СТОПАНСКА АКАДЕМИЯ “Д. А. ЦЕНОВ” – СВИЩОВ
КАТЕДРА "БИЗНЕС ИНФОРМАТИКА"

Асен Петров Божиков

ВЪЗСТАНОВЯВАНЕ НА ИНФОРМАЦИОННАТА ИНФРАСТРУКТУРА ПРИ БЕДСТВИЯ И АВАРИИ

А В Т О Р Е Ф Е Р А Т

НА ДИСЕРТАЦИОНЕН ТРУД ЗА ПРИСЪЖДАНЕ НА ОБРАЗОВАТЕЛНА И НАУЧНА СТЕПЕН „ДОКТОР“ ПО НАУЧНАТА СПЕЦИАЛНОСТ „ПРИЛОЖЕНИЕ НА ИЗЧИСЛИТЕЛНАТА ТЕХНИКА В ИКОНОМИКАТА“

Научен ръководител:
Доц. д-р Петя Емилова

Свищов
2019

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Актуалност на изследването

В ерата на дигитална трансформация, за да осъществява дейността си, организацията[1] става все по-зависима от информационните технологии (ИТ). Основна предпоставка за нейното успешно развитие и удовлетворяване на потребностите на клиентите са данните т.е. наблюдава се преход към базиращ се на данните мениджърски модел. Това е следствие на обстоятелството, че данните представляват сърцевината на съвременната организация. Те са основа за генериране на знания (зависимости, тенденции и нови възможности) и предпоставка за нейното дългосрочно функциониране и съществуване.

Посредством симбиозата на съвременните ИТ и иновативни мениджърски модели, организациите откриват нови възможности и решения, свързани с техните усилия за: лесен достъп до данни, справяне с нарастващата конкуренция, увеличаване на ефективността, подобряване на качеството на предлаганите продукти и услуги, намаляване на времето за предлагане на нови продукти и услуги на пазара, по-добър контакт с клиентите.

Това означава, че постигането на непрекъснатост в работата на критичните за организацията приложения и информационни системи е от изключителна важност. Модерната организация се ориентира към такива ИТ платформи, които ще предоставят[2]:

- висока надеждност, достъпност и мащабируемост на информационната инфраструктура (ИИ) и информационните системи (ИС), които я използват;
- възможност за интегриране на бизнес приложенията и процесите;

[1] За удобство и с цел избягване на повторенията тук и по-нататък в изложението, терминът „организация“ се употребява обобщаващо и еднозначно на понятията стопанска организация, фирма, предприятие, корпорация, компания, организация в публичния или частния сектор, обществена организация с нестопанска цел, организационна единица в администрация на изпълнителната власт като се има предвид, че в тяхното правно и икономическо съдържание съществуват различия, които не влияят на обекта и предмета на настоящото научно изследване.

[2] Bajgoric, N. (2009). Continuous Computer technologies for Enhancing Business Continuity. London: IGI Global.

- способности за поддържане на взаимнозаменяеми хардуерни и мрежови компоненти;
- способности за репликация на данните;
- гъвкавост за възстановяване от бедствия и аварии;
- поддържане на отдалечена администрация;
- по-сигурна среда за достъп, като се използват удостоверяване самоличността на потребителя, откриване на неправомерен достъп до системата, по-сигурни транзакции и др.

Реализирането на тези предимства обаче не е толкова лесна за изпълнение задача. Необходимо е да се гарантира възможност за ***непрекъснатост на бизнес процесите***. Това се отнася с особена сила за мултинационалните компании, тъй като техните служители, клиенти и доставчици се намират в различни държави и съответно в различни часови зони. Поради тази причина непрекъснатото функциониране на бизнеса и достъпът до данни – 24 часа в денонощието, 7 дни в седмицата, 365 дни в годината – е от съществено значение. По този начин ще се гарантират експедитивно и ефективно протичане на бизнес процесите и обслужване на клиентите. За да се постигне това, всяка организация трябва да обезпечи функционирането на критичните си приложения и системи и да разполага с резервни копия на данните си. Ключовият момент е да се определи какво е приемливото време за престой поради възникнали повреди и прекъсвания в хардуера и софтуера и доколко ИТ бюджетът на организацията позволява да се избегне този престой.

Планирането и управлението на възстановяването от бедствия и аварии е част от интегрираната политика на информационна сигурност. Следователно всяка една организация, независимо дали е от малък, среден или голям размер, както и независимо от нейната сфера на дейност, е желателно да имплементира решение за възстановяване от бедствия, което е изключително важна стъпка за постигане на непрекъснатост на бизнеса[3].

[3] Под непрекъснатост на бизнеса се разбира осигуряване на непрекъснатост в изпълнението на критичните бизнес процеси, които водят до реализирането на целите и задачите, които си е поставила организацията.

При планирането на възстановяване от бедствия и аварии съществуват спорни въпроси както в теоретичен, така и в приложен аспект. Тяхното анализиране и разрешаване обуславя ***актуалността на изследваната проблематика***. Освен това някои от понятията в тази област подлежат на уточняване и прецизиране, що се отнася до българската практика. Актуалността на тематиката може да се подплати и с примера от българската реалност, отнасящ се до срива в търговския регистър през миналата година. На 10 август 2018 г. онлайн достъпът до търговския регистър на България временно беше преустановен[4]. Частична функционалност беше възстановена на 15 август, а едва на 28 август регистърът работеше с пълната си функционалност. Същевременно се оказа, че проблемът не е само онлайн, тъй като и службата за справки на гише също нямаше достъп до базата данни. Изтъкнатите причини за този непланиран престой бяха свързани с няколко дефектирали харддиска в RAID масива на регистъра и безотговорност на служители. Възникналата непредвидена ситуация създаде масово недоволство сред обществото и бизнеса в България.

2. Изследователска теза

Изследователската теза, върху доказването на която е насочено нашето внимание, е че посредством адекватно планиране и организация на дейностите по възстановяването от бедствия и аварии ще се гарантира високо ниво на сигурност и поверителност на данните, постоянен достъп до критичните бизнес приложения и услуги, което означава непрекъснато функциониране на критичните бизнес процеси. Това индиректно ще осигури конкурентно предимство, удовлетвореност на всички заинтересовани страни и застраховка срещу възникването на непредвидени събития.

3. Цели и задачи на изследването

Основната цел, която си поставяме в дисертационния труд, е чрез изследване на теоретичните постановки и анализ на съществуващите

[4] Веселинова, М. (17.08.2018 г.). Кой спря Търговския регистър. Капитал. Извлечено от https://www.capital.bg/politika_i_ikonomika/bulgaria/2018/08/17/3297153_koi_spria_turgovskiia_registur/#

стратегически подходи и решения за възстановяване да се предложи концептуален модел на съвременно решение за възстановяване от бедствия и аварии, подходящо за информационната инфраструктура на избрана съвкупност от организации – български общини.

За постигане на целта на научноизследователския труд и доказване на изследователската теза се изпълняват следните ***задачи***:

В теоретичен аспект:

1. Обосноваване на нарастващата роля и значение на информационната инфраструктура на съвременната организация като генератор на ефективност и конкурентни предимства.
2. Изясняване на основните понятия и показатели, съпътстващи планирането на възстановяването от бедствия и аварии и доказване на критичното му значение за съвременната организация през призмата на нарастващата и безалтернативна зависимост на бизнеса от ИТ.
3. Анализ на различните архитектурни и стратегически подходи за възстановяване от бедствия и аварии.

В практикоприложен аспект:

4. Изследване текущото състояние на информационната инфраструктура на българските общини и възможностите за нейното възстановяване от бедствия и аварии.
5. Анализ на влиянието на информационната инфраструктура на община върху бизнеса и оценка на свързаните с нея рискове.
6. Предлагане на концептуален модел на съвременно решение за възстановяване от бедствия и аварии, приложимо и подходящо за българските общини.

4. Обект и предмет на изследването

Обект на изследване в настоящия дисертационен труд е информационната инфраструктура на съвременната организация.

Предмет на изследване е прилагането на различи архитектурни и стратегически подходи и решения за възстановяване на информационната инфраструктура на организацията след бедствия и аварии.

5. Обем и структура на дисертацията

Дисертационният труд е в обем от 224 стандартни страници и се състои от увод, три глави, заключение, приложения, декларация за оригиналност и достоверност, списък на използваните съкращения и списък с използваните източници – 226 литературни източника (44 български и 182 чуждестранни). В основния текст са включени 26 таблици и 45 фигури.

