ВИСОКОНАДЕЖДЕН ДЕЙТА ЦЕНТЪР ЗА КАРДИОЛОГИЧНИ ДАННИ

Росен Радков¹, Йото Йотов²

¹Катедра „Компютърни науки и технологии“,
Технически университет - Варна

²УНС Кардиология, Катедра по вътрешни
болести, Факултет по медицина,
Медицински университет - Варна

HIGH RELIABILITY DATA CENTER FOR CARDIOLOGY INFORMATION

Rossen Radkov¹, Yoto Yotov²

¹Department of Computer Science and Technology,
Technical University of Varna

²Educational Sector of Cardiology, Department of
Internal Diseases, Faculty of Medicine,
Medical University of Varna

РЕЗЮМЕ

Сърдечната недостатъчност като крайна фаза на всички сърдечни заболявания е проблем, за решаването на който е необходимо лекарят да притежава голям обем информация, свързана със състоянието на пациентите. Централизираната обработка на тази информация изисква създаване на база данни с осигуряване на високо ниво на достъп и непрекъснатост на функционирането, чиято практическа реализация се извършва чрез изграждане на Център за наблюдение на болните със сърдечна недостатъчност. Представя се техническо решение за изграждане на високонадежден дейта център, осигуряващ работата на центъра за наблюдение и са дефинирани данните, които е необходимо да бъдат надеждно събирани, обработвани и съхранявани.

Ключови думи: сърдечна недостатъчност, дейта център, достъпност, надеждност, непрекъсваемост, резервираност

ВЪВЕДЕНИЕ

Дейта центрове (ДЦ) са ядрото на ИТ инфраструктурата (ИТИС) на дадена организация. Основните изисквания, поставяни към тях са свързани с осигуряване на високата им надеждност, достъпност и защита на информацията. Адаптирането на процесите в организацията към изискванията на съвременния свят и тяхното разширяване в съответствие с нейното развитие води до увеличаване на броя на ползвателите на ДЦ и необходимостта да бъдат достъпни 24 часа в денонощието и 365 дни в годината. Прекъсванията в работата на ДЦ или забавяне в осигуряването на предоставяните услуги стават все по-неприемливи събития. От особено важно значение при изграждането на ДЦ е внедряването на решения, осигуряващи непрекъсваемост на работните процеси и тяхното бързо възстановяване след инцидент.

Процесите за обработката, съхранението и опазването на данните, свързани с диагностиката и лечението на хората със сърдечни заболявания и работата на учените работещи в тази насока, из-

ABSTRACT

Heart failure as an end stage to all cardiovascular diseases is a problem the solution to which requires that the physician possess a large volume of information related to the patient condition. The centralized processing of this information necessitates the establishing of a database with a provision of high level access and uninterrupted function. In practice this would be accomplished by the creation of a Center for Monitoring of Patients with Heart Failure. We are presenting a technical solution to the establishment of a high reliability data center ensuring the functioning of the monitoring center. In addition to this we have included a definition of the data, which are to be reliably collected, processed and stored.

Keywords: heart failure, data center, availability, reliability, business continuity, redundancy

INTRODUCTION

Data centers (DC) are the core of the IT infrastructure (ITIS) of a specific organization. The main requirements of them are related to the provision of high reliability, availability and data protection. The adaptation of the processes of the organization to the modern world demands and their expansion in accordance with its progress leads to an increase in the number of DC users and the need for 24/7 access. Interruptions in the functions of the DC or delays in providing services are becoming more and more unacceptable. When establishing a DC, the implementation of solutions ensuring process continuity and quick recovery after an incident is of key importance.

The processing, storing and protecting of data related to the diagnostics and treatment of patients with cardiovascular diseases and to the work of the researchers in that sphere, require the enforcement of solutions for the establishment of a high reliability DC.

PROBLEM DEFINITION

Heart failure (HF) is the end stage of all cardiovascular diseases and the main reason for morbidity and

искват прилагането на решения за изграждане на високонадежден ДЦ.

ДЕФИНИРАНЕ НА ПРОБЛЕМА

Сърдечната недостатъчност (СН) е крайна фаза на всички сърдечни заболявания и главна причина за заболяемост и смъртност. Обществената значимост на СН се определя от мащаба на разпространение, лошото качество на живот, високата смъртност и голямата икономическа тежест за обществото. Тя е сърдечно заболяване с широко разпространение – честотата му сред общата популация над 18 год. е 1-2%, а във възрастовата група над 70 год. достига >10% (1). Данни от Фрамингамското проучване в САЩ показват, че заболяемостта от СН сред бялата раса нараства десетократно от възрастта 25-29 год., когато тя е 0,6-0,8/1000 човекогодини, а във възрастовата група 70-74 год. скача до 8,7 случая на 1000 човекогодини. Това означава 550 000 нови случаи годишно само в САЩ (2). Въпреки напредъка на медицината и развитието на технологиите в лечението на болните със СН, смъртността при тях остава висока. Пет-годишната възрастово-коригирана смъртност е около 50 %, т.е. всеки втори след 5 год. от началото на симптомите на СН няма да е между живите (3). СН е най-честата причина за хоспитализации при пациенти над 65г. възраст (3, 4).

