РЕЗЮМЕТА

на научноизследователските трудове на гл. ас. д-р инж. Росен Стефанов Радков
представени за участие в конкурс за академична длъжност „доцент“ в професионално направление 5.3 „***Комуникационна и компютърна техника***“ за учебна дисциплина „***Компютърни мрежи и интернет***“ към катедра „***Софтуерни и интернет технологии***“ при „***Факултет по изчислителна техника и автоматизация***“, обявен в ДВ бр. №65/06.08.2021 г.

За участие в конкурса са представени **23** (двадесет и три) научни труда, представляващи хабилитационен труд – монография, публикации в научни списания и публикувани доклади, изнесени на научни форуми и ръководство за лабораторни упражнения по дисциплината „Интернет сървъри и услуги“.

Научните публикации са разделени в три групи, в съответствие с показателите **В.3, Г.7** и **Г.8** от документ „***5. Подробна справка за изпълнение на минималните национални изисквания***“.

Показател Г.7 включва **4** (четири) научни публикации в издания, които са реферирани и индексирани в базата данни с научна информация ***Scopus***, от които **2** (две) са самостоятелни. Публикациите са разпредени в следните групи:

- Публикации в сборници с доклади в България, реферирани в ***Scopus*** – **4**;

Показател Г.8 включва **17** (седемнадесет) научни публикации в нереферирани списания с научно рецензиране или в редактирани колективни томове от които **14** (четиридесет) са самостоятелни.

Според вида на изданието, публикациите са разпредени в следните групи:

- Публикации в списания, издавани в България – **8**;
- Публикации в сборници с доклади в България – **6**;
- Публикации в сборници доклади в чужбина – **3**;

Според тематиката, общият брой публикации се разпределят в следните групи:

- Проектиране и оценка на надеждността и качеството на дейта центрове – **11**
- Компютърни науки – **4**
- Сигурност на информацията, защита на личните данни и системи за управление на сигурността на информацията – **6**
- Електронно обучение – **1**

По език на публикуване:

- На български език – **14**
- На английски език – **8**

[Показател В.3] Хабилитационен труд – монография

[В.3] Радков, Росен. Непрекъснатост на сигурността на информацията. Анализ и подходи за управление. Варна, ТУ-Варна. **2021**. 130 стр. ISBN:978-954-20-0828-6

В монографичен труд са изяснени същността на понятията информация и данни, както и тяхната важност както за организациите, така и за частните лица. Изяснени са принципите, които трябва да се следват, за да се гарантира сигурност на информацията. Направено е изложение на аспектите, свързани с осигуряването на непрекъснатостта на бизнес процесите и сигурността на информацията, която се обработва в тях. Обоснована е необходимостта от въвеждане на система за управление. Описани са нормативните документи, които регламентират изискванията към системите за управление на сигурността на информацията, чрез внедряването на които се гарантира сигурността на информацията и нейната непрекъснатост. Изяснена е същността на системите за управление и е обобщена информацията, свързана с тяхното сертифициране в съответствие на международните стандарти.

На базата на проведени одити в различни организации е направен анализ на управлението на непрекъснатостта на сигурността на информацията при извършване на дейностите в тях. В резултат на извършения анализ са изведени следните заключения:

1. Внедряването на СУСИ в съответствие с изискванията на стандарт ISO/IEC 27001 е препоръчително, тогава когато дадена организация иска да подобри управлението на сигурността на информацията, но не е достатъчно, ако не се вникне достатъчно дълбоко в неговите изисквания, както и в същината и особеностите на прилаганите технологии;

2. Стандарт ISO/IEC 27001 е добре приет във всички стопански сектори

3. Не се различава процеса на управление на непрекъснатостта на сигурността на информацията, независимо от какъв тип (частен, колокиран или нает) е ДЦ, заложен в архитектурата на корпоративната ИТИС;

4. Констатирани са сериозни слабости в процеса на анализ на въздействието върху бизнеса, в частност върху сигурността на информацията, което се отразява съществено на планирането и управлението на сигурността на информацията и като следствие – на гарантирането на нейната непрекъснатост;

5. Констатирани са слабости в планирането и изпълнението на процеса на възстановяване на информацията при инцидент. Анализирани са процесите на планиране и поддържане на процеса за непрекъснатост на сигурността на информацията.

Създаден е подход, подпомагащ процеса на създаване на ПНВБ и целящ отчитане на всички обстоятелства и особености, които допринасят за създаване на качествен ПНВБ. Представеният подход е универсален и може да се използва както за целите на подпомагане на процеса за управление на непрекъснатостта на сигурността на информацията, така и при управление на непрекъснатостта на дейността. Предложеният подход е адаптиран за практическо приложение.

[Показател Г.7] Научни публикации в издания, които са реферирани и индексирани в световноизвестни бази данни с научна информация.

[Г.7.1] **Radkov R**., An approach to choosing an optimal IT infrastructure in accordance with an assignor's requirements, 2018 20th International Symposium on Electrical Apparatus and Technologies (SIELA), 3-6 June **2018**, Bourgas, Electronic ISBN: 978-1-5386-3419-6, USB ISBN: 978-1-5386-3418-9, Print on Demand (PoD) ISBN: 978-1-5386-3420-2 DOI: 10.1109/SIELA.2018.8447081 (Scopus)

AN APPROACH TO CHOOSING AN OPTIMAL IT INFRASTRUCTURE IN ACCORDANCE WITH AN ASSIGNOR'S REQUIREMENTS

Rosen Radkov

В доклада е представен разработен от автора подход за избор на оптимална ИТ инфраструктура въз основа на изискванията на възложител. Необходимостта от създаване на подход е породена от това, че въпреки съществуването на международни и утвърдени национални стандарти за структурата, проектирането и работата на центровете за данни (ДЦ) и техните ИТ инфраструктури (ИТИС), които се прилагат успешно в при проектирането и внедряването на големи центрове за данни, то при организациите от тип микро-, малко или средно предприятия има затруднения при определянето на ИТИС на ДЦ, от който се нуждаят. Няма унифициран подход, въз основа на който те да могат да оценят предлаганите им решения и да вземат обосновано и адекватно на техните нужди решение за състава на ИТИС на своя ДЦ, което да бъде приложено.