6. Ограничителни условия на изследването

В рамките на настоящото научно изследване са приети следните ***ограничителни условия***:

1. Под възстановяване от бедствия и аварии се разбира възвръщане в работещо състояние на информационните системи и услуги, които са станали недостъпни в резултат на възникване на разрушително събитие.
2. Разгледаните версии на стандарти, свързани с възстановяването от бедствия и аварии и непрекъснатост на бизнеса, са актуални към месец юни 2019 година. Актуализацията на тези стандарти след този период не е намерила отражения в научния труд.
3. Направеният анализ на информационната инфраструктура е насочен към общините поради тяхното съществено значение в концепцията за развитие на електронно управление в България. Анализът се отнася само за общини от категория 2 и 3. Те са избрани поради факта, че категория 1 включва всички областни центрове, които разполагат с повече ресурси и налични ИТ специалисти или могат да си позволят аутсорсване на ИТ дейности. Категория 4 и 5 са изключени, защото разполагат със сравнително ограничени ресурси и дори в някои от общините ИТ дейностите се съвместяват от служител, изпълняващ друга длъжност.

7. Методи и методология на изследването

Методологията на изследването се основава на използването на научно-изследователски подходи и методи като исторически подход, системен подход, метод на анализа и синтеза, метод на индукция и дедукция и на експертна оценка. Приложени са методите на наблюдение, анкета и интервю, статистически методи за анализ и изследване на зависимости и методът на абстракция.

Изследването се базира на проучването и систематизирането на широк кръг научни публикации от български и чуждестранни автори, както и на отчети и прогнози на водещи консултантски фирми.

II. СТРУКТУРА И СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

В структурно отношение дисертационният труд се състои от увод, три глави, заключение и приложения. Освен това в него се съдържат още списък на използваните съкращения, списък с използваните източници и декларация за оригиналност и достоверност. Структурата на изложението е следната:

УВОД

ПЪРВА ГЛАВА

КОНЦЕПЦИЯ ЗА ВЪЗСТАНОВЯВАНЕ НА ИНФОРМАЦИОННАТА ИНФРАСТРУКТУРА НА ОРГАНИЗАЦИИТЕ ОТ БЕДСТВИЯ И АВАРИИ

1. Същност, обхват и състав на информационната инфраструктура
   1.1. Характеристики на съвременната бизнес среда
   1.2. Роля на информационните технологии за организациите
   1.3. Концепция за информационна инфраструктура
2. Особености при възникване на прекъсвания във функционирането на информационната инфраструктура
   2.1. Нефункционални атрибути на информационната инфраструктура
   2.2. Споразумение за нивото на обслужване
   2.3. Престой и последици за организациите от неговото възникване
3. Концепция за възстановяване от бедствия и аварии и непрекъснатост на бизнеса
   3.1. Видове бедствия, засягащи информационната инфраструктура на организациите
   3.2. Същност и особености на възстановяването от бедствия и аварии
   3.3. Управление на непрекъснатостта на бизнеса

ВТОРА ГЛАВА

АНАЛИЗ НА ОСОБЕНОСТИТЕ ПРИ РАЗРАБОТВАНЕ НА СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ ОТ БЕДСТВИЯ И АВАРИИ

1. Особености при разработването на проект за създаване на план за възстановяване от бедствия и аварии

1.1. Управление на риска в условията на дигитална трансформация

1.2. Методология за разработване на план за възстановяване от бедствия и аварии

1.3. Фактори за успешно разработване на план за възстановяване от бедствия и аварии

2. Архитектурни подходи за реализиране на възстановяване от бедствия и аварии

2.1. Показатели за определяне на способността за възстановяване от бедствия и аварии

2.2. Концепция за седемте слоя за възстановяване от бедствия

2.3. Избор на отдалечено място за възстановяване

2.3.1. Вариант „студен“ резервен център

2.3.2. Вариант „топъл“ резервен център

2.3.3. Вариант „горещ“ резервен център

2.3.4. Вариант мобилен резервен център

2.3.5. Избор на вариант на резервен център

3. Стратегически подходи и решения за възстановяване от бедствия и аварии

3.1. Използване на собствен резервен център за данни

3.2. Използване на център за колокация

3.3. Използване на облачни услуги за възстановяване

3.3.1. Използване на сторидж като услуга

3.3.2. Използване на възстановяването от бедствия и аварии като услуга

ТРЕТА ГЛАВА

МЕТОДИКА ЗА ВЪЗСТАНОВЯВАНЕ НА ИНФОРМАЦИОННАТА ИНФРАСТРУКТУРА НА ОБЩИНИТЕ В БЪЛГАРИЯ ОТ БЕДСТВИЯ И АВАРИИ

1. Проучване и анализ на текущото състояние на информационната инфраструктура на българските общини

1.1. Общинската администрация в концепцията за електронно управление

1.2. Методология на емпиричното изследване

III. СИНТЕЗИРАНО ИЗЛОЖЕНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Първа глава. КОНЦЕПЦИЯ ЗА ВЪЗСТАНОВЯВАНЕ НА ИНФОРМАЦИОННАТА ИНФРАСТРУКТУРА НА ОРГАНИЗАЦИИТЕ ОТ БЕДСТВИЯ И АВАРИИ

Изследването в **първа глава** на дисертационния труд е с теоретична насоченост и представя все по-нарастващата зависимост на организацията от ИТ и свързаната с тях информационна инфраструктура (ИИ), която обаче от своя страна е податлива на различни прекъсвания, породени от бедствия и аварии. В тази връзка са разгледани концепциите за планиране на възстановяването от бедствия и аварии и управление на непрекъснатостта на бизнеса.

В **първия параграф** е разгледана ролята на ИТ за организацията в контекста на особеностите на съвременната среда, в която тя функционира, като заедно с това се изяснява същността на понятието ИИ. Посочено е, че съвременните организации не функционират изолирано една от друга, а осъществяват своята дейност в определена среда. Последната може да се дефинира като високо турбулентна, която неминуемо оказва влияние върху постигане на поставените бизнес цели. Тази среда се характеризира с: *динамика, сложност, неопределеност, относително влияние, взаимосвързаност на факторите*.

Разгледан е подходът, представящ организацията като единство на ***три основни компонента:*** *персонал, бизнес процеси и технологии*. Те са утвърдени като ключ към подобряване функционирането на една организация и вниманието на ръководството трябва да е разпределено между всеки от тях. Тези съставни части са интегрирани посредством *информационните потоци* и понеже днес достигнатото ниво на интеграция е значително, то е трудно да разделим всеки един от посочените три компонента от останалите. Подходът, известен още и под

наименованието ***„бизнес триъгълник“*** или ***„златен триъгълник“***, се използва масово от организации от различни сектори на икономиката и с различен размер[5].

Анализирана е съществената роля на ИТ, които помагат на организацията да се приспособява към непрекъснато променящата се бизнес среда и да постига поставените цели. Заедно с това се акцентира, че още в средата на 90-те години на миналия век *ролята на ИТ се променя в посока от поддържаща бизнеса към стратегическа за неговото съществуване*[6], както и че ИТ продължават да се развиват изключително бързо, като *предоставят възможност за подобряване на всеки един аспект на дейността*.

Посочват се ***потенциалните ползи*** от използването на ИТ в организациите, като сред най-важните от тях са изтъкнати*: намаляване на оперативните разходи, реализиране на приходи и нарастване на пазарния дял, непрекъснато подобряване на бизнес процесите, създаване на стойност за потребителите*. Приема се становището, че за да бъдат постигнати тези ползи, е необходимо да се гарантира съответствие между бизнес стратегията, от една страна, и бизнес очакванията от внедряването на ИТ проекти, от друга.

За да се получи по-задълбочена и детайлна представа за същността на ИИ, която е основа за използването на ИТ в организациите, са систематизирани и обобщени редица научни изследвания по темата. Представени са множество дефиниции за ИИ, като между тях се забелязва голяма степен на сходство. Една от основните разлики се изразява в това, дали ИТ персоналът трябва да бъде считан като част от тази инфраструктура или не трябва да присъства там. За целите на настоящото изследване е прието ***следното определение за ИИ***: *комплекс от хардуер, софтуер, мрежови компоненти, оборудване и съответните нефункционални атрибути, които са в основата на функционирането на корпоративната информационна система на организацията*.

[5] Hopson, D. (14.06.2017 г.). The Business Triangle: People, Process and Technology. Извлечено от TotalRetail: https://www.mytotalretail.com/article/the-business-triangle-people-process-and-technology/

[6] Sheth, J. (1994). Strategic Importance of Information Technologies. Strategic Perspective on the Marketing of Information Technologies, 4, 3-16.

Стига се до извода, че днес сме свидетели на изграждането на все по-сложни ИИ в съвременните организации, чрез които те да могат да отговорят на все по-нарастващите изисквания, поставяни от техните потребителите. Отбелязва се, че предложената модифицирана рамка 8i би била много полезен модел за разглеждане и обсъждане на възможните уязвимости в отделните компоненти на инфраструктурата.

