ЕВРО БАЛКАН

ЗБОРНИК НА ТРУДОВИ

Прва меѓународна научна конференција
„Влијанието на научно – технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија“

Скопје 20-21 декември 2013

ЗБОРНИК НА ТРУДОВИ: Прва меѓународна научна конференција
„Влијанието на научно – технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија“

Организатор: Институт за дигитална форензика
Универзитет „Евро-Балкан“ - Скопје

Уредник: Проф.д-р Сашо Гелев

Издавач: Универзитет „ЕВРО-БАЛКАН“ Скопје
Република Македонија
www.euba.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

001.3:330/378(497.7)(063)

МЕЃУНАРОДНА научна конференција (1 ; 2013 ; Скопје)
Влијанието на научно-технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија : зборник на трудови / Прва меѓународна научна конференција, Скопје 20-21 декември, 2013 ; [уредник Сашо Гелев]. - Скопје : Универзитет "Евро-Балкан", 2014. - 706 стр. : граф. прикази ; 24 см

Дел од текстот на англиски јазик. - Библиографија кон трудовите

ISBN 978-608-4714-05-7

а) Научен развиток - Општествени науки - Македонија - Излагања на конференции
COBISS.MK-ID 95578634

Програмски одбор

- Проф. д-р Павлина Витанова, ЕВРО-БАЛКАН, копретседател;
- Проф.д-р Сашо Гелев– Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија копретседател
- Проф. Влатко Чингоски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија
- Проф. д-р Лада Садиковиќ, Факултет за криминалистика, криминологија и безбедност, Универзитет во Сараево;
- Проф. д-р Здравко Скакавац, Факултет за правне и пословне студије, Универзитет УССЕ, Нови Сад;
- Проф. Д-р Божо Крстајиќ, Електротехнички факултет - Подгорица, Црна Гора
- Доц. д-р Марјан Николовски, Факултет за безбедност, Универзитет Св. Климент Охридски, Битола, Република Македонија
- Доц. д-р Ненад Танески, Војна академија, Скопје, Република Македонија
- Проф. д-р Гордан Калајџиев, Правен факултет, Универзитет Св. Кирил и Методиј – Скопје, Република Македонија
- Доц. д-р Митко Богданоски, Војна академија Скопје, Република Македонија
- Доц. д-р Роман Голубовски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија
- Проф. Д-р Драган Михајлов, УКИМ; Република Македонија
- Д-р Никола Протрка, Полициска академија, Загреб, Република Хрватска
- Проф. Д-р Тони Стојановски, Австралија
- Д-р Зоран Нарашанов, Винер осигурување, Скопје, Република Македонија
- Проф. Д-р Стефан Сименов, Академија за внатрешни работи на Република Бугарија

Организацискиодбор

- Проф. д-р Сашо Гелев, претседател;
- Проф. д-р Павлина Стојанова, член;
- Проф. д-р Александар Даштевски, член;
- Доц. д-р Вангел Ноневски, член
- Доц. д-р Јорданка Галева
- М-р Славко Гавриловски, секретар;
- Валентина Гоцевска, член;
- Игор Панев, член;
- Ивана Крајчиновиќ, член
- Драгана Каровска, член

Зорица Каевиќ
Студент на втор циклус Ениверзитет Евро-Балкан
zoricakaevikhristova@yahoo.com
Ристо Христов
risto.hristovst@gmail.com
Сашо Гелев
Електротехнички факултет – Радовиш
Универзитет „Гоце Делчев“ – Штип
saso.gelev@ugd.edu.mk
Роман Голубовски
Електротехнички факултет – Радовиш
Универзитет „Гоце Делчев“ – Штип
roman.golubovski@t-home.mk

