Jsou nápomocni OdIT při řešení bezpečnostně-provozních problémů, provádí bezpečnostní osvětu a dbají na dodržování platných norem a předpisů v oblasti své působnosti. Spolupracují s OdIT při prosazování bezpečnostní politiky a usnadňují komunikaci mezi OdIT a pracovišti.

Podle potřeby je možné, za dodržení podmínek této směrnice, slučovat funkci bezpečnostního správce a správce programového vybavení.

6.7. Porušování pravidel a restrikce

Dodržování pravidel provozu v síti FVZ je jednou ze základních podmínek jejího spolehlivého a bezpečného fungování. Porušování pravidel má za následek omezení uživatelských práv viníka, případně jeho disciplinární nebo jiný postih.

Při zjištění závažného porušení pravidel provozu má správce sítě právo zabránit uživateli v přístupu do sítě, nebo v používání konkrétního zařízení. V krajním případě může do doby vyšetření incidentu zařízení, které bylo předmětem podezřelé činnosti, zajistit.

Podobně se postupuje při zjištění nepovoleného zařízení v síti.

Mezi závažná porušení pravidel patří zejména:

- pokusy o neoprávněný přístup do systému a ke zdrojům sítě, obcházení bezpečnostních funkcí;
- zneužívání software a dat (nepovolené komerční využívání software, neoprávněná manipulace s daty);
- ukládání, instalace, používání nebo šíření nevidovaného programového vybavení;
- poškozování obsahu datových souborů, modifikace programů;
- provádění úprav, poškozování a narušování funkcí hardware;
- používání zavirované pracovní stanice, šíření škodlivých kódů, nebo rozesílání tzv. nevyžádané pošty (SPAMu);
- hrubé nebo opakované porušování pravidel provozu a etických norem.

7. ZÁVĚREČNÁ A PŘECHODNÁ USTANOVENÍ

Tato směrnice nabývá platnosti dnem schválení.

Tato směrnice nahrazuje „Odbornou směrnici pro zřizování a provoz prostředků informatizace v působnosti Vojenské lékařské akademie JEP v Hradci Králové“ ev.č. 19/P z roku 2000, která se tímto ruší.

OBSAH

strana

1. ZÁKLADNÍ USTANOVENÍ	2
1.1. Síť FVZ.....	2
1.2. Služby poskytované sítí FVZ	2
1.3. Účel směrnice.....	2
2. ŘÍDÍCÍ ORGÁN SÍTĚ.....	2
3. ZAŘÍZENÍ V SÍTI FVZ	3
3.1. Tvorba a modernizace pracovišť	3
3.2. Připojení do sítě	3
3.3. Organizace servisní činnosti.....	4
3.4. Použití soukromého počítače	4
3.5. Jmenná konvence	5
3.6. Označení zařízení	5
4. UŽIVATELÉ SÍTĚ FVZ	5
4.1. Zásady používání hesla.....	5
4.2. Založení uživatelského účtu:	5
4.3. Zrušení uživatelského účtu	6
4.4. Uživatel zodpovídá za:.....	6
4.5. Uživatel je povinen:.....	6
4.6. Uživatel nesmí:	6
5. PROGRAMOVÉ VYBAVENÍ.....	7
5.1. Standardní programové vybavení	7
5.2. Pořizování programového vybavení.....	8
5.3. Evidence programového vybavení.....	8
5.4. Správce programového vybavení.....	8
5.5. Audit.....	9
6. BEZPEČNOST SÍTĚ	9
6.1. Bezpečnost dat	9
6.2. Uživatelská bezpečnost.....	10
6.3. Komunikační bezpečnost	10
6.4. Monitorování provozu	10
6.5. Antivirová ochrana	10
6.6. Bezpečnostní správci pracovišť	11
6.7. Porušování pravidel a restrikce.....	11
7. ZÁVĚREČNÁ A PŘECHODNÁ USTANOVENÍ.....	11