Представеният подход решава задачата за оценка на качеството на ДЦ и избора на подходящата ИТИС в съответствие с изискванията на възложителя. За тази цел се използва набор от предварително разработени еталонни ИТИС. Извършва се оценка на тяхното качество чрез изчисляване на шест показателя, които са обосновани като най-важни. Необходимо е възложителят да определи желаните от него стойности на шестте показателя, както и техните коефициенти на значимост. Следваща стъпка в подхода е за се определи „идеална ИТИС", която притежава най-добрите стойности на показателите. За всички ИТИС, еталонните, идеалната и тази на възложителя, се определя комплексен показател на качество използвайки формулата за комплексен геометричен показател. В резултат от работата на подхода е избор на една от еталонните ИТИС като най-подходяща за възложителя. Това е тази еталонна ИТИС, чиято стойност на комплексния показател е най-близка, но по-голяма, от стойността изчислена за желаната от възложителя ИТИС. При отрицателна разлика е необходимо да се направи промяна във входните параметри и да се повторят изчисленията.

Подходът е адаптиран за практическо приложение. Разработени са софтуерни инструменти за неговото приложение. Няма ограничение за броя на предварително дефинираните еталонни ИТИС. Използван е при проектирането на седем центрове за данни.

Естеството на използваните показатели е такова, че всеки бизнесмен или мениджър на организация може без затруднение да ги идентифицира, без да са необходими технически познания.

Подходът може да се прилага не само при проектирането на високо надежден център за данни, но и при оценка на качеството на съществуващ център за данни.

[Г.7.2] Radkov R., Dimitrov I., Are Disaster Recovery Levels sufficient to assess the Data Center's disaster preparedness? ET2018 13-15.09.**2018**, Sozopol, Electronic ISBN: 978-1-5386-6692-0, CD-ROM ISBN: 978-1-5386-6691-3, Print on Demand(PoD) ISBN: 978-1-5386-6693-7, DOI: 10.1109/ET.2018.8549602 (Scopus)

ARE DISASTER RECOVERY LEVELS SUFFICIENT TO ASSESS THE DATA CENTER'S DISASTER PREPAREDNESS?

Rosen Stefanov Radkov and Ivan Dimitrov Dimitrov

Съвременният свят е силно зависим от информационните технологии за управление на бизнес процесите в компаниите, в държавната и местна власт, здравеопазването, образованието и дори за осигуряване на комфорт в дома. От изключителна важност за всяка организация е да осигури непрекъснатост на нейната работа и бързо възстановяване след бедствие. Съществуват класификации за оценка на нивото на ИТ инфраструктурите според техните възможности за възстановяване при бедствия.

В този доклад авторите правят критичен анализ на тези класификации и доказват, че те са остарели и недостатъчни, за да се определи дали са покрити рисковете, свързани с работата на ИТ инфраструктури. Предлага се включването на допълнителни показатели в оценката на устойчивостта на ИТ инфраструктурите срещу бедствия, които отчитат не само техническите решения, прилагани в ИТ инфраструктурите, но и организационни аспекти, като организацията на нейната експлоатация, разделянето на задълженията както и необходимостта от по-честото актуализиране на подхода за оценка, за да се вземат предвид новите технологии промените в заобикалящата среда и новите заплахи за функционирането на ИТ инфраструктура.

[Г.7.3] Radkov R., Reference Highly Reliable IT Infrastructures for the Micro, Small and Medium Sized Companies ET2018 13-15.09.**2018**, Sozopol, Electronic ISBN: 978-1-5386-6692-0, CD-ROM ISBN: 978-1-5386-6691-3, Print on Demand (PoD) ISBN: 978-1-5386-6693-7, DOI: 10.1109/ET.2018.8549601 (Scopus)

REFERENCE HIGHLY RELIABLE IT INFRASTRUCTURES FOR THE MICRO-, SMALL- AND MEDIUM-SIZED COMPANIES

Rosen Stefanov Radkov

Проектирането на дейта център е сложна задача. Когато е необходимо да се проектира дейта център за нуждите на фирми от тип микро, малък и среден бизнес се среща трудност при избор на подходящия за целта дейта център.

Настоящият доклад представя три еталонни ИТ инфраструктури (ИТИС) с висока надеждност, които се използват в подход разработен от автора (публикуван в друг доклад), чрез който се прави обоснован избор на оптимална ИТ инфраструктура по задание от възложител. Представят се изчислените стойности на единичните им показатели за качество.

Разработените еталонни ИТ инфраструктури са с висока надеждност, което се доказва от стойностите на изчислените единични показатели за качество за всяка една от тях. Дефинирани са целите, които трябва да бъдат постигнати със съответната ИТИС. Всяка една от тях е съвкупност не само от апаратни и програмни средства, но и от организационни мерки, които регулират управлението на ДЦ и сигурността на информацията. Без тези организационни мерки стойностите на някои от единичните показатели за качество ще бъдат по-лоши.

Разработените еталонни ИТИС могат да се използват не само в разработения от автора подход за избор на оптимална ИТИС по задание на възложител, но и като ръководство за изграждане на високонадежден ДЦ. В зависимост от особеностите на съответния проект на базата на една и съща ЕИТИС могат да се получат реализации с прилагане на различни хардуерни и софтуерни компоненти.

[Г.7.4] Radkov R., D. Vankova, Z. Radkova, Y. Petkova, "E-learning in a COVID-19 context - epidemiological and educational challenges," ICAI 2020 01-03.10.**2020**, Varna, DOI: 10.1109/ICAI50593.2020.9311307 (Scopus)

E-LEARNING IN THE COVID-19 CONTEXT - EPIDEMIOLOGICAL AND EDUCATIONAL CHALLENGES

Radkov Rosen Stefanov, Radkova Zhaneta Grigorova, Vankova Desislava Ivanova, Petkova Yulka Petkova

Технологиите трансформират образованието постепенно и завинаги. Пандемията на коронавируса създаде редица предизвикателства във всички области на живота. За разлика от нормалната еволюция, коронавирусът (COVID-19) наложи промени в образованието внезапно и временно (ако приемем). По-специално, продължаващо образование в дистанционна форма, в условия на социална изолация. Въпреки това, пандемичният контекст улесни по-широкото въвеждане на технологии в консервативната академична среда в България.