Вторият параграф разглежда особеностите на нефункционалните атрибути на ИИ и изяснява какво влияние оказва ***престоят***, довел до прекъсване във функционирането на дадена информационна система или услуга върху дейността на съвременната организация. Изхождайки от твърдението, че ИИ представлява „гръбнака“ за осъществяване на бизнес дейностите на организацията, се представят трите най-съществени характеристики, отразяващи качеството на компонентите на тази инфраструктура, представени чрез акронима ***RAS (Reliability, Availability, Serviceability)***, а именно – *надеждност (Reliability), достъпност (Availability) и обслужване (Servicebility)*.

Изяснени са същността и начинът за измерване на всяка от трите качествени характеристики на ИИ. ***Надеждността (Reliability)*** се използва за измерване на възможността да се избегне възникването на някаква повреда. Изразява се чрез вероятността, че *определена система все още ще функционира в даден период от време t+1, след като е функционирала в периода от време t*[7]. Според някои специалисти, надеждността често се представя чрез показателя ***Средно време между повреди (Mean Time Between Failure, MTBF, СВМП)***, който се изчислява в часове работно време на даден инфраструктурен компонент.

Достъпността (Availability) се използва за измерване на това, колко често дадена услуга или системен компонент е достъпен за използване[8]. Достъпността може да се представи като *съотношение на времето, в което системата е активна и работи (uptime) и общото време на работа на системата*

[7] Schmidt, K. (2006). High Availability and Disaster Recovery: Concepts, Design, Implementation. Berlin: Springer.

[8] Lie, D. (27 May 2000 г.). Reliability, Availability, and Serviceability. Извлечено от EE482: http://cva.stanford.edu/classes/ee482a/scribed/lect16.pdf

включително и планираните и непланирани прекъсвания (downtime). Това може да се представи със следната формула:

$$\textbf{Достъпност} = \frac{\text{uptime}}{\text{uptime} + \text{downtime}}$$

Този показател *може да се представи като число, отразяващо часове или минути* (100 часа от общо 101 работни часа за даден месец) *или като процент* (99,7% за даден месец). Дефинирането на достъпността като процент донякъде интегрира сложността на този показател в една единствена стойност, която *отразява достъпността до съответната ИТ услуга или система 24 часа на ден, 7 дни в седмицата, 365 дни в годината*.

Обслужването (Serviceability) е измерител за това, колко лесно системата може да се поддържа или поправя в случай на възникване на дадено прекъсване[9]. Обслужването може да се представи чрез следната формула:

$$\textbf{Обслужване} = \frac{\text{Време за поддръжка}}{\text{Брой повреди}}$$

Полученият резултат от показателя обслужване подпомага анализа и откриването на причините за възникването на системни повреди, както и системната диагностика и откриването на проблеми, преди те да причинят прекъсване на работата на системата.

Представена е ролята на ***споразумението на нивото на обслужване (СНО)***, което урежда въпросите за нивото на достъпност по отношение на предлаганите услуги и евентуални неустойки, които следва да се удържат, ако доставчикът не осигури предвиденото ниво на безотказна работа. СНО се получава като стойност в резултат на дискутиране между мениджмънта на организацията и нейния ИТ отдел. В практиката обаче все по-често става възможно, тази дейност да се изнася към външна организация. Чрез подготвянето и подписването на СНО организацията знае какво трябва да получи, а доставчикът (било то вътрешен или външен за организацията) знае какво трябва да предостави – договореното ниво на достъпност на услугите. Отбелязано е, че с развитието на

[9] Пак там

различните модели на облачни услуги все по-често СНО се налага като подход за постигане на по-високо качество в нивото на обслужване.

Разгледани са понятията „***активно време на работа на дадена система“ (uptime)*** и „***престой“ (downtime)*** като именно времето за престой е в основата на възстановяването от бедствия и аварии, тъй като е пряко свързано с достъпността на предлаганите от организацията услуги. Ако дадена система, която обезпечава конкретно предлагана услуга, е в състояние на престой, то тази услуга няма как да бъде достъпна.

На базата на цитирани проучвания на консултантски фирми е достигнато до извода, че в съвременните условия на осъществяване на бизнес, когато организацията става все по-зависима от внедряването на ИТ, дори няколко минути престой поради повреда могат да доведат до значителни загуби. Освен пропуснатите ползи това може *да окаже негативно влияние и върху удовлетвореността на клиенти, доставчици, акционери както и върху имиджа на организацията*. Поради тази причина времето за престой трябва да се минимализира и избегне, доколкото е възможно. По-нататък в изложението е разгледано класифицирането на престоя като ***планиран и непланиран***. Подчертано е, че в 90% от случаите той е планиран и само в 10% е неочакван и възниква инцидентно за неопределен период.

В **третия параграф** се разглеждат концепциите за възстановяване от бедствия и аварии и непрекъснатост на бизнеса. Изложението започва с дефинирането на понятието „***бедствие“***. Подчертава се, че в специализираната литература могат да се срещнат много определения за термина „бедствие“, погледнати през призмата на различни науки като *мениджмънт, екология, информатика, психология*. Уточнено е, че *за нуждите на настоящото изследване това понятие ще се разглежда от гледна точка на връзката му с компонентите на ИИ на организацията*.

Систематизирани са определенията за бедствие, дадени от различни автори през годините. На базата на представените дефиниции и за нуждите на настоящия научен труд е изведено следното определение за бедствие: ***поява на непредвидено събитие, което нарушава нормалното функциониране на компоненти на ИИ***

на организацията, като по този начин се засягат критични бизнес процеси, което може да доведе до загуба на данни и бизнес ползи.

Тъй като бедствията могат да възникнат под различна форма и да окажат различна степен на влияние върху организациите, са представени няколко ***класификации на видовете бедствия***. Въз основа на посочените класификации е направен изводът, че последните *могат да бъдат причинени от природни стихии, хора или технологии, като в същото време може да се окажат вътрешни или външни за организацията.*

Анализирани са резултатите от редица проучвания, свързани с най-честите източници на прекъсвания или повреди, които водят до загуба на данни и създават проблеми за нормалното протичане на бизнес процесите в организацията. В резултат на тях е направено заключението, че възможните причини за възникване на бедствия и аварии са сравнително едни и същи, но последователността им, определена на база степен на проявлението им, е различна. Въпреки това достатъчно ясно се забелязва необходимостта *да се обърне сериозно внимание върху достъпността и надеждността* на хардуера, софтуера и комуникационното оборудване, които са в основата на ИИ на всяка организация.

Направен е исторически анализ на развитието на концепцията за възстановяването от бедствия и аварии, като е подчертано, че тя намира своите корени във военните игри и планирането на сценарии още в древността. ***Теорията за възстановяване от ИТ бедствия и аварии възниква през 60-те години на XX век в резултат на масовото навлизане на ИТ в бизнеса.*** Сериозно развитие в областта на възстановяването от бедствия и аварии се отчита през 80-те и 90-те години на XX век, а появата на Интернет и масовото му използване от организациите след 2000 г. за достигане бързо и лесно до нови пазари и потребители увеличава още повече важността на плана за възстановяване от бедствия и аварии (ПВБА).

Трябва да се подчертае и значението на редица директиви, които също задължават организациите пряко или косвено да поддържат такъв план, който да използват в случай на възникване на непредвидени инциденти. Наличието на този план предполага, че организацията ще се справи при възникване на някакво

непредвидено прекъсване в компоненти на ИИ. Очертани са следните ***ползи от присъствието на такъв план***, а именно:

- *елиминиране на объркването и човешката грешка;*
- *редуциране на възможните причини за прекъсвания и повреди;*
- *предоставяне на отдалечени места за възстановяване;*
- *защита на данните на организацията;*
- *бързо и ефективно справяне със стресови ситуации.*

Подчертава се, че в края на 90-те години на XX век еволюцията на технологиите и широкото им приложение в организациите, както и появата на нови мениджърски подходи, премества фокуса от планиране на възстановяването от бедствия и аварии към концепцията *планиране непрекъснатостта на бизнеса (Business Continuity Planning, BCP).* Разгледани са множество дефиниции за последната, от които може да се обобщи, че това е управленски подход, който има за цел разработването и поддържането на процедури, насочени към продължаване на изпълнението на критичните за организацията процеси дори в условията на възникване на неочаквано събитие за неприемлив период.