Непрекъснато се търсят начини за справяне с проблема сърдечна недостатъчност и намаляване на лавинообразно нарастващите хоспитализации. Един от методите е чрез разкриване на специализирани амбулаторни клиники или кабинети за проследяване и наблюдение на болни със сърдечна недостатъчност. Грижата след изписването може да се осъществява на три нива: Специализирани амбулаторни клиники за наблюдение и лечение на болни със СН; Домашно базирани структури за наблюдение и мениджмънт; Телемониторирание. Съществуват доказателства за ефективност на амбулаторните клиники за СН в реализацията на комплексните грижи за пациентите (5, 6).

За да се осъществи адекватен контрол е необходимо изграждане на информационна система за поддържане на база данни в Център за наблюдение на болните със СН (ЦНБСН).

Необходимите данни за пациенти със сърдечна недостатъчност, които трябва да бъдат въведени и съхранявани в база данни са:

- Демографски: пол, възраст, населено място (село град, голям град), образование, заетост (пенсионер по болест или по възраст).

mortality. The social significance of HF is defined by its incidence, the poor quality of life, the high mortality rates and the heavy financial burden for the society. This is a widely spread cardiovascular disease – its incidence among the general population under 18 years of age is 1-2% but in the group above 70 years of age it reaches >10% (1). Data from the Framingham Heart Study in the US indicate that the HF morbidity rate among Caucasians increases tenfold from the age of 25-29 years, when it is 0.6-0.8/1000 patient years, up to 8.7/1000 patient years in the 70-74 age group. This means that there are 550 000 new cases annually only in the US (2). Despite the progress in the field of medicine and the advanced technologies applied in the treatment of HF patients, their mortality rate remains high. The 5-year age-adjusted mortality rate is 50%, i.e. every other patient would not survive beyond the 5th year after the occurrence of the symptoms (3). HF is the most common reason for hospitalization of patients over 65 years of age (3, 4).

There is a continuous search for ways to solve the problem with HF and decrease the rapidly increasing number of hospitalizations. One of the methods is through setting up specialized outpatient clinics or offices for follow-up and monitoring of patients with HF. Patient care after discharge is conducted on three levels: Specialized outpatient clinics for monitoring and treatment of HF patients; home-based structures for monitoring and management; and telemonitoring. There is evidence of the efficiency of the outpatient HF clinics in the provision of complex patient care (5, 6).

In order to ensure adequate control, it is necessary to construct an information system for database maintenance in a Center for Monitoring of Patients with HF (CMPHF).

The necessary data about HF patients, which need to be entered and stored in a database are as follows:

- Demographic: gender, age, place of residence (village, town, city), education, occupation (retired due to an illness or old age).
- Disease information: cause (ischemic heart disease, valvular defects, hypertension, congenital heart defects), duration (how long), functional class by the New York Heart Association (NYHA) classification.
- Concomitant diseases: chronic obstructive pulmonary disease, diabetes mellitus, anemia, hypertension, kidney failure, thyroid diseases, etc.
- Clinical examination: initial data about additional heart sounds, bruit, heart rate (HR), blood pressure, edema, body weight, etc.; as well as during the follow-up process, if there is any change.

- Данни за заболяването: причина (исхемична болест на сърцето, клапни пороци, хипертония, вродени сърдечни пороци), давност (от колко време), функционален клас по класификацията на НюЙорската Кардиологична асоциация (New York Heart Association, NYHA)
- Придружаващи заболявания: хронична обструктивна белодробна болест, захарен диабет, анемия, хипертония, бъбречна недостатъчност, заболявания на щитовидната жлеза и др.
- Клиничен преглед: изходни данни за допълнителни сърдечни тонове, шумове, сърдечна честота, артериално налягане, отоци, телесно тегло и др.; същото в хода на наблюдението, ако има промяна
- ЕКГ: изходни данни и след това – ритъм, СЧ, наличие на блокове и т.н. Към този раздел – данни от Холтер ЕКГ мониториране (24-48 ч.), ако е необходимо.
- Ехокардиография: данни за сърдечни размери, функция на лява камера (Фракция на изтласкване), параметри на диастолно пълнене на лява камера, наличие на стенози или регургитации, и др. Всичко това се въвежда изходно и в хода на проследяването.
- Лабораторни изследвания: Кръвна картина, кръвна глюкоза, креатинин, eGFR, йонограма, чернодробни, пикочна киселина, желязо и параметри на желязна обмяна и др. (по преценка). Изходно и в хода на наблюдение.
- Качество на живот: 6-минутен тест с ходене, въпросници за качество на живот – изходно и при проследяване.
- Лечение: вид медикаменти: дози, промяна в дозата; оперативно лечение – дата и вид на операция; приложение на дивайси – пейсмейкъри, устройства за ресинхронизиращо лечение, имплантируеми кардиовертер-дефибрилатори, за последните – данни от записи изходно и при проследяване, по възможност да са 24-часа, 7 дни в седмицата.
- Хоспитализации (приемания в болница): кога, с каква диагноза, какво лечение (ако е известно).
- EKG: initial and subsequent data – rhythm, HR, presence of blocks, etc. To this section belong as well: data from Holter heart monitor (24-48 hrs), if necessary.
- Echocardiogram: data for heart dimensions, left ventricular function (ejection fraction), parameters of the diastolic filling of the left ventricle, presence of stenosis or regurgitations, etc. All this is entered initially and during the follow-up process.
- Laboratory tests: blood count, blood sugar, creatinine, eGFR, ionogram, liver function, uric acid, iron and total iron-binding capacity, etc. (as needed). Initially and during the follow-up process.
- Quality of life: a 6-minute test involving walking, quality of life questionnaires – initially and during the follow-up process.
- Therapy: medicament types: dosage, dosage changes; surgical therapy – date and type of the operation; application of devices – pacemakers, cardiac resynchronization devices, implantable cardioverter defibrillator. For the latter – data from records initially and during follow-up, 24/7, if possible.
- Hospitalizations (hospital admissions): when, with what diagnosis, what kind of therapy (if known).