ХАВАРИЈА И ОЗДРАВУВАЊЕ ОД ХАВАРИЈА НА КОМПЈУТЕРСКИТЕ СИСТЕМИ

Апстракт *– Живееме во време на се` поинтензивен техничко – технолошки развој и примена на автоматска обработка на податоци, речиси да не постои сфера на човечка дејност во која не е навлезен (инволвиран) компјутер или некој од многуте микропроцесори.*
Големата архива на податоци сместени во компјутерските системи, денес ги користат се поголем број на корисници, а поголемите комуникациони компјутерски системи од поодамна ја поминале границата и постанале светски, во повеќето вакви системи безбедноста на истите претставува ограничувачки елемент на понатамошниот развој. Денешното време се смета за ера на информации во која живееме и се карактеризира со масовно комуницирање помеѓу луѓето, бизнис системите, држави и континенти. Писма, книги, дневен печат, телефон, радио, телевизија и други современи средства за комуникација, повеќе пати го забрзале процесот за размена на искуствата, знаењата и идеите. Напредниот процес на комуницирање помеѓу луѓето го поттикнал се побрзиот развој на научни мисли, а со тоа и напредокот на човештвото во целина
Во овој труд ќе биде објаснета методологијата на заздравување на компјутерски систем кој поради било која причина доживеал хаварија.
Колку што ни е познато во Република Македонија се уште никој сериозно не се занимава со проблемот на изготвување на план за реагирање во случај на хаварија, како да се реагира во случај на хаварија во насока на заздравување на оштетениот компјутерски систем, односно намалување на штетните последици.
Овој труд нема некои големи научни претензии. Авторите се надеваме дека со него ќе ги анимираат институциите/компаниите сериозно да ја сватат

потребата од постоење на план за заздравување на компјутерскиот/информацискиот систем после хаварија.
Во рамките на овој труд е изработен „План за заздравување на информацискиот систем на Европскиот универзитет Република Македонија – Скопје после хаварија“.
***Клучни зборови** – хаварија на компјутерски системи; Ризици кои доведуваат до „Хаварија на компјутерски системи“; елементи на безбедност на компјутерскиот систем; заштита од ризикот на хаварија; критериум за избор на оптимални мерки за безбедност; обнова на компјутерскиот систем во случај на хаварија.*

Crash and recovery from a crash of the computer systems

***Abstract** - We live in a world of more and more intensive technical-technological development and use of automatic processing of data. There is almost no sphere in the human activity where the computer or one of the many microprocessors isn't involved.*
The big archives of data placed in the computer systems today are being used by a bigger number of users, while the bigger communication computer systems have risen the boundaries recently and become world ones. Concerning these kind of systems, the security of the same represents limiting element of the further development. Todays world is considered for an era of information and is characterised with mass comunication among people, business systems , countries and continents. Letters, books, daily press , telephone, radio , television and other contemporary means of communication, have accelerated the process of exchanging experience, knowledge and ideas.The advanced process of communication among people encouraged the faster development of scientific thinking and by that advancement of the entire humanity.
This labour deals with the methodology of healing (recovering) of the computer system that experienced a crash for any reason.
As we know, in Republic of Macedonia noone seriously deals with the problem of preparation of a plan for reaction in case of a computer system crash, steps that should be taken for recovering of the damaged computer system, i.e. reducung the harmful consequences. We hope that this labour will animated young enthusiasts to enter in these field of research.
***Keywords**– crash of a computer system, risks that lead to a crash of the computer system, elements of security of the computer system, protection from the risks of crash, criteria for election of optimal measures for security, reconstruction of a computer system in case of a crash*

ВОВЕД

Со тек на времето, зависноста од употреба на компјутерите во секојдневните бизнис активности станала императив. Скоро и да не постои организација која претставува исклучок од овој тренд. Во скоро секоја организација, постојат моќни компјутери. Овие компјутери меѓусебно се поврзани во софистицирани мрежи кои обезбедуваат комуникации со другите машини во рамките на фирмата па дури и низ целиот свет. Функциите кои се од витално значење за бизнисот се зависни од достапноста на ваквите мрежи.

Да претпоставиме за момент дека некоја катастрофа извршила удар врз виталните функции на компјутерскиот систем и тие се недостапни со недели. Во ваква ситуација скоро да не е можно да се претпостават штетите кои би настанале како резултат на ваквиот испад. Една поголема катастрофа би можела да нанесе такви штети за да ги прекине виталните функции на компјутерскиот систем од кои зависи успешното деловно работење на фирмата.

Без адекватна согледување на ризиците кои можат да доведат до хаварија, на безбедните елементи кои можат да спречат хаварија или барем да ги ублажат последиците, односно без изготвување на план за реагирање во случај на хаварија, компјутерски систем на фирмата би бил недостапен за подолг временски период. Тоа може да предизвика застој на деловното работење, а во одредени случаи и до пропаѓање на деловниот систем.