Таблица 1

Сравнение на концепциите за възстановяването от бедствия и аварии и непрекъснатост на бизнеса

Характеристика	**Възстановяване от бедствия и аварии**	**Непрекъснатост на бизнеса**
Фокус	Информационни системи	Целият бизнес
Участващ персонал	ИТ отдел	Персонал от различни отдели
Цел	Защита на критичните процеси	Защита на цялата организацията
Основна задача	Възстановяване	Превенция
Подход за възстановяване	Конкретен фокус върху ИТ	Холистичен подход
Реакция	Реактивен	Проактивен
Концепция	Стара	Нова

Същевременно е уточнено, че често понятията „непрекъснатост на бизнеса“ и „възстановяване от бедствия и аварии“ се използват като взаимнозаменяеми. Това не е правилно, защото планирането на възстановяването от бедствия и аварии може да се определи като част от цялостната дейност по планиране на непрекъснатостта на бизнеса. Тази част по-скоро е ориентирана към възвръщане на техническото оборудване в работещо състояние и възстановяване на наличието и достъпа до критичните данни и услуги по време и след възникване на някакво непредвидено събитие. Разликата между двете концепции е изведена в таблична форма (табл. 1).

В края на изложението на първа глава са направени ***следните изводи***:

- Бързото развитие на ИТ през последните две десетилетия доведе до превръщането им в жизненоважен компонент за осъществяването на дейността на съвременната организация. Информацията, която се създава и обработва в организацията, вече е достъпна не само за нейните служители, но също за потребители, доставчици и други партньори, което изисква, отделните информационни системи и услуги да бъдат постоянно достъпни.
- В литературата все още няма общоприето понятие за ИИ и нейния състав. Това обаче не е проблем, тя да еволюира и структурата й постоянно да се усложнява. Това води до нарастване броя на заплахите пред информационната сигурност на организацията. За да се минимализира влиянието на възникнало бедствие или авария, всяка организация трябва да планира възстановяването при възникване за непредвидени събития.
- Планирането на възстановяване от бедствия и аварии е насочено към възстановяването на функционирането на отделните компоненти от ИИ на организацията, които обезпечават изпълнението на ключови бизнес процеси. То може да се възприеме като „застраховка“ срещу появата на фактори, които могат да окажат негативно влияние върху бизнес процесите в организацията. Планирането на възстановяването от бедствия и аварии е част от цялостната концепция за осигуряване на непрекъснатост на бизнеса.

Втора глава. АНАЛИЗ НА ОСОБЕНОСТИТЕ ПРИ РАЗРАБОТВАНЕ НА СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ ОТ БЕДСТВИЯ И АВАРИИ

Втора глава на дисертационния труд представя задълбочен теоретичен анализ на особеностите при разработването на стратегия за възстановяване от бедствия и аварии. Разгледани са различни съществуващи методологии за разработване на ПВБА и са анализирани възможните архитектурни и стратегически подходи и решения за реализиране на възстановяване от бедствия и аварии.

В **първия параграф** е отделено съществено внимание на нарастващата роля на управлението на риска и по-специално на ИТ-базирания риск, вследствие на дигиталната трансформация, която претърпява съвременната организация. Отчитането на тези рискове намира отражение и в ПВБА, като за неговото успешно създаване в литературата се срещат няколко сходни помежду си методологии, които да се следват.

Разгледана е ***ролята на дигиталната трансформация*** и технологиите, които са залегнали в нея. Отбелязано е, че тази тенденция е съпроводена с наличието на ИТ-базирани рискове, които непрекъснато се увеличават по брой и сложност. Изяснена е същността на понятието ***„риск“***. Подчертано е, че ***управлението на риска*** се отнася до опита на ръководството на организацията *да управлява несигурността*. То се свързва с всички дейности, условия и събития, които могат да окажат влияние върху организацията и нейната способност за постигане на зададените бизнес цели.

Централно място в управлението на риска заема процесът по ***анализ на риска***. Той включва идентифициране на заплахите и оценяване на нивата на риска и потенциалното му влияние върху дейността на организацията. Оценяването на нивото на риска обикновено се реализира на база на *вероятността и важността на заплахите* и *ефекта от тях*. ***Колкото по-голяма е вероятността от появата на дадена заплаха, толкова по-голям е този риск за организацията.*** Разгледан е модел на матрица за нивото на риска и са изяснени вариантите на

стратегии за противодействие на риска – *приемане на риска, прехвърляне на риска, намаляване на риска, избягване на риска*.

Представени са четирите основни групи риск, пред които е изправена съвременната организация, а имено: ***стратегически, финансов, риск от несъответствия, оперативен***. Отбелязано е, че първите три могат да се обединят като един общ риск, който съпътства дейността на организацията в динамичната обкръжаваща я среда, а четвъртият може да се третира като резултат от функционирането на компонентите на организацията[10] (персонал, бизнес процеси и технологии).

Посочено е, че *ИТ-базираните рискове се отнасят към групата на оперативния риск*. Стига се до извода, че ИТ-базираният риск е бизнес риск, който се асоциира с внедряването, използването и влиянието, което ИТ оказват върху организацията и следователно на управлението на ИТ-базираните рискове трябва да се обръща сериозно внимание.

Анализирани са няколко ***методологии за разработване на план за възстановяване от бедствия и аварии***, като всяка от тях е разгледана детайлно в изложението – на Kadlec и Shropshire[11], Al Hassan[12], Cook[13]. Част от методологиите, на Snedaker & Rima[14] и Tipton & Krause[15], се използват за създаване на *комбиниран или интегриран план*, който да обхваща едновременно осигуряване на възстановяването от бедствия и аварии и непрекъснатост на бизнеса. Изхождайки от сходните стъпки, които ясно се открояват във всички тях, процесът по планиране на възстановяването от бедствия и аварии е визуализиран чрез блок схемата на Фигура 1.

[10] Karkoszka, T. (2013). Risk Management as an Element of Processes Continuity Assurance. Procedia Engineering, 63, 873-877. doi:https://doi.org/10.1016/j.proeng.2013.08.286

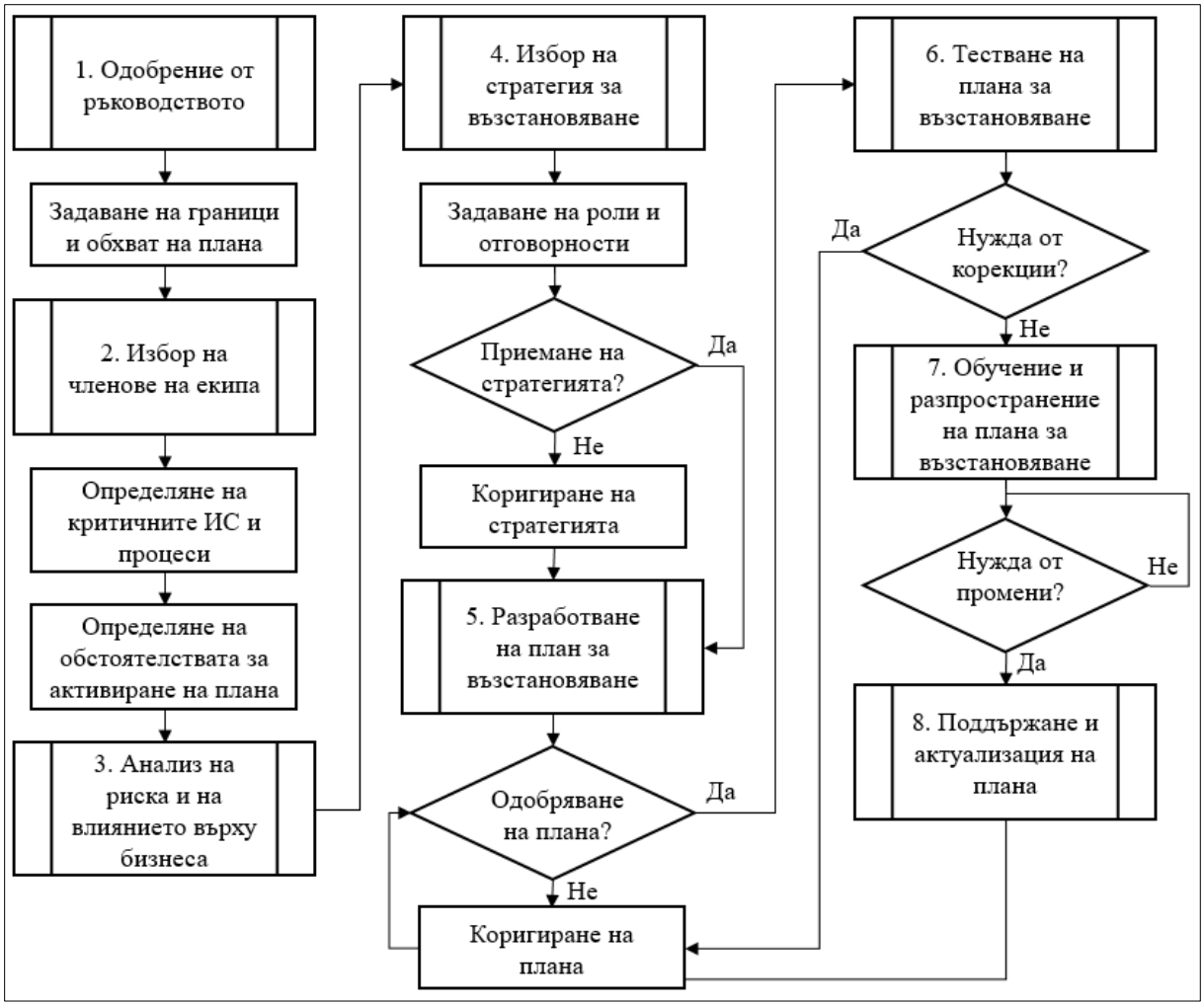
[11] Kadlec, C., & Shropshire, J. (2009). Establishing the IT disaster recovery construct. Journal of Information Technology Management, XX(4), 37-56.