В доклада се анализират както социални, така и учебни проблеми в контекста на COVID-19. Предизвикателствата в електронното обучение се разглеждат от обективна и субективна гледна точка, както и от технологична гледна точка. Представени са добри примери от практиката за справяне със ситуации в зависимост от спецификата на изучаваните дисциплини. Представени са някои предложения за изграждане на подходяща инфраструктура за целите на електронното обучение. Освен това са дадени примери в академичните области на компютърните науки и общественото здраве.

Докладът посочва и отговаря на следните изследователски въпроси: Какво е различното в електронното обучение в контекста на пандемията 2020? С какви проблеми и предизвикателства се сблъскахме? Как да подобрим електронното обучение и да облекчим щетите от социалната изолация? Общата цел на тази статия е да класифицира и анализира предизвикателствата за е-обучение в контекст на COVID-19 и да предложи решения.

Идеята на настоящата дискусия е да популяризира и подкрепи устойчивата интеграция на цифровите технологии в българските колежи и университети. Авторите са университетски преподаватели и трябва да се справят ежедневно с възникващите образователни предизвикателства. Следователно предложените стратегии са ориентирани към практиката. Развитието на технологичната грамотност се превърна не само в лична отговорност, но и в социален императив.

COVID-19 поиска промени в краткосрочен план и академичните среди реагираха. Предстоят обаче дългосрочни промени в учебните програми, подходите за преподаване и програмата за научни изследвания. Пандемията на COVID-19 може да се разглежда като възможност за „голяма реализация". Безспорно бъдещето принадлежи на смелите, но не егоцентрични, на е-грамотните, но и професионално компетентни. Предстоящата учебна година 2020/2021 ще се случи в необикновени времена и ние трябва да сме готови!

[Показател Г.8] Научни публикации в нереферирани списания с научно рецензиране в България и редактирани колективни томове в България

Научни публикации в редактирани колективни томове в България

[Г.8.1] **Радков Р**., Колев С., Мрежов маршрутизатор. Научно-тематичен сборник ЮНС. Т. 2. 1995, 471-479. Юбилейна научна сесия с международно участие, 22-23 Май **1995**, ВВВУ "Г. Бенковски" гр. Долна Митрополия.

МРЕЖОВ МАРШРУТИЗАТОР

Р. Ст. Радков, Ст. Г. Колев

В публикацията се изтъква нарасналата необходимостта от предаване на информация между различни видове устройства. Създадени бяха мрежи за предаване на данни. Така се оформи ново направление на науката, което се развива изключително бързо. Създаването и управлението на компютърните мрежи, изисква използването на нова техническа база, нови принципи за предаване и комутация. Дефинират се проблемите, които възникват при свързване на компютърни мрежи с различни архитектури. Преодоляването на тези различия става чрез изграждане на междумрежови възли, които осъществяват връзката между мрежите на определен слой от тяхната архитектура.

В публикацията се описва архитектурата на проектирано апаратно-програмно устройство от тип мрежов маршрутизатор. Работата на програмното осигуряване е анализирана с помощта на специално написана програма, която анализира времената за изпълнение на инструкциите на процесора CPU32+, отчитайки конвейерната му организация и отчитайки времето за изпълнение на инструкциите от RISC процесора.

Проектираното устройство дава възможност без промяна в апаратната му конфигурация, да се добавят нови възможности за управление на комуникационни устройства. Успешно са тествани процедурите за управление заложени в протоколите PPP и SLIP.

[Г.8.2] **Радков Р**., Антонов П., Проблеми на проектирането на Ethernet превключватели, Сборник доклади. Т. 3. 1999, 138-144. Осма национална научна и научно-приложна конференция „Електронна техника ЕТ-99“, Созопол, 23-25 Септември **1999**.

ПРОБЛЕМИ НА ПРОЕКТИРАНЕТО НА ETHERNET ПРЕВКЛЮЧВАТЕЛИ

Росен Радков, Петър Антонов

В публикацията са дискутирани тенденциите за увеличаване както на пазара на Ethernet платформите за локални компютърни мрежи, така и на изискванията към ефективността на тяхното функциониране. Направен е извод, че за редица практически приложения е недостатъчна Ethernet конфигурация с един сегмент или разширена конфигурация с повторители, а в повечето случаи се налага разбиване на мрежата на няколко сегмента с използване на мостове или превключватели на кадри, наричани за краткост превключватели или комутатори.

В доклада се разглеждат методически проблеми на проектирането на Ethernet комутатори за конкретни цели. Предвид сложността на тези устройства, на етапа на проектиране се предлага да се разработи блокова схема на апаратната част и съответното програмно осигуряване, след което с помощта на аналитичен и/или имитационен модел да се анализират вероятностно-времевите характеристики на функциониране и да се конкретизира необходимия обем на буферната памет и скоростта на работа на процесора. Предложен е математически модел, с който да се опише работата на комутатора. В модела са обособени две самостоятелни фази: (1) едноканална система с очакване за обслужване на сумарен поасонов поток, и (2) многоканална система за масово обслужване. Изведени са зависимости за вероятността за загуба на кадри и средното време за пребиваване на кадрите.

[Г.8.3] **Радков Р**. Високонадежден дейта център за здравна информация. Сборник доклади „Иновации и бизнес 2017“, 24-27. Научен форум „Иновации и бизнес“, 13-14 Октомври **2017**. ISBN 978-954-20-0779-1

ВИСОКОНАДЕЖДЕН ДЕЙТА ЦЕНТЪР ЗА ЗДРАВНА ИНФОРМАЦИЯ

Росен Радков

Грижата за здравето на хората налага използването на нови приложни технологии, с помощта на които да се следят непрекъснато стойностите на определени показатели, които се снемат чрез специално разработени за тази цел устройства. В доклада се предлага обосновано решение за високонадежден дейта център, необходим за надеждно събиране, обработка и съхранение на данните в център за наблюдение на пациенти (ЦНП).