Причини кои можат да предизвикат хаварии

Брзиот развој на информатичко-комуникациската технологија овозможи нејзина примена во сите пори од човечката активност, односно нејзина глобализација. Но, нејзината огромна транспарентност, истовремено ја прави и многу ранлива, односно доведува до зголемување на бројот и видовите на ризици кои влијаат на безбедноста на податоците во текот на обработката, чувањето и дистрибуцијата на информациите.

Предусловот за развој на оптимален информациски систем, односно на развојот на неговата безбедност систем е добро познавање на ризиците кои се закануваат на компјутерскиот систем, т.е. доведуваат до создавање на т.н. "**хаварија**" на системот.

Ризиците кои доведуваат до т.н. "**хаварија**" на компјутерскиот систем, можат да се поделат во две групи:

- Ризици кои настануваат како последица од природни појави;
- Ризици кои ги предизвикува човекот со својата активност.

Како последица од природни појави, можат да се појават: оган, чад, загадена околина, прашина, поплава, невреме, земјотрес, гром, струјни

удари, уништување (кршење) на хардверот, дефект при инсталацијата и друго.

Ризици кои настануваат како последица на човечката активност се: саботажа, шпионажа, вандализам, грешки и пропусти, невнимание, замор на операторот, кражба, штрајкови, случајно или намерно предизвикување на дефект на уредот и инсталацијата.

Ризиците може да се класифицираат и според зависно од местото на појавата на ризикот на: надворешни и внатрешни,

Веројатноста од појавата на некои од наведените ризици кои доведувааат до хаварија, зависи од опремата која се наоѓаат во составот на некој компјутерски центар, персоналот и локацијата на тој систем. Така на пример во центрите лоцирани во урбаните средини, поголема е веројатноста на појавата на некои од природните ризици (особено пожар, чад, загадена околина), а и олеснети се условите за смислена саботажа.

Безбедност на компјутерскиот систем

Постојат различни дефиниции на поимот безбедност. Секоја од нив го објаснува од свој аспект. Цениме дека најпотполна дефиниција за безбедност е: “Безбедност претставува множество на мерки насочени за спречување на настанување на појави во системот кои би биле предизвикани со намерна или ненамерна акција, односно со постапки кои можат да го нарушат нормалното и севкупно функционирање на одреден компјутерски систем или други системи со кои функционално е поврзан во една целина”.

Према оваа дефиниција безбедноста на било кој систем се карактеризираат со низа од поголем или помал број параметри. Безбедноста на компјутерските системи се карактеризира со следните параметри:

- Тајност – е право на поединецот и организацијата (сопственикот на податоците и информациите) самиот да одлучи кога, како и која количина на информации може да се пренесе на останатите за користење.
- Заштита – е оневозможување на случајно или намерно откривање или користење на податоци од неавторизирана личност, како и неавторизирана модификација или уништување на истите.
- Сигурност – е зголемување на веројатноста да компјутерскиот систем го работи тоа за што е предвиден.
- Осигурување – е збир на активности и мерки кои се спроведуваат пред и после хаваријата, а со цел намалување на штетата.

2.1 Тајноста на податоците/информациите

Тајноста на податоците/информациите во компјутерските системи можат да се класифицираат во две основни групи: податоци со ограничени можност за дистрибуцијаикористење и јавни податоци".

Во првата група , спаѓаат податоци/информации со следните степени на тајност:

- Државна тајна;
- Воена тајна;
- Строго доверлива информација;
- Доверлива информација;
- Лични податоци;
- Информации за интерна употреба.

Во втората група на јавни податоци/информации со следните степени на тајност:

- Информации кои се даваат по барање;
- Информации кои се нудат.

Заштита од ризикот за хаварија и критериуми за избор на оптимални мерки за безбедност

Компјутерскиот систем е пожелно да има што повисок степен на безбедност. Во таа насока правиме анализа на системот со нагласен акцент на неговите безбедни аспекти. Целта на анализата е изберате такви мерки на безбедност кои го намалуваат ризикот од настанување на "хаварија" , односно да се намалат границите на неговата толеранција а при тоа да се користат минимални издатоци. Постапката се сведува на утврдување на ризикот кој реално постои и истиот да се елиминира или во најлош случај да се минимизира во границата на толеранцијата.