[12] Al Hassan, L. (2017). Information Technology Disaster Recovery Plan (IT DRP) Framework – A study on IT Continuity for Smart City in Abu Dhabi Smart Government. Dubai.

[13] Cook, J. (2015). A Six-Step Business Continuity and Disaster Recovery Planning Cycle. S.A.M. Advanced Management Journal, 80(3), 23-33.

[14] Snedaker, S., & Rima, C. (2014). Business continuity and disaster recovery planning for IT professionals. Waltham: Syngress.

[15] Tipton, H. F., & Krause, M. (2007). Information Security Management Handbook. Boca Raton: CRC Press.



Фигура 1. Обобщена блок схема на стъпките по планиране на възстановяването от бедствия и аварии

Систематизирани са резултатите от научни изследвания, на база на които са очертани ***факторите за успешно разработване на ПВБА***. Като такива може да се посочат: *подкрепа от ръководството на организацията; наличие на достатъчен финансов ресурс; съответствие на целите на плана с бизнес целите; непрекъснато актуализиране и тестване на плана.* Приема се становището, че самото съществуване на плана не означава, че организацията е защитена и може да се справи при възникване на сериозна повреда в компоненти от ИИ. За да може да се твърди безспорно, че той е актуален и функционален, е необходимо извършването на регулярно тестване и поддържане на плана.

Във **втория параграф** са разгледани съществуващите архитектурни подходи за реализиране на възстановяване от бедствия и аварии. За целта е

отделено внимание на основните показатели, които се използват за определяне на способността за възстановяване от бедствия и аварии и са анализирани различните варианти на отдалечено място за възстановяване.

Разгледани са няколко ***основни показателя***, които се използват активно и подпомагат ИТ мениджърите при избор на архитектурен и стратегически подход за възстановяване от бедствия и аварии. Такива са: *максимално приемлив период на прекъсване (Maximum Tolerable Period of Disruption, MTPD, МППП); време за възстановяване (Recovery Time Objective, RTO, ВВ); точка на възстановяване (Recovery Point Objective, RPO, ToB); максимално приемлива загуба на данни (Maximum Tolerable Data Loss, MTDL, МПЗД).*

МППП се свързва с *продължителността от време, след която функционирането на организацията ще бъде сериозно заплашено поради невъзможността да се възстановят предлагани услуги*. В зависимост от неговата стойност се задават и границите на показателя ВВ. ***ВВ указва*** *за колко дълго организацията може да си позволи да не използва дадено приложение, услуга или система*. Това е времето от възникване на бедствието (обявяването на бедствието) до възстановяване нормалната работа на приложението, услугата или системата (връщането в нормален режим на работа). Стойността на ВВ винаги трябва да бъде по-малка от стойността на МППП или *трябва да се спазва следното ограничение:* ***ВВ ≤ МППП.***

ToB дефинира *колко данни може да си позволи да загуби организацията или това е количеството данни, които са въведени в системата в периода между създаването на последното резервно копие, респективно последно репликираните данни, и възникването на бедствието (обявяването на бедствието).* ***МПЗД се изразява*** *в задаване на максималния обем изгубена информация, който може да бъде „понесен“ от организацията и след който оперативното й възстановяване може да се окаже невъзможно.*

Подчертано е, че *определянето на показателите ToB и ВВ е основа за избиране и разработване на подходящо решение за възстановяване от бедствия и аварии.* Дефинирането на стойностите за тези показатели предполага обвързване на функциониращите ИС с целите на организацията. Това изисква определяне на

критичните бизнес процеси и свързаните с тях ИС. В тази връзка като основни проблеми се отбелязват *липсата на точно дефинирани изисквания за възстановяване,* а така също и *разминаване в разбиранията на ръководството и ИТ отдела по отношение на показателите за възстановяване.*

Разгледана е концепцията за ***седемте слоя за възстановяване от бедствия***, която е създадена от SHARE Technical Steering Committee, съвместно с IBM, през 1980 г. Тази класификация, в която най-ниският е Слой 0, а най-високият – Слой 6, продължава да се използва широко и днес. Всеки от слоевете кореспондира с различни цели, които са поставени по отношение на възстановяването от бедствия.

Изследвани са детайлно различните варианти при избор на ***отдалечено място за възстановяване***, а имено:

- *„студен“ резервен център (Cold site);*
- *„топъл“ резервен център (Warm site);*
- *„горещ“ резервен център (Hot site);*
- *мобилен резервен център (Mobile site).*

Направен е сравнителен анализ на отделните варианти (Таблица 2). Отбелязано е, че съществува *обратнопропорционална зависимост* между разходите, които се правят за подготвянето и поддържането на съответното отдалечено място за възстановяване, и показателите ВВ и ТоВ. Подчертана е важността на въпроса за ***собствеността върху съответното отдалечено място,*** като са разгледани две основни възможности: *поддържане на собствено отдалечено място за възстановяване и аутсорсинг на дейността по възстановяване.*

В **третия параграф** се разглеждат три отделни стратегически подхода за възстановяване от бедствия и аварии, а именно – *поддържане на собствен резервен център за данни (ЦД), използване на център за колокация (ЦК) и използване на облачни услуги за възстановяване*.

Таблица 2

Сравнение на възможностите на различните варианти на резервни центрове

Характеристика	Студен	Топъл	Горещ	Мобилен
Типично ВВ (RTO)	> 72 часа	30 минути – 72 часа	30 секунди – 30 минути	60 минути – 24 часа
Типично ТоВ (RPO)	Значителна загуба на данни	Известна загуба на данни	Няма загуба на данни	Сериозна загуба на данни
Компютърно оборудване	Липсва	Налично	Налично	Налично
Свързаност	Липсва	Налична	Налична	Налична
Активен преди прехвърляне към него	Не	Не	Да	Не
Разходи	Ниски	Средни	Високи	Високи
Време на готовност за пренасочване на операциите	Седмица/и	Ден/Дни	Минути/Часове	Часове
Предназначение	Отдалечено място за резервни копия	Възстановяване на некритични за бизнеса приложения	Възстановяване на критични за бизнеса приложения	Възстановяване на критични за бизнеса приложения

Отбелязано е, че в исторически аспект по-голямата част от организациите са изграждали и поддържали ***собствен резервен ЦД***. Причините за това са, че при този вариант цялата отговорност по планирането, изграждането и функционирането на ЦД е била на ръководството на самата организация, която го стопанисва, и по специално на ИТ отдела. Подчертава се, че към съвременния резервен ЦД се предявяват редица изисквания, сред които[16]: *осигуряване на непрекъснатост на достъпа до информационни ресурси, прилагане на облачни изчисления и виртуализация, гарантиране на сигурност и защита на съхраняваните данни*. В тази връзка всяка организация, която иска да разполага със собствен резервен ЦД, е необходимо да направи задълбочен анализ на

[16] Илиев, Р. (2014). Съвременни центрове за данни за нуждите на отбраната. CIO. Извлечено от http://cio.bg/6510/

съществуващите информационни потребности (услуги, ползвателите, натоварване) и да прецени дали не е по-целесъобразно да се премине към използването на специализирани наети услуги.