Дефинирано е, че проектирането и изграждането на ИТ решение, удовлетворяващо посочените по-горе функционалности изисква прилагането на съвременни апаратни и програмни технологии. Определянето на състава на ДЦ, оптимален за всеки един случай, изисква задаването на стойностите на определени показатели. След анализ на необходимото качество на дейта център (ДЦ) за ЦНП и извършена оценка на риска са определени техните стойности. Създаден е модел на дейта центъра и е описан състава на неговите компоненти. Описани са целите, които са заложени, при проектирането на ДЦ. Приложен е авторския подход, предмет на друга публикация, за проектиране на ДЦ и е определен ДЦ, който е необходим, за да бъдат удовлетворени поставените изисквания.

Изчислени са показателите за качество на проектирани дейта център и е доказано, че те удовлетворяват поставените изисквания. Направени са изводи, че:

- Осигуряването на по-добро лечение и справянето с предизвикателствата свързани със здравословните проблеми обусловени от високото ниво на стрес и други фактори изисква използването на приложни технологии осигуряващи постоянен мониторинг на пациенти на болничните организации.
- Успешното им прилагане изисква надеждно събиране, обработка и съхранение на данните, както и тяхната постоянна достъпност.
- Представеното решение осигурява достъпност 99.9048% или осем часа и двадесет минути недостъпност за една година.
- Извършването на планирани и непланирани профилактики става без необходимост от изключване на оборудването.
- Предвидена е възможността за лесно разширяване на ДЦ при увеличаване на обема на данните или необходимост от поемане на задачи свързани с нови процеси.

[Г.8.4] **Радков Р**., Технологични решения за постигане на съответствие с GDPR. Сборник с доклади. 2018, 218-229. Шести национален семинар на тема "Европейските граждани и интелектуалната собственост, възприятие, осъзнатост, поведение", УниБИТ, 25-26 Април **2018**, ISBN 978-619-185-350-2

ТЕХНОЛОГИЧНИ РЕШЕНИЯ ЗА ПОСТИГАНЕ НА СЪОТВЕТСТВИЕ С GDPR

Росен Радков

В публикацията е направен анализ на изискванията, които въвежда приетият от Европейският съюз нов регламент за защита на физическите лица във връзка с обработката на техните лични данни. Определени са новите предизвикателства пред организациите, засегнати от него, които са свързани с необходимостта да бъдат направени подробни анализи на процесите при изпълнението, на които организациите събират и обработват лични данни, вследствие на които да бъдат разработени и внедрени адекватни организационни и технически мерки. Повдигнат е въпросът: Кои са технологичните решения, чрез прилагането на които, организациите ще извършват обработката на лични данни в съответствие с изискванията на регламента?

В доклада се анализират изискванията на регламента, които могат да бъдат удовлетворени чрез въвеждане на технически мерки и се разглеждат приложимите технологични решения. Дискутирано е голямото разнообразие от технологични решения като в доклада се анализират и възможностите чрез прилагане на блокчейн технологии, известни с анонимността на субектите, да се постигне съответствие с регламента.

Разгледани са конкретните технологични решения, които могат да се приложат в ИТ инфраструктурите за да се постигне съответствие с определени изисквания на регламента. Дефинирано е, че изборът на конкретно технологично решение не е тривиален и еднакъв за всички организации. Той е зависим както от размера и структурата на организацията, така и от обема на данните, които се събират и обработват. Решението е различно за всяка една организация, защото зависи от същността на нейните бизнес процеси. Определено е, че правилното решение е резултат от изпълнението на последователност от няколко стъпки: започва се с анализ на бизнес процесите определяне на личните данни на физическите лица, които се използват в тях, защо се налага да се обработват, кой и кога ги обработва и къде се съхраняват; извършва се оценка на риска по отношение на личните данни и преглед на приложените до този момент в организацията контроли за минимизиране на риска; на база на получените резултати се прави избор на технологични решения, с чиято помощ да се усъвършенства текущата ИТИС и да се постигне удовлетворяване на изискванията на регламента.

Описаните технологични решения и определените стъпки, за тяхното прилагане, могат да бъдат използвани като ръководство подпомагащо процеса на внедряване на мерките за удовлетворяване на изискванията на регламента.

[Г.8.5] **Радков Р**., Организационни и технически мерки за осигуряване на съответствие с GDPR,", Политиката на Европейския съюз по защитата на информацията и личните данни, НВУ „В. Левски", Факултет „А, ПВО и КИС" Шумен 12-13.04.**2018**, стр. 262-268, ISBN 978-954-9681-89-5

ОРГАНИЗАЦИОННИ И ТЕХНИЧЕСКИ МЕРКИ ЗА ОСИГУРЯВАНЕ НА СЪОТВЕТСТВИЕ С GDPR

Росен С. Радков

Докладът разглежда основните принципи на защитата на личните данни, въведени с приетия регламент 2016/679 на 27 Април 2016г от Европейският съюз. Регламентът постави редица нови изисквания към администраторите и операторите на лични данни (АОЛД). Една от основните поставени цели с неговото въвеждане е да се хармонизира законодателството в страните членки на ЕС по отношение на защитата на физическите лица във връзка с обработването на техните лични данни и осигуряването на свободното движение на такива данни. С определената дата за неговото прилагане 25 Май 2018г, се осигурява период от две години, през който организациите да предприемат необходимите мерки за да приведат начина, по който обработват личните данни на физическите лица, в съответствие с неговите изисквания. За АОЛД възниква необходимост да направят адекватни промени в съществуващите процедури или да създадат нови такива, както и да намерят правилните решения в случаите когато изискванията на регламента влизат в конфликт с други правилници или законови разпоредби.

За осигуряване на съответствието с регламента, АОЛД е необходимо да приложат и подходящи технически средства за защита на личните данни. Обемът на мерките, които трябва да се приложат, зависи от контролите за сигурност на информацията, които вече са внедрени. Настоящият доклад предлага процесен подход, чието приложение да подпомогне процеса на постигане на съответствие с новия регламент. Определени са и техническите мерки, които е необходимо да бъдат приложени за да се удовлетворят изискванията на конкретни клаузи в регламента.