SUGGESTED SOLUTION

The functional solution involving a DC, needed for the maintenance of the work process of the information system in CMPHF, is built on the basis of the requirements for the management of the specific medical problem and a thorough analysis of such solutions in practice (7-11). As a result, the following requirements of DC have been defined:

- 99.99% availability of DC (duration of compromised function 52 minutes per year);
- Duration of time in which the work process must be restored after a disruption – Recovery Time Objective (RTO) - ≤ 1 hour;
- Acceptable time interval for which data might be lost – Recovery Point Objective (RPO) - ≤ 1 hour.

Regardless of the specific user software, which might be implemented in a CMPHF, having in mind the confidential nature of the information, the need of fast and timely access to it and the continuously increasing volume, the data center maintaining the processes must be a sum of premises, hardware and software components, server roles, services and management procedures as follows:

- Premises with controlled access and air-condi-

ПРЕДЛАГАНО РЕШЕНИЕ

Функционалното решение за ДЦ, необходим за осигуряване на работата на информационната система в ЦНБСН е изградено на базата на изискванията за обслужване на конкретния медицински проблем и обстоен анализ на подобни решения в

практиката (7-11). В резултат са дефинирани следните изисквания към ДЦ:

- достъпност на ДЦ 99.99% (време на неработоспособност 52 минути в годината);
- стойност на времето за възстановяване на работата след инцидент (RTO) - ≤ 1 час;
- допустимия интервал от време, за който ще се загубят данни (RPO) - ≤ 1 час.

Независимо от конкретния потребителски софтуер, който би бил приложен в ЦНБСН, имайки предвид конфиденциалния характер на данните, необходимостта от бърз и навременен достъп до тях и непрекъснато увеличаващия им се обем, дейта центърът, осигуряващ процесите представлява съвкупност от помещения, хардуерни и софтуерни компоненти, сървърни роли, услуги и процедури за управление както следва:

- Помещения с контролиран достъп и осигурена климатизация;
- Един източник на електрозахранване и изградена система за аварийно електрозахранване;
- минимум два доставчика на Интернет;
- Сървър(и) за база от данни;
- Сървър(и) за приложения;
- Файлов сървър(и);
- Пощенски сървър(и);

tioning;

- One source of power supply and available emergency power supply system;
- At least two Internet service providers;
- Database server(s);
- Application server(s);
- File server(s);
- Mail server(s);
- Web server(s);
- Server(s) for identity management;
- Virtualization platform giving the opportunity for optimal use of the hardware resources, easy DC expansion and meeting the requirements for accessibility, RTO, and RPO;
- Components providing protection against data leaks, unauthorized access to them and/or their modification;
- Network infrastructure dividing the traffic into zones;
- Perimeter protection eliminating the undesired breaches and attacks leading to compromised or impossible functioning of ITIS.

The DC architecture has been designed in order to comply with the set requirements for DC availability, the continuous functioning of the applications used in CMPHF and the acceptable data loss in a disaster. It is

Fig. 1. DC architecture including hardware components (ISP – Internet service provider, FW- firewall, NAS – network-attached storage)

- Уеб сървър(и);
- Сървър(и) за управление на идентичностите и достъпа до приложенията;
- Виртуализационна платформа, даваща възможност за оптимално използване на хардуерните ресурси, лесно разширяване на ДЦ и удовлетворяване на стойностите на достъпност, RTO и RPO;
- Компоненти, осигуряващи защита от изтичане на данни, неправомерен достъп до тях и/или тяхната модификация;
- Мрежова инфраструктура, разделяща трафика на зони;
- Защита на периметъра, елиминираща действието на нежелани пробиви и атаки, водещи до затруднена или невъзможна работа на ИТИС.

За удовлетворяване на поставените изисквания за достъпност на ДЦ, непрекъсваемостта на приложенията, използвани в ЦНБСН и допустимата загуба на данни при бедствие е проектирана архитектура на ДЦ, която е представена на Фиг.1.

Отчитайки оценката на риска, за изпълнение на задачите са поставени следните **цели**:

Цел 1. Защита на периметъра - за ограничаване или елиминиране на възможността за проникване на нежелан трафик, вируси, малуер и хакерски намеси от Интернет, както и за филтриране на съдържанието, пренасяно с мрежовите протоколи;

Цел 2. Защита на крайните устройства - за ограничаване или напълно елиминиране на възможността за проникване и разпространение на вируси и малуер, изтичане на информация;

Цел 3. Осигуряване на цялостност, наличност и конфиденциалност на информацията;

Цел 4. Възстановяване на услугите, предлагани от ДЦ до 1 час след бедствие;

Цел 5. Процесът на експлоатация на ДЦ да бъде с приемливо прекъсване на работните процеси.