3.1 Улогата и значењето на софтверот во зачувување на податоците од хаварија

Се до крајот на минатиот век хардверот ја имаше доминантната улога во функционирањето, финансиските вложувања и безбедноста на системот. Денес тој тренд рапидно се менува. Софтверот претставува се позначаен фактор во компјутерската обработка на податоци. По својата вредност, комплексност и можностите на софтверот во многу работни системи го надминува хардверот. Особено тоа е изразено во подрачјето на безбедноста.

Улогата на софтверот во рамките на безбедноста се дели на две групи: заштита на самиот софтвер и развој на софтверот за зголемување на безбедноста на комплетниот систем, почнувајќи од хардверот преку оперативниот софтвер, до податоците и медиумите на кои се чуваат податоците.

Значи, кога се говори за безбедносната улога на софтверот се зборува неговата улога за заштита себеси, останатите програми од неовластено користење, злоупотреба или уништување. Но, истовремено и неговата функција е да го штити системот од разни ризици, да ги дијагностицира грешките, да ја зголеми сигурноста на софтверскиот и хардверскиот дел и спречување на создавање на појава на хаварија на системот.

3.2 Безбедносни карактеристики на софтверот

Апликативниот софтвер (софтвер кој корисникот кој сам го развива или купува за своја потреба од производителот на софтвер) обично служи за решавање некои конкретни проблеми на корисникот. Класични примери на апликативен софтвер се книговодствени програми кои го имаат развиено, или услужните книговодствени сервиси, софтверски пакети за продажба и резервација на карти, за инжинерски симулации и пресметки, и др.

Овие програми се многу специфични од аспект на безбедност затоа што тие од една страна претставуваат технологија за работа која е поинаква во однос на останатите. При развој на овие програми, мора да се вгради интерен систем за безбедност кој ќе овозможи контрола на влезните податоци, контрола на пристапот до податоците и програмите, контрола на исправноста на работата на програмата, заштита на тајноста на податоците, зголемување на сигурноста на работата. Наједноставен но и најуспешен начин да се оствари безбедноста, е создавање на генерациски дадотеки "дедо – татко - син", односно формирање **"back up"** – дадотеки со витални податоци заради нивната безбедност во случај на хаварија и други елементи кои ќе овозможат безбедна обработка на податоци и информации.

Овој интерен безбеден систем треба да ги извршува следните контролни функции:

- Контрола на влезни податоци– може да се обезбедат со верификација на везните податоци, со програма за логичка контрола, со проверка на контролен број, контролен паритет и слични методи;
- Контрола на пристапот на податоци– може да се постигне со примена на лозинки со лаберирање на магнетни медиуми, со дефинирање на овластувањата и слично;
- Контрола на исправност на работата на програмата – може да се постигне со помош на контролни листи кои покажуваат статистички податоци на работата на програмата (влезен број на слогови, излезни број на слогови, и број на обработени слогови), со тестирање на резултатот на работата на програмата, паралелна работа на два програми, и споредување на нивните резултати;

- Заштита на тајноста на податоците – може да се изврши со правилна сегментација на податоците, нивно сместување на различни медиуми, екстерни тврди дискови, со одвоено испраќање на вакви сегментирани податоци, делимично шифрирање на податоците и со примена на криптографија при пренос и меморирање на податоците;
- Зголемување на сигурноста на работата при обработка на податоци – може да се постигне со чување на историјата на промена и со обезбедување најмалку три генерации на дадотеки кои се ажурираат;
- Формирање на back up дадотеки – со витални податоци и нивно чување во сигурносни архиви се обезбедува можност за обновување и продолжување со обработка и после поголема хаварија која може да се случи на компјутерскиот систем.

3.3 Дијагностички програми

Во поголемите и модерни компјутерски системи постои посебен систем за следење на работата на компјутерот. Грешките кои се појавуваат во текот на работата се запишуваат и се чуваат за сервисерот кој го одржува системот (OFF – LINE дијагностика). Ваквите системи се состојат од хардверски уреди и софтверски пакети кои ги развил производувачот на компјутери и претставуваат многу силно средство при одржување на компјутерскиот систем и зголемување на сигурноста на компјутерот и во голема мерка влијае со значително намалување на времето потребно за уврдување на грешката и отстранување на хаваријата.

Иако човекот е основен фактор на активности за отстранување на грешки во софтверот, денес на располагање има поголем број на дијагностички и помошни средства. Процесот на дијагностицирање се вика “debugging” и може да се дефинира како постапки со кои се врши детекција, изолација и отстранување на грешките во компјутерскиот систем и воопшто на софтверот.