В резултат на извършения анализ на регламента за защита на личните данни са направени изводи, че за осигуряване на съответствие с регламент 2016/679 на Европейският съюз, АОЛД е необходимо да:

- приложат процесно ориентиран подход, какъвто се предлага в настоящия доклад;
- въведат и прилагат организационни мерки;
- приложат адекватни технически апаратни и програмни средства;
- осъзнаят, че прилагането само на технически мерки не е достатъчно;
- осигурят подкрепа от ръководството;
- извършват постоянна оценка за работата на въведените контроли и вземане на решение за тяхното подобряване.

[Г.8.6] **Радков Р**. Анализ на защитата на личните данни и интелектуалната собственост в системите за управление на сигурността на информацията. УниБИТ, 26 Април **2021** (под печат)

АНАЛИЗ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ И ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ В СИСТЕМИТЕ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Росен Радков

Защитата на личните данни е въпрос, чиято актуалност е непреходна, но с повсеместното развитие на Интернет, внедряването на ИТ технологиите във всеки един бизнес процес и нарастването на обема на информацията, която се обменя вътре в една организация и между организациите, изисква все по-голямо внимание. Необходимо е да се отчитат и промените в нормативната уредба както в национален, така и в европейски и световен мащаб.

В доклада е направен анализ на личните данни, обработвани в множество организации, както и мерките, които са внедрени за осигуряване на тяхната защита. Анализирани са и прилаганите начини за идентифициране и удовлетворяване на приложимите законови и договорни изисквания относно правата на интелектуална собственост. Определени са нормативните актове и документи, които са актуални към настоящият период от време.

Анализът се основава на резултатите от одит на системите за управление на сигурността на информацията, проведени в организации от различен стопански сектор, размер и собственост. Идентифицирани са типичните слабости, които се допускат, и са дадени препоръки за тяхното елиминиране. Определени са седем зони за подобрение, които организациите трябва да имат предвид, за да приведат техните системи за управление на сигурността на информацията в състояние, което ще гарантира реална защита на личните данни и интелектуалната сонственост.

Научни публикации в редактирани колективни томове в чужбина

[Г.8.7] **Radkov R.**, Selecting the optimal IT infrastructure of a data center, Proceedings of the 1st International Conference Applied Computer Technologies ACT 2018, Ohrid, Macedonia, 21-23 June **2018**, pp.26-29, ISBN 978-608-66225-0-3

SELECTING THE OPTIMAL IT INFRASTRUCTURE OF A DATA CENTER

Rosen Radkov

Успешната работа на всяка организация в съвременния свят зависи от качеството на услугите на Центъра за данни, използвани за тази цел. За да се отговори на изискванията за качество на предоставяните услуги, е необходимо да се направи подходящ дизайн на архитектурата и правилен подбор на използваните компоненти. Изборът на оптималната ИТ инфраструктура (ИТИС) за дейта центъра (ДЦ), необходим за работата на всяка организация, е сложен въпрос. Сложността му е резултат от противоречието, което съществува между цената на необходимата инвестиция и цената, която организацията иска да плати. Колкото по-високо качество и по-надеждна е ИТ инфраструктурата, толкова по-висока е нейната цена. От друга страна, лишено от смисъл е да се инвестира в ИТ инфраструктура с по-ниска цена, която не отговаря на изискванията на организацията и нейните бизнес процеси.

Този доклад демонстрира използването на авторски подход за избора на оптимална ИТ инфраструктура и анализира нейната работа.

Представено е прилагане на подхода за подбор на оптималния ИТИС за решаване на конкретна задача. Демонстрира се, че трудността при решаването на задача от такова естество, може да бъде преодоляна и сведена до задаване на стойности за шест показателя, чието естество е такова, че всеки бизнесмен или мениджър на организация може без затруднение да ги определи, без да са необходими специфични технически познания.

Демонстриран е начинът за анализ на резултатите и оценка на възможностите за промяна на входните параметри при необходимост.

[Г.8.8] **Radkov R.**, Analysis and evaluation of a Data Center quality indicators. Proceedings of 15-th International Conference on Informatics and Information technologies CIIT2018, Mavrovo, Macedonia, 20-22 April **2018** pp.173-178, ISBN 978-608-4699-08-8, http://ciit.finki.ukim.mk/

ANALYSIS AND EVALUATION OF DATA CENTER QUALITY INDICATORS

Rosen Radkov

Трудно можем да си представим съвременния свят без присъствието на информационните технологии. Те са навсякъде около нас. Използваме ги когато сме на работа, когато си почиваме и дори когато се забавляваме. Всяка една ИТИС се променя по време на своята експлоатация поради промяна в стойностите на различни показатели: брой отработени часове на нейните компоненти, обем на обработваните и съхранявани данни, брой на обслужваните потребители, промени в изискванията на бизнес процесите, дестабилизиращи фактори на заобикалящата среда и други. Пред организациите, за които е изградена ИТИС, възникват следните въпроси:

- Как да се уверят, че изградената ИТИС има качествата, заложени в проекта?
- Как да се осигури непрекъснато поддържане на високо качество на услугите, които се осигуряват от ИТИС?

Този доклад представя авторски подход за намиране на отговор на поставените въпроси. Представени са съставните компоненти на типичната ИТ инфраструктура. Подбрани и обосновани са едни от най-важните показатели за оценка на качеството на един дейта център – достъпност и натоварване. Обосновани са зависимостите на тези от други показатели на дейта центъра.

Извършено е наблюдение и анализ на работата на конкретна ИТИС. За целта са инсталирани подходящи системи за мониторинг и са събирани данни за период от половин година. времесе вижда, че постигната достъпност на системата за наблюдавания период е 99.977%, а натоварването на отделните и компоненти е под 16%. Следва извода, че през наблюдавания период на експлоатация на системата тя е работила според предварителните очаквания, има възможности за обслужване на нови бизнес процеси и позволява извършване на обслужване и планирани профилактики без да се прекъсват бизнес процесите.