Архитектурата на проектирания ДЦ се състои от две части – основен и резервен ДЦ. Пасивните и активни апаратни компоненти на основния (активен) ДЦ (Сайт1) са:

- два броя сървъри (SRV1 и SRV2) от среден клас с два процесора, необходимото количество оперативна памет (обикновено 64/128GB), контролер за управление на DAS с възможности за организиране на масив от дискове от ниво минимум RAID 0, 1, 5, четири гигабитови мрежови интерфейса, два захранващи блока, адаптер (HBA) за връзка чрез FC, SAS или iSCSI интерфейси и модул за отдалечено KVM управление;

presented on Fig.1.

Taking into account the risk assessment, the following **aims** have been set in order to fulfil the task:

Aim 1. Perimeter protection – limiting or eliminating the possibility of breaching of unauthorized traffic, viruses, malware and hacker attacks from the Internet, as well as filtering the content transferred with the network protocols;

Aim 2. Endpoint protection – limiting or fully eliminating the possibility of breaching and spread of viruses and malware, and data leak;

Aim 3. Ensuring integrity, availability and confidentiality of the information;

Aim 4. Recovery of the services provided by DC within 1 hour after a disaster;

Aim 5. The process of DC exploitation must be with an acceptable interruption of the work processes.

The architecture of the designed DC consists of two parts – primary and backup DC. The passive and active device components of the primary (active) DC (Site1) are:

- two servers (SRV1 and SRV2) of medium class with two processors, the needed amount of operating memory (usually 64/128GB), a controller for DAS management with options for setting up a disk array with a minimum level of RAID 0, 1, 5, four gigabit network interfaces, two power supply units, host bus adapter (HBA) for a connection through FC, SAS or iSCSI interfaces and a module for remote KVM management;
- storage server (SAN) with 24 HDD bays and capabilities for additional expansion modules, FC, SAS or iSCSI interfaces, and two control units. The number, type and size of the hard drives is defined by the volume of the information, specific for each individual case;
- two firewall devices (FW1 and FW2) of the UTM or NGFW type with options of setting up zones and working in an active/passive mode. It is necessary to have two WAN ports and at least five fully configurable network ports;
- two managed switches for the backbone network (SW1 и SW2) with options of creating virtual local area networks (VLAN). It is not compulsory to provide the option of working in a high-availability (HA) cluster;
- workstations (WS);
- two uninterruptible power supplies (UPS1 и UPS2) with a power of no more than 2000VA and network management interface, enough to ensure the functioning of the servers, firewall, switch and NAS during power surges, deviations of the voltage from the normal values and short-

- сториџ сървър (SAN) с възможност за вграждане на 24 диска и включване на модули за разширение, интерфейси FC, SAS или iSCSI и два управляващи модула. Броят, типът и размерът на дисковете се определя според обема на информацията, характерен за всеки конкретен случай;
- два броя защитни стени (FW1 и FW2) от тип UTM или NGFW с възможности за организиране на зони и работа в режим на активен/пасивен. Необходимо е да имат два WAN порта и поне пет мрежови порта с възможност за конфигурация;
- два броя комутатори за опорната мрежа (SW1 и SW2) с управление и възможности за организиране на виртуални локални мрежи (VLAN). Не е задължително условие възможността за работа в HA клъстер;
- работни станции (WS);
- две непрекъсваеми захранващи устройства (UPS1 и UPS2) с мощност не повече от 2000VA и мрежов интерфейс (LAN) за управление, достатъчно да осигури работата на сървърите, защитната стена, комутатора и NAS при токови удари, отклонение на напрежението от нормалните стойности и кратковременни (до 15 минути) спирания на захранващото ел. напрежение;
- източник на електрозахранване (PNET1) и генератор с мощност 10kW (GEN1).

Пасивните и активни апаратни компоненти на резервния ДЦ (Сайт2) са:

- един брой сървър (SRV4) от среден клас с два процесора, необходимото количество оперативна памет (типично 64/128GB), контролер за управление на DAS с възможност за вграждане на 24 диска и организиране на масив от дискове от ниво минимум RAID 0, 1, 5, четири гигабитови мрежови интерфейса и два захранващи блока и отдалечено KVM управление. Броят, типът и размерът на дисковете се определя според обема на дисковото пространство, необходимо за разполагане на всички виртуални машини;
- защитна стена (FW3) от тип UTM или NGFW с възможности за организиране на зони, с два WAN порта и поне четири мрежови порта, с възможност за конфигурация;
- комутатор (SW3) с управление и възможности за организиране на виртуални локални мрежи (VLAN);
- непрекъсваемо захранващо устройство (UPS3) с мощност не повече от 1500VA и мрежов ин-

term (up to 15 minutes) interruptions of the voltage supply;

- a source of power supply (PNET1) and a generator with a power of 10kW (GEN1).