Анализирани са предимствата и недостатъците на ***колокацията***, която осигурява разполагане на физически сървъри на организацията или наемане на такива в специално пригоден за целта технологичен център – *център за колокация*. Сред положителните страни на този подход са посочени: *ефективност от гледна точка на направените разходи, лесна мащабируемост на наетата инфраструктура, присъствие на висококвалифицирани мрежови инженери в ЦК, високото равнище на физическа и мрежова сигурност в ЦК, гарантиране на висока достъпност (в съответствие със СНО)*. От своя страна като недостатъци са отчетени: *разположението на ЦК, липсата на мониторинг на сървъри с по-малко разпространени операционни системи, неразбиране на модела за формиране на месечната такса за плащане.*

Разгледани са особеностите на използване на ***облачните услуги за възстановяване***, като са анализирани две основни разновидности – *сторидж като услуга (Storage as a Service)* и *възстановяване от бедствия и аварии като услуга (Disaster Recovery as a Service)*. Изведени са предимствата за организациите от използването на тези услуги, основните от които са обобщени и систематизирани по следния начин: *не е нужно да се правят големи капиталови разходи, възможност за по-висока производителност и мащабируемост на облачната инфраструктура, сравнително кратко време за внедряване на облачното решение в организацията, високо ниво на поддръжка на услугата и компетентно и експертно обслужване*. Ключовите предизвикателства и заплахи пред използването на подобен стратегически подход за възстановяване от бедствия и аварии са: *сигурността на приложенията и данните, бързодействието при функциониране на приложенията, възможността с наличните изчислителни ресурси да се обслужват всички абонирани потребители, географското местоположение на ЦД на облачния доставчик.* Посочено е, че се среща и схващането, че възстановяването като услуга е вариант на колокация, при който организацията не закупува хардуер, а просто го наема.

В Таблица 3 е представено сравнение между трите разгледани стратегически подхода за възстановяване от бедствия и аварии, като са изведени най-важните им характеристики.

Таблица 3

Сравнение между различните стратегически подходи за възстановяване от бедствия и аварии

Показател	**Собствен резервен център за данни**	**Колокация**	**Възстановяване от бедствия като услуга**
Капиталови разходи	Високи	Високи	Няма или минимални
Време за внедряване	Месеци	Седмици/месеци	Часове/дни
Продължителност на контракта	Няма	Месец, тримесечие, година	Месец, тримесечие, година
Контрол върху настройването на решението	Високо ниво на контрол	Сравнително високо ниво на контрол	Ниско ниво на контрол
Време за възстановяване	Секунди до минути	Секунди до минути (ако е налична Fiber channel свързаност)	Минути до часове (зависи от СНО на доставчика)
Разходи	Високи	Относително високи	Относително ниски

В края на изложението на втора глава са направени ***следните изводи***:

- В литературата могат да се открият различни методологии за изготвяне на план за възстановяване от бедствия и аварии, но между тях съществува значителна степен на сходство както по отношение броя на разглежданите етапи, така и по отношение на наименованието и същността на дейностите, които трябва да се извършват на всеки етап.
- Независимо от избраната методология, по която ще се изготвя планът за възстановяване, от първостепенно значение е правилното дефиниране на показателите за определяне на способността за възстановяване от бедствия и аварии. Най-важните от тях са: *време за възстановяване и точка на възстановяване*. Те трябва да се дефинират по отделно за всяка информационна

система и услуга, като изключително полезно за тази цел е създаването на каталог на системите и услугите и тяхното категоризиране по степен на важност за бизнеса.

- Съществуващите стратегически подходи за възстановяване обхващат както класически решения за възстановяване като използване на собствен резервен център за данни или център за колокация, така и съвременни технологични концепции като облачните услуги, които намират широко приложение за обогатяването на информационната инфраструктура на организации от всякакъв размер и сфера на дейност.

Трета глава. МЕТОДИКА ЗА ВЪЗСТАНОВЯВАНЕ НА ИНФОРМАЦИОННАТА ИНФРАСТРУКТУРА НА ОБЩИНИТЕ В БЪЛГАРИЯ ОТ БЕДСТВИЯ И АВАРИИ

В **трета глава** на дисертационния труд, която е изцяло с практическа насоченост, е представено авторово проучване за състоянието на ИИ на общините в България, както и възможността за възстановяване на тази инфраструктура в случай на бедствия и аварии. Направен е анализ на резултатите и е изведен логически модел на ИИ на община, който впоследствие е използван, за да се оцени важността и критичността на отделните компоненти на ИИ за нормалното протичане на процесите в общината. В последния параграф на главата е ***изведен концептуален модел на решение за възстановяване*** на ИИ на община от бедствия и аварии.

В **първия параграф** е представено осъщественото от автора проучване за състоянието на ИИ на общините в България, както и възможността за възстановяване на тази инфраструктура в случай на бедствия и аварии. Аргументиран е изборът на общините за практически обект на изследване, като е посочено, че, явявайки се основни административно-териториални единици, те ***предоставят услуги на гражданите и бизнеса*** на съответната територия. Активното прилагане на концепцията за електронно управление в България през последните две години доведе до електронизиране на една голяма част от тези

услуги. Това налага необходимостта от използване на съвременни и ефективни ИКТ в общините, което е заложено и като един от приоритетите в *Стратегията за развитие на държавната администрация 2014–2020 г.* От своя страна това е свързано с наличието на подходяща ИИ, която да се поддържа, обновява и разширява регулярно.

Същевременно с новоприетия Закон за киберсигурност (обн. ДВ., бр. 94 от 13 ноември 2018 г.) се изисква поддържането на система за управление на сигурността на информацията, като част от предвидените организационни мерки включват *управление на риска, управление на инциденти и управление на непрекъснатостта на дейността или услугите*. Съобразно горепосоченото може да заключим, че в общинската администрация също е необходимо да съществува актуален ПВБА, който да гарантира бързото възстановяване на нейната ИИ в случай на възникване на непредвидено събитие или инцидент.

Посочено е, че категорията на общината е комплексна величина и при нейното изчисляване се вземат под внимание редица важни характеристики, което я прави индикатор със съществено значение. Поради това е подчертано, че се ***изследва само ИИ на общините от втора (26 на брой) и трета категория (81 на брой)***, като са отбелязани мотивите за изключване на другите категории.

Изследването се базира на проучване с анкетна карта, като преди тя да бъде изпратена до респондентите, е направена апробация на картата. За селектиране на общините, включени в извадката, е използван актуалният към 2019 година списък на общините в ЕКАТТЕ. За целите на проучването са селектирани 36 общини (по 18 от всяка от двете категории), което представлява 30% от генералната съвкупност. Извадката е направена на случаен принцип.

Броят на върнатите попълнени анкетни карти е 14. При 3 от тях респондентите не са отговорили на всички въпроси, поради което те се приемат за невалидни и се изключват от анализа. Коректно попълнените анкетни карти са 11 (5 от втора категория и 6 от трета категория), което представлява *28% от извадката* или *10% от генералната съвкупност*. Относително малкият брой върнати анкетни карти не позволява да се претендира за представителност на резултатите по отношение на цялата генерална съвкупност. Те обаче *носят*

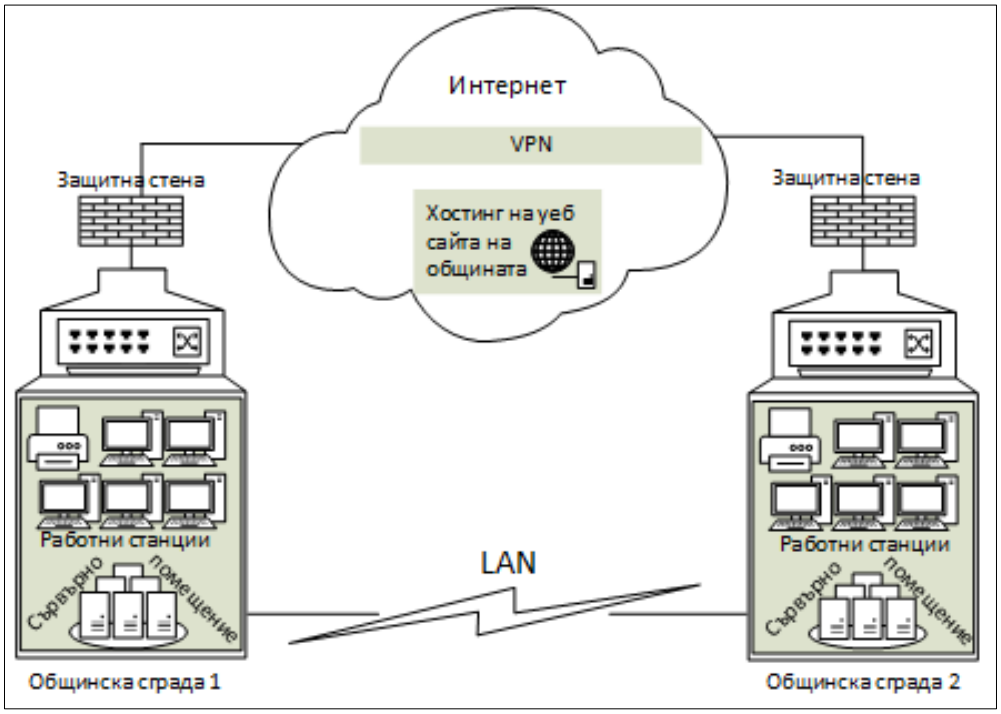
полезна информация и могат да се използват за извършване на индикативен анализ на потенциални проблеми в общини от категория 2 и 3.