В заключение може да се твърди, че прилагането на предложения подход за анализ на функционирането на ИТИС дава възможност да се получат реални резултати за работата на системата. От анализа им могат да се направят изводи за това дали показателите за качество на реализираната ИТИС съответства на заложените в проекта стойности, както и дали непрекъснато се осигурява заложеното качество на услугите.

[Г.8.9] **Radkov R.**, External factors destabilizing the operation of Data Centers. Proceedings of 15-th International Conference on Informatics and Information technologies CIIT2018, Mavrovo, Macedonia, 20-22 April **2018** pp. 169-172, ISBN 978-608-4699-08-8, http://ciit.finki.ukim.mk/

EXTERNAL FACTORS DESTABILIZING THE OPERATION OF DATA CENTERS

Rosen Radkov

Осигуряването на цялостността и достъпността на информацията са едни от най-важните задачи в областта на информационните технологии. Това е обусловено от зависимостта, която бизнес процесите имат от ИТ инфраструктурата (ИТИС), която обеспечава тяхното изпълнение. Съвременните условия на бизнес средата са такива, че тази зависимост е почти 100%, и изискват ИТИС, да осигуряваат приемливо прекъсване на бизнес процесите, което в голяма част от случаите, особено когато се говори за организация спадаща към големия бизнес, е сведено до няколко минути и дори секунди.

В доклада се прави анализ на външните дестабилизиращи фактори, които оказват влияние на работата на един дейта център. Въз основа на проведения анализ на отделните компоненти на ДЦ и особеностите на тяхното функциониране и на външните фактори, влияещи на тяхната работа, е създаден модел на околната среда, включващ основните заплахи за нарушаване целостта и достъпността на данните, дестабилизиращите фактори, които могат да ги предизвикат, причислени към съответната категория на бедствията. Използването на представения модел би помогнало за изготвянето на оценка на риска, при която да се идентифицират всички източници на риск чрез определяне на възможните заплахи, вероятността за тяхната поява и потенциални последици. Целта на тази стъпка е да се генерира изчерпателен списък на рисковете въз основа на събития, които биха могли да повлияят на работата на ДЦ.

Извършеният анализ за влиянието на заобикалящата среда върху работата на ДЦ показва необходимостта от извършване на оценка на риска от проява на всеки един от нейните ДФ. На базата на тази оценка могат да се вземат адекватни решения за състава на ДЦ и организацията на неговото управление за да може организацията, която ползва ДЦ да е защитена от нарушаване на целостта и достъпността на нейните данни и всички негативни последици, които би имало ако няма такава защита.

Прилагането на предложеният модел на заобикалящата среда при оценката на риска дава възможност да се включат всички потенциални заплахи за работата на ДЦ.

Научни публикации в нереферирани списания с научно рецензиране в България

[Г.8.10] **Радков Р**., Йотов Й. Високонадежден дейта център за кардиологични данни. Сърце - Бял дроб, Варна, Медицински университет – Варна, 18, **2012**, 3-4, 35-46, DOI: http://dx.doi.org/10.14748/hl.v22i0.5487. ISSN 1310-6341

ВИСОКОНАДЕЖДЕН ДЕЙТА ЦЕНТЪР ЗА КАРДИОЛОГИЧНИ ДАННИ

Р. Радков, Й. Йотов

В публикацията се разглежда важността на въпроса, свързан с информацията за състоянието на пациентите, която е необходима на лекарите за да се борят за решаване на проблема със сърдечната недостатъчност като крайна фаза на всички сърдечни заболявания. Обосновава се необходимостта от централизирана обработка на тази информация. Тя 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. Успешната работа на ЦНБСН е зависима от осигуряването на надеждна обработка, съхранение и резервиране на кардиологичните данни. 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.

Описаната архитектура е ИТ решение с централизирано съхранение и обработка на информацията, контрол на мрежовия трафик, внедряване на решение за репликиране на информацията, както и на система за създаване на резервни копия и архивиране на информацията.

Създаден е надеждностен модел на чрез прилагане на моделите за свързване и са изчислени показателите за качество на ИТ инфраструктурата. 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.

[Г.8.11] **Радков Р**., Йотов Й. Аспекти на защитата на личните данни при обработката на кардиологични данни, Сърце - Бял дроб, Варна, Медицински университет – Варна. 22, **2016**, 32-39. DOI: http://dx.doi.org/10.14748/hl.v18i3-4.4198. ISSN 1310-6341

Аспекти на защитата на личните данни при обработка на кардиологични данни

Р. Радков, Й. Йотов

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. Процесите на консултации, диагностика и лечение са свързани с обработка на специални категории лични данни, която трябва да бъде приведена в съответствие с общия регламент относно защитата на данните на физическите лица, приет на 4 май 2016г и влизащ в сила от 25 Май 2018г. В доклада се изясняват задължителните изисквания, които е необходимо да бъдат изпълнени и се дават препоръки за приложимите организационни и технически мерки за постигане на съответствие с регламента.

Изискванията на закона предполагат разработчиците на програмни продукти да вложат решения, които да привеждат в съответствие разработените програмни продукти с принципите заложени в ОРЗД. Приложимите мерки включват използване на анонимизация, псевдонимизация и криптиране на данните, както и въвеждане на контрол на достъпа до информацията чрез прилагане на директорийна услуга, управление на идентичностите, въвеждане на матрица на достъпа, прилагане на системи за управление на документите и др.

Справянето с проблема сърдечна недостатъчност изисква индивидуално постоянно и дългосрочно наблюдение на редица клинични, лабораторни и инструментални параметри, които независимо къде се извършват са свързани с обработка на ЛД на пациентите.

Извършеният анализ на изискванията, поставяни от ОРЗД показва, че постигане на съответствие с тях е възможно само в резултат от въвеждане на адекватни организационни и технически мерки. Най-голям успех ще има ако за обработката на ЛД се въведе система, която е базирана на процесно ориентиран подход. Успешно постигане на съответствие с ОРЗД може да бъде осигурено само ако има подкрепа от ръководството и ако се осъзнае, че прилагането само на технически мерки не е достатъчно, както и това, че трябва да се извършва постоянна оценка за работата на въведените контроли, прегледи на резултатите от ръководството и вземане на решение за тяхното подобряване.