Постапките во “debugging” се извршуваат во пет фази:

1. Идентификација на типот на грешката;
2. Собирање на информации за видот на грешката;
3. Анализа, информација и изолација на грешката;
4. Употреба на помошни средства;
5. Корекција на програмата и обнова на работатата на системот.

План за обнова на компјутерскиот систем во случај на хаварија

Информацискиот систем е множество од ресурси како што се: луѓе, знаење, програми, податоци, информации, хардвер, комуникациски уреди и линии, енергија, зграда, потрошен материјал, уред за заштита и друго. Сите ресурси не се подеднакво важни, нити еднакво подложни на оштетување. Поради тоа е неопходно при изборот на мерките за заштита да се земат во предвид кои ресурси ги подржуваат кои функции, изложеноста на секој ресурс на потенцијални ризици, подложноста на оштетувања и последици од такви оштетувања.

Критична зависност

Обновата на информацискиот систем, зависи од расположливите минимални ресурси неопходни за неговата работа и функционирање. Оние ресурси кои се апсолутно неопходни за повторно воспоставување на операциите на системот (воспоставување на работа на одредени работни функции) се викаат **“критични ресурски”**, а зависноста од нив **“критична зависност”**.

На критичните ресурси и зависноста на обновата на хаварисаниот систем од нив треба да се посвети посебна грижа за да се обезбеди нивното трајно располагање и брзо отстранување на престанокот на таа расположливост.

4.2 Дефинирање на стратегија

При дефинирање на стратегијата за обнова на работата на системот за автоматска обработка на податоци нереално е да се појде од претпоставка дека може да дојде до целосно уништување на сите ресурси, а со тоа да прекине работата на овие функции на системот. Поради тоа е невозможно да се дефинира само една стратегија со која ќе се врши обнова на компјутерскиот систем, односно потребно е да се дефинира стратегија и за случаи кога ќе дојде до помали оштетувања на системот во односно на целосната неоперативност на системот.

Во таквите случаи можни се следните видови стратегии:

- Стратегија бр. 1, Толеранција на подолг прекин во работата на информацискиот систем;
- Стратегија бр. 2, Заемна помош (екстерен back up);
- Стратегија бр. 3, Центар за вонредна состојба (back up центри);
- Стратегија бр. 4, Еден уред, два или повеќе локации.

Планот за вонредна состојба

Примарна должност на секој информациски систем, особено ако неговата континуирана работа е императив, е да креира план кој ќе обезбеди адекватен одговор во случај на уништување или сериозно оштетување на централниот компјутерски систем.

Овој план за опоравување од катастрофи е базиран на следните претпоставки:

Безбедност на персоналот, безбедност на хардверот, софтерот и други потреби кои произлегуваат од потебите за опоравување.

Кога некој инцидент ќе биде препознаен како катастрофа, ќе се пристапи кон опоравување, по приоритет заснован на нивото на ризик и ќе се активираат ресурсите предвидени за опоравување, како што е назначено во планот за опоравуање од катастрофи.

Зависно од тежината на катастрофата други оддели би можеле да ги модифицираат нивните операции и на тој начин да придонесат во ублажување на падот на перформансите на системот или да обезбедат физичка локација за компјутерските системи до целосно опоравување.

Планот за вондредна состојба треба да содржи две различни групи на активности:

- Мерки кои треба да се преземат пред настанување на хаварија поради зголемување на безбедносниот систем, односно да се намали штетата или да се помогне во процесот да се нормализира;
- Мерки кои треба да се преземат кога ќе се случи хаварија, како да се намалуваат издатоци во нарушување на функцијата на работниот систем на кого му се даваат автоматска обработка на податоци.

Слика 1. Изглед на насловната страна на формуларот за изработка на план за вонредна состојба

Планот за вондредна ситуација да ги содржи следните поглавија:

- Вовед;
- Цели на планот;
- Стратегија;
- Припремни акции;
- Личности;
- Податоци;
- Софтвер;
- Хардвер;
- Комуникации;
- Простор, енергија, вода, клима;
- Снабдување и транспорт;
- Преглед на договорот со кој се обезбедува подршка во вондредни ситуации;
- Сценарио за обнова на системот во случај на хаварија; и
- Прилози.