The passive and active device components of the Backup DC (Site2) are:

- one server (SRV4) of medium class with two processors, the needed amount of operating memory (typically 64/128GB), a controller for DAS management with 24 HDD bays and capabilities of setting up a disk array with a minimum level of RAID 0, 1, 5, four gigabit network interfaces and two power supply units, as well as remote KVM management. The number, type and size of the hard drives is defined by the volume of disc space, needed for the setup of all virtual machines;
- firewall (FW3) of a UTM or NGFW type with options of setting up zones, with two WAN ports and at least four network ports, and a configuration option;
- switch (SW3) with management and options of setting up virtual local area networks (VLAN);
- an uninterruptible power supply (UPS3) with a power of no more than 1500VA and network management interface, enough to ensure the functioning of the server, firewall, and switch during power surges, deviations of the voltage from the normal values and short-term (up to 15 minutes) interruptions of the voltage supply;
- a source of power supply (PNET2) and a generator with a power of 5kW (GEN2).

The system and application software includes the following components:

- hypervisor (VMware, Hyper-V, KVM, Proxmox, XEN, Veeam or another), which allows the setting up of a high reliability cluster with a minimum of three hosts, with options of automating start of a virtual machine on a different host in case of a problem with the one, which has been used up to that moment;
- server operation system (Windows/Linux server) with the following roles: directory service (AD, eDirectory или дпура), file server, DNS, print server, a role for management of privileges and access rights related to the resources as well as options for virtualization;
- operation system of a server type (preferably Linux Server) for MS (mail server), WWW (web server) and DNS roles;
- server operation system (preferably Linux Server) for a device status monitoring system;
- server operation system (preferably Linux Server) for a software for organizing backup/archive

терфейс (LAN) за управление, достатъчно да осигури работата на сървъра, защитната стена и комутатора при токови удари, отклонение на напрежението от нормалните стойности и кратковременни (до 15 минути) спирания на захранващото електрическо напрежение;

- източник на електрозахранване (PNET2) и генератор с мощност 5kW (GEN2).

От гледна точка на системните и приложни програмни средства, конфигурацията включва следните компоненти:

- хипервайзор (VMware, Hyper-V, KVM, Proxmox, XEN, Veeam или друг), който да позволява организирането на високонадежден клъстер от минимум три хоста, с възможности за автоматично стартиране на виртуална машина върху друг хост в случай на проблем с този, върху който се е изпълнявала машината досега;
- операционна система от сървърен тип (Windows/Linux server), със следните роли: директорийна услуга (AD, eDirectory или друга), файлов сървър, DNS, принт сървър, роля за управление на привилегии и права на достъп до ресурсите и възможности за виртуализация;
- операционна система от сървърен тип (за предпочитане Linux Server) за реализиране на роли MS (пощенски сървър), WWW (уеб сървър) и DNS;
- операционна система от сървърен тип (за

copies of the data;

- licensed antivirus system for the server and the workstations with a centralized management console;
- application software with a MySQL/PostgreSQL database or another;
- license for firewall services.

The solution includes the implementation of virtualization with license for a high-reliability host cluster. It is used as a base for the installation and functioning of the following virtual and physical machines:

- virtual servers (vApS1 and vApS2) with AppSRV, DC, DNS and FS roles;
- virtual server (vInS1 and vInS2) with DNS, MS and WWW roles;
- virtual server (vMnS1 and vMnS2) with a Monitor role;
- virtual server (vBcS1 and vBcS2) with a Backup role;
- physical server for virtual structure management (VCenter).

The information, which the CMPHF users utilize, consists of files and databases, which are located on the discs of vApSx and vInSx. The databases related to the management of the systems for information reservation and the device monitoring are situated on the discs of vBcSx and vMnSx, respectively. The topology of the infrastructure including the functional components is shown on Fig.2.

DC functions in the following way:

Fig. 2. DC topology including the functional components

предпочитане Linux Server) за система за мониторинг на състоянието на устройствата;

- операционна система от сървърен тип (за предпочитане Linux Server) за софтуер за организиране на резервните/архивни копия на информацията;
- лицензирана антивирусна система за сървъра и работните станции с централизирана конзола за управление;
- приложен софтуер с база от данни MySQL/PostgreSQL или друга;
- лиценз за защитната стена.

Решението включва прилагане на виртуализация с лиценз за високонадежден клъстер от хостове, на базата на която се инсталират и работят следните виртуални и физически машини:

- виртуални сървъри (vApS1 и vApS2), изпълняващи роли AppSRV, DC, DNS и FS;
- виртуален сървър (vInS1 и vInS2), изпълняващи роли DNS, MS и WWW;
- виртуален сървър (vMnS1 и vMnS2), изпълняващи роля Monitor;
- виртуален сървър (vBcS1 и vBcS2), изпълняващи роля Backup;
- физически сървър за управление на виртуалната структура (VCenter).

Информацията, с която работят потребителите на ЦНБСН, се състои от файлове и бази данни, които се намират на дисковете на vApSx и vInSx. Базите данни, свързани с управлението на системите за резервиране на информацията и мониторинга на устройствата, са разположени съответно на дисковете на vBcSx и vMnSx. Топологията на инфраструктурата, включваща функционалните компоненти, е показана на Фиг.2.

ДЦ функционира по следния начин:

Съхранение и обработка на информацията: Описаната архитектура е ИТ решение с централизирано съхранение и обработка на информацията. Всички файлове, които се ползват от конкретния потребител, както и базите данни на приложните програми се съхраняват на vApS1, vApS2, vInS1 и vInS2. Контролът на достъпа до приложенията и ресурсите се извършва чрез директорийна услуга DC. Профилите на потребителите също се съхраняват на сървъра. По този начин може да се автоматизира решението за създаване на резервни и архивни копия на информацията. Целостта, достъпността и конфиденциалността на информацията се реализират със средствата на сървърната операционна система.