Посочените мерки трябва да бъдат творчески прилагане за да не се затруднява и пречи на работата на медицинските работници.

[Г.8.12] Радков Р. Модел на Дейта център за фирми от тип микро, малък и среден бизнес“ Устойчиво развитие, Варна, Международна асоциация „Устойчиво развитие“, VII, **2017**, 3, 73-78. ISSN 1314-4138

МОДЕЛ НА ДЕЙТА ЦЕНТЪР ЗА ФИРМИ ОТ ТИП МИКРО, МАЛЪК И СРЕДЕН БИЗНЕС

Росен Радков

В доклада се отчита, че фирмите от тип микро, малко и средно предприятие (ММСБ) по статистически данни представляват над 90% от общия брой фирми и създават всеки две от три работни места. Дейта центровете (ДЦ) на тези фирми представляват ядрото на ИТ инфраструктурата им и имат особено важно значение за функционирането на работните процеси. Предизвикателство пред ИТ специалистите е изграждането на дейта център, който да осигурява безпрепятственото и устойчиво на външните дестабилизиращи фактори протичане на бизнес процесите във фирмата.

В зависимост от спецификата на всеки един от трите типа фирми е описано различието в техните ИТ инфраструктури, а в резултат на обобщаване на характеристиките на фирмите е предложен обобщен модел на дейта център, който да се използва при проектиране на неговата ИТ инфраструктура.

Предложеният модел описва не само софтуерните и хардуерни компоненти на ДЦ, а и дейности, свързани с въвеждането на политики за неговото управление и управлението на сигурността на информацията. Посочени са и необходимите за неговата работа услуги. Следвайки предложения модел на ДЦ успешно може да се проектира ВНДЦ за фирми от тип ММСБ. Основните различия в ИТ инфраструктурите на трите типа фирми, причислявани към ММСБ са обусловени от разликите в броя на бизнес процесите, които се обслужват, броя на потребителите и обема на данните, с които работят, броя на площадките и тяхното географско разположение. Тези разлики се отразяват съществено както на необходимата изчислителна мощ, така и на прилаганите в дейта центъра ИТ концепции и решения.

[Г.8.13] **Радков Р**. Методика за осигуряване на висока надеждност на дейта центрове. Компютърни науки и технологии. Варна, Технически университет – Варна. **2017**. 17-23. ISSN 1312-3335

МЕТОДИКА ЗА ОСИГУРЯВАНЕ НА ВИСОКА НАДЕЖДНОСТ НА ДЕЙТА ЦЕНТЪР

Росен С. Радков

Дейта центровете осигуряват работата на бизнес процесите в организациите и фирмите. В резултат на тяхната работа гражданите и фирмите получават възможност да използват приложенията използвани от съответен бизнес процес и услугите, които се генерират от него. Важно условие за предоставяне на качествени услуги е осигуряването на висока надеждност на дейта центъра. Тази статия анализира решенията за създаване на висока надеждност и предлага методика за нейното осигуряване.

В настоящият момент съществуват множество стандарти и добри практики за проектиране и изграждане на ДЦ или части от неговата инфраструктура, но се констатира липса на методика, която да описва действията и дейностите, които е необходимо да се извършат за да се осигури високо надежден дейта център (ВНДЦ).

В доклада се предлага методика, която да помогне на организациите и фирмите да решат по оптимален начин тази задача. От нейното съдържание става ясно, че реализирането на решение за ВНДЦ се осъществява не само чрез проектиране и въвеждане на високонадеждна ИТИС и комплекс от планове и процедури, но и чрез обучение на персонала, тренировки и оценка на работата на системата. Предложената методика е адаптирана за практическо приложение.

[Г.8.14] **Радков Р**. Анализ и сравнение на международните стандарти за дейта центрове. Компютърни науки и технологии. Варна, Технически университет – Варна. **2017**, 8-16. ISSN 1312-3335

АНАЛИЗ И СРАВНЕНИЕ НА МЕЖДУНАРОДНИТЕ СТАНДАРТИ ЗА ДЕЙТА ЦЕНТРОВЕ

Росен С. Радков

В доклада се обосновава важността на дейта центровете (ДЦ) за бизнеса и необходимостта при тяхното проектиране и изграждане да се вземат под внимание не само изискванията на бизнеспроцесите, но и изискванията на международните и национални стандарти. Тази статия анализира стандартите и определя тяхната приложимост при решаването на отделните задачи, решавани при проектиране и изграждане на ДЦ, тъй като е важно специалистите, които проектират и изграждат ДЦ да са запознати със съществуващите стандарти и добри практики.

В настоящият момент съществуват множество стандарти за проектиране и изграждане на ДЦ или части от неговата инфраструктура. Задачата на тази статия е да определи кой от стандартите за центрове за данни трябва да се следва при проектиране и изграждане на ДЦ или част от неговата инфраструктура.

В резултат на анализа е направен извод, че само EN 50600-X и ANSI/BICSI 002 разглеждат всички аспекти на проектирането, внедряването и поддръжката. Единствено EN 50600-X определя минималните изисквания за проектиране, но ANSI/BICSI 002 предоставя най-изчерпателна информация, която може да се използва като препоръки и добри практики. ДЦ трябва да бъдат стандартизирани и сертифицирани. Това помага на заинтересованите да намерят правилния отговор на много въпроси, например: какъв тип ДЦ бизнес модел да се избере, колко пари да инвестира в ДЦ, как да изберем подходящ доставчик на ДЦ и т.н.

[Г.8.15] **Радков Р**. Международни научни комуникации по проблемите на електронното досие на пациента и облачните технологии. Асклепий. XV, **2019**, 55-61. ISSN 1310-0637

МЕЖДУНАРОДНИ НАУЧНИ КОМУНИКАЦИИ ПО ПРОБЛЕМИТЕ НА ЕЛЕКТРОННОТО ДОСИЕ НА ПАЦИЕНТА И ОБЛАЧНИТЕ ТЕХНОЛОГИИ

Росен Радков

В доклада се прави анализ на използването на облачните технологии за целите на здравеопазването в последните десет години. Отчита се, че тяхното прилагане в разработването на електронно досие на пациента и достъпа до него набира все по-голяма популярност в практиката на лечебните заведения.