Вовед

Во воведниот дел, неопходно е да се опише компјутерскиот и да се даде кратка содржина на планот за вондредни ситуации.

Цели на планот

Планот за заздравување од катастрофи ги имаследните цели:

- Опис на акциите кои ќе бидат превземени за да се обезбедат критичните компјутерски сервиси во најкраток можен рок по иницијализација на планот.
- Да се постават критериуми за одлучување за тоа дали системите ќе се постават на алтернативна локација или ќе се изврши поправка на сегашната локација.
- Опис на организационата структура кој треба да го спроведе планот.
- Обезбедување на информации кои се потребни на персоналот за да може да го изведе планот.
- Опис на процедурите и друго што е потребно за опоравувањето.

Стратегија

Се дефинира и опишува стратегијата врз која ќе се врши разработка на планот за работа во вондредни ситуации према упатствата од поглавие 4.2.

Припремни акции

За да се скрати времето потребно за спроведување на планот во вондредни ситуации, потребно е да се преземе цела низа на припремни акции.

Личности

Тие се најважни сегменти од компјутерскиот систем што најчесто доаѓаат до израз во вондредни ситуации. Во случај на хаварија од луѓето се очекува да извршуваат невообичаени задачи, импровизираат, да работат подолго од пропишаното работно време и тоа во стресни услови.

Општи начела за формирање на тимовите кои би учествувале во процесот на опоравување од аспект на нивните квалификации и стручност, кои барања произлегуваат од одговорностите на секој тим за опоравување поединечно. Дефинирање на одговорностите на секој тим поодделно и дефинирање на фазите во кои тимовите се вклучуваат во процесот на опоравување.

Во насока на остварување на овие задачи, најдобро е да се формираат работни тимови, да се дефинираат целите за секој тим, да се одредат членови на тимот, итн. Во најголем број случаеви потребно е да се формираат следните тимови:

- Тим за простор;
- Тим за хардвер;
- Тим за комуникација;
- Тим за системски софтвер;
- Тим за апликационен софтвер;
- Работен тим;
- Тим за припрема на податоци;
- Тим за контрола на податоци и резултати на обработката;
- Снабдување и администрација.

Европски Универзитет
Република Македонија

Факултет за информатика

Состав на тимот за менаџирање на опоравувањето				
Позиција	**Име и презиме**	**Адреса**	**Домашен телефон**	**Мобилен телефон**
Менаџер на опоравувањето	Д-р Тони Стојановски декан	Даме Груев 24	3063 728	078/482-693
Координатор на тимот задолжен за локацијата за опоравување	Д-р Сашо Гелев	АВНОЈ 26/28	2 424 389	078/203-759
Технички координатор	М-р Димитар Младеновски	Јане Сандански 33	2 454 079	078/482-020
Административен координатор	М-р Ивана Атанасова	АСНОМ 24/12	2 440 060	078/227-703
Мрежен координатор	М-р Александар Соколовски	Климент Охридски 12	3 224 333	078/482-200
Апликациски координатор	Ирена Скрческа	БУЛ Србија 34	2 488 456	078/482-36
Координатор на компјутерски операции	Самоил Крстевски	Тетовска 10	3 105 105	077/976-557

Слика 2. Преглед на тимот за извршување на заздравувањето

Софтвер

Во секој компјутерски систем, постојат неколку врсти на софтвер, тоа се: оперативен систем и системски софтвер, разни **"utility"** програми, програмски пакети на независни производувачи на софтвер и апликативен софтвер во сопствениот центар. Во планот е предвиден попис на сите програми. Посебен акцент е потребно да се стави на информациите на кој медиум се чуваат, адресата на медиумот, местото каде се чува медиумот и важноста на програмата (дали е сотавен на минималната софтверска конфигурација за нормална работа на критичките функции на компјутерскиот систем).

Хардвер

Во планот се прави пописот на актуелна компјутерска инсталација со дефинирани карактеристики на поедини врсти на уреди (производувач, капацитет, снага, тип на уредот, година на производство, карактеристики за поврзување и сл). Во пописот е потребно да се потенцира минималната конфигурација која е неопходна за работа на критичните функции.