Повишаването на надеждността в ДЦ се осигурява чрез добавяне към Сайт1 на резервен горещ сайт,

Storage and processing of information:

The described architecture is an IT solution with a centralized storage and processing of information. All files, which are used by the specific user, as well as the databases of the application programs are stored on vApS1, vApS2, vInS1, and vInS2. The control of the access to the applications and the resources is conducted by the directory service DC. User profiles are also stored on the server. This way, the solution for the creation of spare and archived copies of the information can be automatized. The integrity, accessibility and confidentiality of the information are provided by means of the server operation system.

The increase of the DC reliability is ensured by the addition of a spare hot site to Site1. It is at such distance from the first one so that it would not be possible for it to be affected by the same destabilizing factors. The backup Site2 has an architecture different from that of Site1 but with the ability to ensure functioning of the CMPHF work processes, if needed. For this purpose, both sites work in an active-passive mode and the files and application databases are periodically replicated or copied from Site1 to Site2. The three hosts – the two from Site1 and the one from Site2, form a cluster, which is managed by a special server - VCenter. In case of an accident, the company work is transferred to Site2 manually. After the restoration of Site1, the work transfer to it is done manually as well. The time and complexity of the transfer from one site to the other depend on the specific applications used and their replication options.

Network traffic control:

It is conducted by a firewall. The network communication is based on TCP/IP protocols. The implementation of a firewall of the UTM or NGFW type gives the opportunity of controlling the traffic at all layers of the communication stack. Both sites are divided into six zones in order to: isolate the workstation in a separate segment (zone1 LAN); isolate MS and WWW in a separate segment (zone2 DMZ); isolate the application and monitoring servers in a separate segment (zone3 Servers); isolate the backup server and NAS in a separate segment (zone4 Backup); control and analyze (IPS, IDS, Application control, Content filtering) the traffic from the workstations to vApS, vInS, and the Internet. On the basis of the set rules, FW gives the servers access only to the needed services; controls the traffic from vApS to NAS; bans the access from the Internet zone to the LAN, Servers and Backup zones. This way unrequested traffic from the Internet zone can only end up in the DMZ zone where the publicly accessible servers are connected. The traffic between the zones is regulated so from the LAN zone only al-

който е на такова разстояние от първия, че да не е възможно да бъде засегнат от същите дестабилизиращи фактори. Резервният Сайт2 е с архитектура, различна от тази на Сайт1, но с възможност да осигури работата на работните процеси в ЦНБСН при необходимост. За тази цел двата сайта работят в режим активен-пасивен, като файловете и базите данни на приложенията се репликират или копират периодично от Сайт1 към Сайт2. Трите хоста-двата от Сайт1 и този от Сайт2, образуват клъстер, който се управлява от специален сървър - VCenter. В случай на инцидент, работата на фирмата се прехвърля към Сайт2 ръчно. След възстановяване на Сайт1, прехвърлянето на работата към него става отново ръчно. Времето и сложността на прехвърлянето от единия сайт към другия зависи от конкретните приложения, които се използват и вградените в тях възможности за репликация.

Контрол на мрежовия трафик:

Постига се с помощта на защитната стена. Комуникацията в мрежата е базирана на TCP/IP протоколи. Прилагането на защитна стена от тип UTM или NGFW дава възможност да се контролира трафика на всички нива от комуникационния стек. И в двата сайта се прави разделяне на шест зони, за да се: изолират работните станции в отделен сегмент (зона1 LAN); изолират MS и WWW в отделен сегмент (зона2 DMZ); изолират сървърите за приложения и мониторинг в отделен сегмент (зона3 Servers); изолира сървърът за резервните/архивни копия на информацията и NAS в отделен сегмент (зона4 Backup); управлява и анализира (IPS, IDS, Application control, Content filtering) трафикът от работните станции към vApS, vInS и Интернет. На базата на създадени правила, FW пропуска към SRV само необходимите услуги; управлява трафика от vApS към NAS; забранява достъпа от зона Интернет към зони LAN, Servers и Backup.

lowed traffic is permitted just to the Servers zone and the communication with NAS is permitted only from vApS.

The communication between both sites is organized through four VPN tunnels.

Data replication:

The files and the databases of vApS and vInS are replicated by means of application programs or databases. Depending on latency of the Internet connection between both sites, an asynchronous or synchronous replication can be made. In asynchronous replication the usual interval in which the data is replicated is at least 15 minutes and in the synchronous one – close to 0.

Creating backup/archive copies of data:

This is performed via a server, which provides means for creating automatized tasks and managing the process of their fulfilment, functions for restoring a virtual machine or a specific file or folder. Adhering to the DC requirements, each work day the following tasks are initiated: by schedule, each day, at a specific time, usually after working hours, the creation of a spare copy of each of the virtual machines starts automatically; the backup copies of the configurations of the VCenter server, firewalls and switches are done manually if any changes are made.

In order to provide the opportunity for system restoration in case of a disaster, which may lead to a damage to the NAS device or the information it contains, a cloud service (Cloud Backup) is used for information reservation.