Проведено е наукометрично проучване на динамиката на международните научни комуникации по тази проблематика и е установено значително нарастване през последните години на публикациите и дискусиите на тази тема. Анализирани са публикациите, реферирани в базите-данни Web of Science Core Collection (WoS) и Scopus през периода между 1999 г. и 2018 г. вкл. Откроени са водещите страни, автори и списания през този период. Резултатите показват постоянния интерес на световната научна общност към тази социално значима проблематика, насочена към по-нататъшната оптимизация на системите на здравеопазването.

От направения анализ и използвана литература мениджърите на лечебните заведения могат да получат информация за употребата на облачните технологии в сферата на електронното здравно досие, а научните работници и ръководителите, определящи научната политика у нас могат да повишат ефективността на научната си дейност и международната видимост на своите постижения.

[Г.8.16] **Radkov R**. Software Defined Networks - a brief study. Компютърни науки и технологии. Варна, Технически университет – Варна. **2019**, 103-109. ISSN 1312-3335

SOFTWARE DEFINED NETWORKS – A BRIEF STUDY

Rosen S. Radkov

Съвременните компютърни мрежи са сложни за управление и адаптирането към новите бизнес изисквания и проблеми е много трудно. Тази статия представя кратко проучване на новата технология за управление на компютърна мрежа, наречена Софтуерно дефинирани мрежи (SDN). В тази статия са представени мотивацията за тяхното създаване, основните им концепции и тенденции в тяхното развитие. Софтуерно дефинираните мрежи отделят един от друг функционалните слоеве на компютърна мрежа – т.н. равнина за данни от равнина за управление. Тази функционалност подобрява възможностите за програмиране, гъвкавостта и управляемостта на мрежата. Представено е проучване за прогнозите за развитие на SDN мрежите и са дефинирани основните изисквания, на които трябва да отговарят.

Тъй като традиционните мрежи са сложни, те са трудни за управление. Развитието на облачни услуги е трудно при традиционния начин на управление на мрежите. Софтуерно дефинираните мрежи създават способността да направят управлението на мрежата по-лесно и по-умно. Освен, че разделят равнината за данни от равнината за управление в мрежовата архитектура те включват и централизирано управление на мрежата. Това позволява управлението на мрежата да се извършва директно от приложенията, използващи API, без да е необходимо да се знае подробно мрежовата архитектура. Заедно с прекрасните идеи, които са вградени в SDN, има и нови предизвикателства, свързани с надеждността, мащабируемостта и сигурността на SDN.

[Г.8.17] **Радков Р**. Сигурност и конфиденциалност на данните от електронното досие на пациента - динамична институционализация на проучванията по проблематиката. Асклепий. XVI, **2020**. ISSN 1310-0637

СИГУРНОСТ И КОНФИДЕНЦИАЛНОСТ НА ДАННИТЕ ОТ ЕЛЕКТРОННОТО ДОСИЕ НА ПАЦИЕНТА - ДИНАМИЧНА ИНСТИТУЦИОНАЛИЗАЦИЯ НА ПРОУЧВАНИЯТА ПО ТАЗИ ПРОБЛЕМАТИКА

Росен Радков

В доклад се обобщават въпросите свързани със създаването, поддържането и ползването на електронното досие на пациента. През последните години сигурността и конфиденциалността на данните представляват основен фокус при изграждане и ползване на електронното досие на пациента. В световен мащаб са въведени редица стандарти за най-добри практики и препоръки за управление на сигурността на информацията, оценка на рисковете и въвеждане на контроли в системите за управление на сигурността на информацията.

Анализирани са публикациите, свързани със сигурността и конфиденциалността на данните от електронното досие на пациента и реферирани в базите данни Web of Science Core Collection (WoS) и Scopus през периода между 1999 г. и 2018 г. вкл. Откроени са водещите страни, научни институции, тематични профили, списания и автори през този период. Проведеното наукометрично проучване показва нарастващ брой публикации през последните години и потвърждава все по-нарастващото значение на сигурността и опазването на данните при работа с електронното здравно досие.

Специалистите, разработващи системи за електронно досие на пациента, могат да използват настоящото проучване и обобщената библиографска и фактографска информация, за да открият систематизирана информация за стандартите, които се прилагат в световен мащаб, и за използването им в различните държави и институции. Младите изследователи могат да обогатят теоретичните си познания, с което ще подпомогнат научноизследователската си дейност и бъдещата си практическа дейност.

Учебно помагало

Радков, Росен, **Мартин Иванов** Ръководство за лабораторни упражнения по „Интернет сървъри и услуги“. Варна, Университетско издателство на ТУ-Варна. **2021**. 144 стр. ISBN: 978-954-20-0831-6

В ръководството са представени дванадесет теми за лабораторни упражнения по дисциплината „Интернет сървъри и услуги“, изучавана в шести семестър от студентите в специалност „Софтуерни и Интернет технологии“. За всяка една от темите е включено кратко теоретична изложение, след което са представени конкретната лабораторна постановка, която трябва да се реализира и задачите за изпълнение. Лабораторните упражнения могат да бъдат изпълнявани както при присъствена, така и при неприсъствена форма на обучение. За изпълнението на задачите на лабораторния компютър се създава виртуална среда, в която се стартират и работят една или две от общо трите виртуални машини: Windows server, RouterOS и Asterisk. Резултатите от изпълнението на десет от лабораторните упражнения се документират във вид на протокол. В резултат от изпълнението на лабораторните упражнения придобиват знания и се развиват умения у студентите за съвременните концепции и начин на работа на Интернет услугите (DNS, email, VPN, web, ftp, proxy,VoIP). Придобиват се знания за архитектурата, начина на работа, конфигурирането и настройката на протоколите и услугите. Отделено е внимание на въпросите свързани с осигуряване на оптимални конфигурации и висока достъпност на услугите

09.09.2021г Подпис: ……

гр. Варна / гл. ас. д-р инж. Росен Радков /