Основните ***резултати и изводи от проведеното анкетно проучване*** са следните:

- общините разполагат със сравнително добре развита ИИ, в състава на която влизат няколко разнородни по вид сървъри, работни станции, мрежово и комуникационно оборудване, които са изцяло общинска собственост;
- компонентите на ИИ обикновено са разположени в съседни сгради, които в преобладаващата част от случаите имат изградена мрежова връзка помежду си;
- почти половината от разглежданите общини не разполагат с изградено сървърно помещение, което да осигурява контрол на достъпа до сървърите, възможности за резервно захранване, както и подходяща температура;
- регулярно се създават резервни копия на данните на различните сървъри, но има какво още да се желае по отношение на мястото, където те се съхраняват от гледна точка на възстановяването от бедствия и аварии и гарантиране непрекъснатост на бизнеса;
- за всяка община са регистрирани прекъсвания в работата на компоненти от нейната ИИ, като най-честата причина за тях са технологичните бедствия и хардуерните повреди;
- продължителността на отчетените прекъсвания варира от 15 минути до над 24 часа в зависимост от естеството на повредата;
- най-сериозните последици от прекъсванията са свързани с невъзможността да се предоставя определена услуга, намалена продуктивност на служителите и неизпълнение на поставените цели;
- не е наличен каталог на информационните системи и услуги, в който да е дефинирана критичността на всяка от тях за нормално протичане на процесите в общината, а на повечето места дори не се прави оценка на ИТ рисковете;

- присъствието на разписан и одобрен ПВБА е по-скоро изключение, а когато такъв съществува, той се актуализира твърде рядко и въобще не се тества.

В заключение е изведен ***логически модел на ИИ на община от изследваните категории***, показан на Фигура 2.



Фигура 2. Логически модел на ИИ на община от категория 2 и 3

От него се вижда, че сървърите са разположени в близко намиращи се сгради, като между тях съществува мрежова свързаност. Във всяка от сградите освен сървъри има разположени и работни станции, както и мрежово и комуникационно оборудване, което се използва за нуждите на изградената локална мрежа. Осигурен е достъп до Интернет само чрез един доставчик. При липса на локална мрежова свързаност между двете сгради се използва VPN връзка през Интернет. Дейностите по разработването, поддържането и хостването на уебсайта се изнасят към външна фирма изпълнител.

Във **втория параграф** изведеният логически модел на ИИ на община се използва за идентифициране на отделните компоненти на ИИ. Последните се разглеждат като информационни ресурси, които имат определена стойност. За да

се оцени как всеки от тях влияе върху изпълнението на процесите в общината и да се определят потенциалните рискове, е разработена и приложена методика за оценяване на критичността на компонентите на ИИ в общината, която включва прилагане на анализ на влиянието върху бизнеса и оценка на риска.

Приложен е анализ на влиянието върху бизнеса за един от процесите в общината – *предоставяне на услуги за гражданите и бизнеса, вчастност услуга за проверка на задължения и плащане на местни данъци и такси.* За него е установено, че в първите 8 часа последиците са свързани основно с прекъсване в предоставяната услуга и намалена работоспособност на служителите. След този период обаче се появяват и други като накърняване на репутацията на общинското ръководство, защото гражданите няма да са доволни от факта, че услугата за проверка и плащане на данъците не е налична за повече от ден.

Подчертано е, че *нивото на влияние* до голяма степен се определя на база експертна оценка в резултат на проведено интервю със собственика на процеса или участници в него. След като е направен анализът, се стига до извода, че ***стойностите на показателите за възстановяване*** са следните: *МППП – 24 часа, ВВ – 8 часа и ТоВ – 1 час* (резервните копия на данните е зададено да се правят на всеки час).

По-нататък, на основата на изведения логически модел за ИИ на община, са обособени ***пет групи информационни ресурси***: *сървъри (С)*; *работни станции (Р)*; *периферни устройства (П)*; *комуникационно оборудване (К)*; *физическа среда (Ф)*. За всеки от описаните ресурси се задава код, който е съчетание от първата буква на групата, в която влиза ресурсът, и пореден номер, който винаги се представя с три цифри (Таблица 4). Наред с това се отбелязват всички процеси, в които той участва, и на база на това се определя неговата критичност. Последната се отбелязва в колоната *„Степен на въздействие“*, която може да приема три стойности – *ниска, средна и висока* (тристепенна скала). Ако даден ресурс се използва в няколко процеса, стойността, която се задава в тази колона, трябва да нараства.

Таблица 4

Описание на информационните ресурси в общината

Код на ресурс	**Наименование**	**Процеси, в които ресурсът се използва**	**Степен на въздействие**	**ВВ**
С001	Сървър за бази от данни 1	- Предоставяне на услуга на клиенти за проверка и плащане на местни данъци и такси - Предоставяне на услуга на клиенти за гражданско състояние	Висока	8 часа
Р001	Работни станции в отдел „Човешки ресурси“	- Управление на човешките ресурси	Средна	8 часа
П001	Принтери в отдел „Човешки ресурси“	- Управление на човешките ресурси	Ниска	48 часа
К001	Комутатор 1	- Предоставяне на услуга на клиенти за гражданско състояние - Управление на човешките ресурси	Висока	8 часа
…...				

Последната колона дава информация за периода, за който съответният ресурс трябва да бъде върнат в изправно състояние. Времето за възстановяване на компонента трябва да е съобразено и да не надхвърля стойността на същия показател на ниво процес. Ако той се използва в няколко процеса, стойността, която се задава в тази колона, трябва да е най-малката посочена измежду тези процеси. Направено е заключението, че по този начин може да се определи критичността на отделните информационни ресурси, което е предпоставка, впоследствие да се създаде и каталог на информационните системи и услуги, в който се определя критичността на всяка от тях за нормалното протичане на съответните процеси, които обслужват.

Анализирани са заплахите, които могат да засегнат отделните компоненти на ИИ. Представена е ***класификация на заплахите***, като тя е разделена на две

нива. На ***първо***, заплахите са систематизирани на: *породени от природни бедствия, породени от човека и породени от заобикалящата среща.* За още по-голяма яснота е добавено ***второ ниво***, в което са обособени *физически (Ф) и дигитални (Д)* заплахи. Разработен е ***регистър на заплахите*** (табл. 5), които могат да засегнат компонентите на ИИ на общината. Той дефинира основните заплахи, които могат да възникнат и да доведат до прекъсване в работата на компонентите на ИИ. Отбелязано е, че тъй като могат да се появяват нови заплахи, добра практика е редовното преглеждане и актуализиране на регистъра на заплахите.

Таблица 5

Регистър на заплахите за ИИ

Категория заплахи	**Код на заплаха**	**Наименование на заплахата**	**Описание**
Породени от природни бедствия	Ф001	Земетресение	Опасност от разрушаване на сградите, където са разположени компонентите на ИИ
	Ф002	Наводнение	Опасност от наводняване на сградите, където са разположени компонентите на ИИ
	Ф003	Пожар	Опасност от унищожаване на сградите, където са разположени компонентите на ИИ
	…….		
Породени от технологични бедствия	Ф005	Продължително прекъсване на електричеството	Опасност от прекъсване на електрозахранване в града/региона за продължителен период от време
	Ф006	Продължително прекъсване в телекомуникационните канали	Опасност от продължително прекъсване в каналите за телекомуникация - телефон, Интернет
	…….		
Породени от човека	Ф008	Напускане/загуба на персонал	Опасност от неочаквано напускане или загуба на квалифициран персонал

	…….		
	Д001	Зловреден софтуер	Опасност от заразяване на компютър или сървър, причинено от зловреден софтуер като вирус, червей, троянски кон, руткит, рансъмуеър и др.
	…….		

Приложен е един от най-често използваните модели за оценка на риска, а именно използването на ***вероятността за проявление на заплахата и степента на въздействие, която тя оказва*** върху протичането на бизнес процесите в организацията. Използвана е ***тристепенна скала за всеки от двата показателя –*** *ниска (числова стойност 1), средна (числова стойност 2) и висока (числова стойност 3)*. Комбинираната оценка на риска се получава от умножението на съответните числови стойности за зададената *вероятност и степен на въздействие*. Определени са ***четири нива на риска***: *незначителен* (резултатна стойност 1), *приемлив* (резултатни стойности 2 и 3), *значим* (резултатни стойности 4 и 6) и *висок риск* (резултатна стойност 9). Представен е ***регистър на рисковете*** (табл. 6), в който всеки ред обвързва конкретна заплаха от регистъра на заплахите (табл. 5) с конкретен информационен ресурс (табл. 4). Вероятността се определя на основата на експертно мнение, а степента на въздействие се взема от Таблица 4. Възможно е, в регистърът на рисковете да има повече от един ред за конкретна заплаха, защото тя може да повлияе на няколко информационни ресурса едновременно.