RESULTS

According to the described above way of functioning, the DC needed for the purposes of a CMPHF with the proposed architecture is in compliance with two of the given indicators RTO and RPO. The third especially

Fig. 3. Decomposed DC structure

По този начин непоискан трафик от зона Интернет може да попадне само в зона DMZ, където са свързани публично достъпните сървъри. Трафикът между зоните е регламентиран, така че от зона LAN се допуска само разрешен трафик само до зона Servers, а комуникация с NAS е разрешена само от vApS.

Комуникацията между двата сайта е организирана чрез четири VPN тунели.

Репликиране на информацията:

Файловете и базите данни на vApS и vInS се репликират чрез средствата на приложните програми или базите данни. В зависимост от латентността на Интернет свързаността между двата сайта се прави асинхронна или синхронна репликация. При асинхронната репликация обичайния интервал, през който се репликират данните е минимум 15 минути, а при синхронната – близко до 0.

Създаване на резервни копия и архивиране на информацията: Решението се реализира чрез сървър, който предоставя средства за създаване на автоматизирани задачи и управление на процеса на изпълнението им, функции за възстановяване на виртуална машина или съответен файл или фолдер. Спазвайки изискванията към ДЦ всеки рабо-

important indicator – its availability (A), can be calculated by creating a reliable structure of DC (12). It can be presented as consecutive connection of components with a series, parallel, parallel-series or series-parallel structures (Fig. 3).

The decomposed structure of DC consists of three branches – a main one and two supplementary ones. Each of them is replicated. The main branch (PNETx/GENx÷InSx) includes the components of the function on which depends the completion of the business processes in CMPHF. The second (PNETx/GENx÷vMnSx) and the third (PNETx/GENx÷NASx÷Cloud) one include the components forming the work processes related to system monitoring and information reservation. A malfunction in the supplementary branches increases the risk of missing an event or an improper procedure of information reservation but does not lead to an interruption of the work processes. Therefore, the calculation of the availability of ITIS is done on the basis of the availability of main branch sections and is presented in Table 1.

It is evident from the calculation that the proposed DC is in compliance with the third indicator for DC reliability as well since the calculated availability is

Table 1. Availability of DC components

Component	MTBF (hour)	MTTR (hour)	A _i	Calculating Availability	A
PNET1	-	-	0.998000	1-(1-A _{PNET})*(1-A _{GEN})	0.999997
GEN1	14 000	24	0.998288		
UPS1 & UPS2	785 000	72	0.999908	1-(1-A _{UPS} *A _{FW} *A _{SW} *A _{ISP})^2	0.999992
FW1 & FW2	516 840	72	0.999860		
SW1 & SW2	516 840	72	0.999860		
ISP1 ^ISP2	-	-	0.997500		
SRV1 & SRV2	100 000	72	0.999280	1-(1-A _{SRV1})*(1-A _{SRV2})	0.999999
SAN	2 000 000	72	0.999964	A _{SAN}	0.999964
SRV3	70 000	72	0.998972	A _{SRV3}	0.998972
HV	-	-	0.999999	A _{HV}	0.999999
OS vInS, vApS	-	-	0.999999	A _{OS} ^2	0.999998
App vInS, vApS	-	-	0.999999	A _{APP} ^2	0.999998
Site1 Accessibility					0.998920
PNET2	-	-	0.998000	1-(1-A _{PNET})*(1-A _{GEN})	0.999997
GEN2	14 000	24	0.998288		
UPS3	785 000	72	0.999908		0.999908
FW3	516 840	72	0.999860		0.999860
SW4	516 840	72	0.999860		0.999860
SRV4	100 000	72	0.999280	A _{SRV3}	0.999280
(HV	-	-	0.999999	A _{HV}	0.999999
OS vInS, vAp)	-	-	0.999999	A _{OS} ^2	0.999998
App vInS, vApS	-	-	0.999999	A _{APP} ^2	0.999998
ISP3 & ISP4	-	-	0.997500	1-(1-A _{ISP3})*(1-A _{ISP4})	0.999994
Site2 Availability					0.998894
DC Availability: 1-(1-A_{site1})*(1-A_{site2})					0.999999

тен ден се стартират следните задачи: по създаден график всеки ден в определен час, обичайно след края на работния ден, автоматично се стартира създаване на резервно копие на всяка една от виртуалните машини; резервни копия на конфигурациите на VCenter сървър, защитната стена и комутатора се правят ръчно при промени в тях.

За да бъде осигурена възможността за възстановяване на системата в случай на бедствие, в резултат на което е повредено NAS устройството или информацията в него, се използва облачна услуга за резервиране на информацията Cloud Backup.

ПОСТИГНАТИ РЕЗУЛТАТИ

Съгласно описания по-горе начин на работа, ДЦ необходим за работата на ЦНБСН с така предложената архитектура удовлетворява два от зададените показатели RTO и RPO. Третият особено важен показател – достъпността (A) му, може да бъде изчислена чрез създаване на надеждна структура на ДЦ (12). Тя може да се представи като последователно свързване на последователни, паралелни, паралелно-последователно и последователно-паралелно свързани компоненти (фиг. 3).