Комуникации

За нормално функционирање на компјутерскиот систем важен фактор е и системот на комуникации. Затоа и дефиницијата на тој систем во планот е од суштествена важност (компјутерскиот систем најчесто работи во мрежно опкружување). При проектирање на комуникацискиот систем може со адеквантни мерки да се зголеми сигурноста така да во случај на хаварија, обновата на системот да биде побрза.

Простор, енергија, вода, клима

Во овој дел на планот за вондредна ситуација треба да се соберат податоци неопходни за обезбедување на потребниот простор, енергија, водоснабдување, климатизација на просторот и останатите неопходни мерки за работа на компјутерскиот систем.

Снабдување и транспорт

Во случај на природна непогода (невреме), социјални немири, транспортот и снабдувањето мора да бидат лимитиран фактор за работа во компјутерскиот центар.

Преглед на договорот со кој се обезбедува подршка во вондредни ситуации

Во што пократки црти да се даде преглед на договорот и видот на подршка која со наведениот договор е обезбедена.

Сценарио за обнова на системот во случај на хаварија

Најпогодно е во облик на дијаграм да се даде преглед на активности (што се треба да се направи) во случај на хаварија во компјутерскиот центар.

Прилози

Во прилог на планот за вондредна ситуација треба да се најдат:

- Имиња, адреси, домашни телефони на своите работници кои имаат некоја улога во остварување на планот за обнова на системот (Слика 2.). Називи и телефони на сите важни служби од поблиското и подалечното опкружување (пр. противпожана служба, агенција за управување со кризи, Министерство за внатрешни работи, ЕВН, ...). При изработката на овој именик мора да се почитуваат тајноста на личните податоци, и мора да се заштити од неовластен пристап;

- Попис на неопходните стручни знаења (квалификација) на луѓето кои можат да бидат од корист при одвивање на планот за обнова на системот;
- Во оваа датотека треба да се приложат копии на сите договори со кои се обезбедува подршка на другите единици (организации) во случај на вондредна ситуација;
- Преглед на производителите и доставувачие на опрема од референтните листи на опрема која е инсталирана во земјата и странаство.
- Останати прилози.

Како и сето останато што е значајно за безбедноста на компјутерскиот систем, односно информацискиот систем како целина.

Непоходно е планот да се направи во најмалку три примероци од кои еден мора да се смести во сигурносна архива. Многу е значајно да се води сметка за сите постоечки копии на овој план, редовно да се ажурираат промените кои можат битно да влијаат на безбедносниот систем.

Заклучок

Во нашта секојдневна пракса цениме дека изработката на план за заздравување на компјутерскиот / информацискит систем претставува залудно изгубено време, труд, материјални и финансиски ресурси. Цениме дека хаварија ќе се случи на некој друг и дека нам да ни се случи е невозможно. Дури кога хаваријата ќе ја доживееме, утврдуваме дека сме биле во заблуда, бидејќи штетите кои може да настанат со лутањето при обидот за заздравување на хаварисаниот систем (штетите од неработењето на системот) да бидат поголеми од вложувањата во планот. Зборуваме за материјално-финансиските штети, губењето на податоци знае да биде често непроценливо.

Од изнесеното можеме да заклучиме дека мора, секогаш кога се инсталира одреден компјутерски систем, да се направи и посебен план за негово заздравување доколку настане хаварија, како што е (мараката на производителот, опремата и деловите кои го сочинуваат тој систем, софтверот, хардверот, поврзувањето со други системи доколку е поврзан, потребно време за обновување на системот, но пред се лица кои ќе го оспособуваат тој систем, а секој со своја специјалност за одреден сегмент на инсталираниот систем) сето ова претставува безбедносна мерка за самиот компјутерски систем за да може навремено да се реагира при хаварија.

Вакви хаварии во светот на поголеми компании, институции, се познати со тоа што вложуваат во безбедноста на своите компјутерски системи за да ја осигураат својата база на податоци и информации.

Литература

1. M. L. Shooman: Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design, Wiley-Interscience, 2002
2. D. P. Siewiorek, R. S. Swarz: Reliable Computer Systems: Design and Evaluation, Third Edition, A. K. Peters, 1998
3. J.C. Geffroy, G. Motet: Design of Dependable Computing Systems, Kluwer Academic Publishers, Boston, 2002
4. TechRepublic resource Guide: Backup and Recovery guide
5. TechRepublic resource Guide: Disaster planning and Recovery
6. Healthy and Secure Computing: Restoring IT infrastructure (Manual for Disaster Recovery)