Декомпозираната структура на ДЦ се състои от три клона – основен и два спомагателни, всеки един от които е дублиран. Основният клон (PNETx/GENx÷InSx) включва компонентите, от работата на които зависи изпълнението на бизнес процеси във ЦНБСН. Вторият (PNETx/GENx÷vMnSx) и третият (PNETx/GENx÷NASx÷Cloud) включват компонентите, формиращи служебните процеси по мониторинг на системата и резервиране на информацията. Повреда в спомагателните клонове увеличава риска да се пропусне събитие или да не се изпълни правилно процедурата за резервиране на информацията, но не предизвиква прекъсване на работните процеси. Затова изчисляването на достъпността на ИТИС се изчислява на база на достъпността на отделни само за основния клон и е представено в Таблица 1.

От направеното изчисление се вижда, че предложеният ДЦ удовлетворява и третият заложен показател за надеждност на ДЦ, тъй като изчислена та достъпност е 99.9999%.

ЗАКЛЮЧЕНИЕ И ИЗВОДИ

Справянето с проблема сърдечна недостатъчност изисква индивидуално постоянно и дългосрочно наблюдение на редица клинични, лабораторни и инструментални параметри. Проследяването на

99.9999%.

CONCLUSION

Solving the problem with heart failure requires continuous individual and long-term follow-up of multiple clinical, laboratory and instrumental parameters. The patient follow-up will be more successful if a Center for Monitoring of Patients with HF is established, which will allow more thorough monitoring of a larger number of patients but also an easier way to analyze the applied therapies.

The successful functioning of CMPHF depends on the provision of reliable processing, storage and reservation of cardiology data. The presented solution guarantees the needed availability of DC at 99.99% (fifty-two minutes per year) and an acceptable data loss. It is constructed via designing an architecture with high-reliability and applying modern IT solutions. The maintenance of the hardware and the software of DC is performed without interrupting the work processes in CMPHF. There are possibilities for an easy expansion of DC in case of an increase in the work volume and the processed data.

Address for correspondence:

Rossen Radkov
Department of Computer Science and Technology
Technical University of Varna
1 Studentska St
9010 Varna
Bulgaria
e-mail: rossen@actbg.bg

REFERENCES

1. Mosterd A, Hoes AW. Clinical epidemiology of heart failure. *Heart*. 2007;93: 1137-46.
2. Dickstein K, Cohen-Solal A, Filippatos G, McMurray JJ, Ponikowski P, Poole-Wilson PA, et al. ESC Guidelines for the diagnosis and treatment of acute and chronic heart failure 2008: the Task Force for the Diagnosis and Treatment of Acute and Chronic Heart Failure 2008 of the European Society of Cardiology. Developed in collaboration with the Heart Failure Association of the ESC (HFA) and endorsed by the European Society of Intensive Care Medicine (ESICM). *Eur Heart J*. 2008; 29: 2388-442.
3. Hunt SA, Abraham WT, Chin MH, et al. 2009 focused update incorporated into the ACC/AHA 2005 guidelines for the diagnosis and management of heart failure in adults: a report of the American College of Cardiology Foundation/American Heart Association Task Force on Practice Guidelines. *J Am Coll Cardiol*. 2009;53:e1-90.

болните ще е бъде по-успешно, ако бъде изграден Център за наблюдение на болните със СН, чрез който не само ще бъдат обстойно наблюдавани голям брой пациенти, но и по-лесно ще бъдат анализирани прилаганите терапии.

Успешната работа на ЦНБСН е зависима от осигуряването на надеждна обработка, съхранение и резервиране на кардиологичните данни. Представеното решение гарантира необходимата достъпност на ДЦ 99,99% (петдесет и две минути на година) и приемлива загуба на данни и е изградено чрез проектирана високонадеждна архитектура и прилагане на съвременни ИТ решения. Извършването на профилактика на апаратната и програмна част на ДЦ се извършва без прекъсване на работните процеси в ЦНБСН. Предвидени са възможности за лесно разширение на ДЦ, в случай на увеличаване на обема на работата и обработваните данни.

Адрес за кореспонденция:

Росен Радков
Катедра „Компютърни науки и технологии“
Технически университет - Варна
Ул. „Студентска“ 1
9010 Варна
e-mail: rossen@actbg.bg

4. Alla F, Zannad F, Filippatos G. Epidemiology of acute heart failure syndromes. *Heart Fail Rev.* 2007; 12: 91-5.
5. Savard LA, Thompson DR, Clark AM. A meta-review of evidence on heart failure disease management programs: the challenges of describing and synthesizing evidence on complex interventions. *Trials.* 2011, 12:194
6. Rich MW, Beckham V, Wittenberg C et al. A multidisciplinary intervention to prevent the readmission of elderly patients with congestive heart failure. *N Engl J Med.* 1995, 333: 1190-1195
7. BDS ISO/IEC 27001. Bulgaria, 2005, p. 30.
8. ANSI/TIA, TIA-942-A Telecommunications Infrastructure Standard for Data Centers, no. March. USA, 2005, p. 120
9. ANSI/BICSI, ANSI/Bicsi 002. 2011
10. Julio P. Designing an IT solution. 2011. [Online]. Available: <https://www.slideshare.net/PhilippeJulio/infrastructure-design-en>.
11. EU, “Unified state requirement to the setting up and certification of centers for storage of especially sensitive information for the needs of the central state administration in compliance with the requirements of BDS ISO/IEC 27001:2005,” 2011 (in Bulgarian).
12. Antonov P, Radkov R. Analysis of reliable characteristics of highly reliable data centers. *Comp Sci Technol.* 2011; 9(1):43-9 (in Bulgarian).