В **третия параграф** е изследвана структурата на ПВБА и са анализирани отделните стратегически подходи за възстановяване на ИИ на община, като са отчетени техните силни и слаби страни, възможности и заплахи. На базата на анализа е предложен концептуален авторов модел на решение за възстановяване на ИИ на община от бедствия и аварии чрез използване на отдалечено място за възстановяване и технологията на сървърна виртуализация.

Посочени са ***основните секции***, които задължително присъстват в един ПВБА, а именно: *въведение, обхват на плана, история на промените, членове на екипа по възстановяване, активиране на плана, план за действие, приложения*.

Таблица 6

Регистър на рисковете

Код на заплаха	Код на инф. ресурс	Оценка на текущия риск		Ниво на риск	Действащи контроли	Приемливо ниво на риска	Действия за достигане на приемливо ниво на риска	Нужен финансов ресурс	Отговорник	Срок	Дата на оценка на остатъчния риск	Оценка на остатъчния риск		Ниво на остатъчния риск
		В	С									В	С	
Ф003	С001	Н	В	ПР	Сървърното помещение има система за детекция на пожарни огнища	ПР								
Ф003	С002	Н	С	ПР	Сървърното помещение има система за детекция на пожарни огнища	ПР								
Ф006	С001	С	В	ЗН	Няма	ПР	Осигуряване на дублирана Интернет свързаност	3000 лв.	Експерт Инф. осигуряване	1 мес.				
……														

* Н-ниска, С-средна, В-висока, НЗ- незначителен, ПР-приемлив, ЗН-значим, ВС-висок

Отбелязано е, че в Интернет съществуват множество свободни за ползване шаблони на ПВБА, но в повечето случаи в тях се наблюдават различия от гледна точка броя на секциите и техните наименования. Изследвани са ПВБА на чуждестранни общини, публикувани в Интернет, в резултат на което са направени някои *препоръки относно разработването на подобен план в българските общини*.

На базата на ***SWOT анализ*** на възможните стратегически подходи за възстановяване на ИИ на община (табл. 7) се стига до извода, че най-подходящ вариант е създаването на собствен резервен център за данни (като по-скоро се визира резервно сървърно помещение). ***Причините за избора*** на подобен вариант са обосновани от следното:

- *ще се създаде отдалечено място за възстановяване, към което да се пренасочат дейностите, ако се случи непредвидено събитие, което засяга основната сграда на общината;*
- *данните няма да напускат рамките на общината, т.е. физическият контрол върху данните ще е наличен;*
- *оборудването ще бъде изцяло собственост на общината.*

Таблица 7

SWOT анализ на възможните стратегически подходи за възстановяване

Собствен резервен център за данни	
Силни страни	**Слаби страни**
✓ Висока равнище на информационна сигурност ✓ Данните не напускат рамките на общината ✓ Собствеността на ЦД и оборудването в него е изцяло на общината ✓ Лесно разширяване на съществуващата инфраструктура	✓ Скъпоструващо решение, изискващо сериозна инвестиция ✓ Неподходящ терен за изграждането на центъра за данни
Възможности	**Заплахи**
✓ Предоставяне на услуги за колокация на други общини в областта	✓ Липса на достатъчно ИТ специалисти в общината

	✓ Сигурността на ЦД е изцяло поверена на ИТ специалистите в общината
Използване на център за колокация	
Силни страни	**Слаби страни**
✓ Високо равнище на физическа и мрежова сигурност ✓ По-малко или нулеви капиталови разходи ✓ Висококвалифицирани ИТ специалисти, работещи в ЦК	✓ Липса на собствени сървъри и оборудване ✓ Необходимост от закупуване на специален тип сървъри ✓ Неподходящо разположение на ЦК ✓ Липса на физически контрол върху данните
Възможности	**Заплахи**
✓ Лесна мащабируемост на ИТ инфраструктурата	✓ Неизпълнение на параметрите в споразумението за ниво на обслужване ✓ Неразбиране на модела за формиране на месечна такса
Използване за облачни услуги за възстановяване	
Силни страни	**Слаби страни**
✓ Нулеви капиталови разходи ✓ Намаляване на сложността на решенията ✓ Плащане само при използване на ресурси	✓ Необходимост от висикоскоростна дублирана Интернет свързаност ✓ Липса на физически контрол върху данните ✓ Съществена зависимост от доставчика на облачната услуга
Възможности	**Заплахи**
✓ Лесна мащабируемост на ИТ инфраструктурата ✓ Използване на съвременни решения за възстановяване	✓ Неизпълнение на параметрите в споразумението за ниво на обслужване ✓ Неразбиране на модела за формиране на месечна такса ✓ Съмнения относно сигурността на данните ✓ Трудности при миграция към различни платформи и решения

Подчертава се, че в организациите от публичния сектор *икономическата ефективност на инвестициите в ИТ се измерва чрез оценка на обществената полза*, поради което изграждането на резервно сървърно помещение може да не изглежда икономически оправдано, но наличието на отдалечено място за

възстановяване е предпоставка за осигуряване на непрекъснатост на процесите по предоставяне на административни услуги на гражданите и бизнеса. Приема се становището, че за нуждите на изследваните общини резервната локация може да е празно помещение в същия град, което разполага с електрозахранване, климатична система, система за детекция и предотвратяване на пожари и Интернет свързаност. Трябва да се прецени типът на строителството на сградата, където се намира помещението, разположението на сградата и наличието на определено ниво на физическа сигурност на помещението – метални врати, СОТ и др. От гледна точка на типа на отдалеченото място за възстановяване е отбелязано, че поддържането на „студен“ резервен център не е обосновано, а най-доброто решение е *„топъл“ резервен център*, който предполага наличие на сървъри, които са с последните актуализации на софтуера и при необходимост на тях могат само да се възстановят данните от последното резервно копие и трафикът да се пренасочи временно към тях.

Подчертава се, че виртуализирането на някои от сървърите на общината, от една страна, ще подобри тяхното управление, а от друга страна, ще освободи хардуерен ресурс, който може да се използва за нуждите на резервното сървърно помещение и възстановяването от бедствия и аварии. За представяне на цялостния процес по вземане на решение за сървърна виртуализация в общината е разгледан ***модел за имплементиране на виртуализация*** (фиг. 3), който представлява модифицирана версия на модела на Uddin & Rahman[17].

Фигура 3. Модел за имплементиране на виртуализация

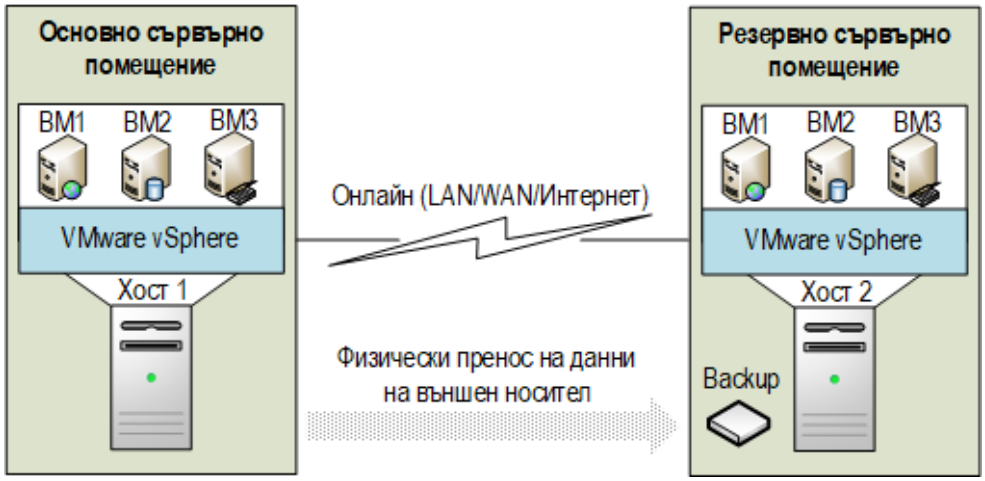
[17] Uddin, M., & Rahman, A. (2011). Virtualization Implementation Model forCost Effective & Efficient Data Centers. International Journal of Advanced Computer Science and Applications, 2(1), 69-74.

Стига се до извода, че при положително решение за консолидиране на сървъри задължително е необходимо да се закупи нов сървър, който ще изпълнява ролята на хост за виртуалната среда в основното сървърно помещение. Цената на такъв сървър може да бъде от порядъка на 12-15 хиляди лева, като минималните спецификации, които трябва да се покрият, са следните: *16-ядрен процесор, 80 GB оперативна памет, поддръжка на поне 7 хард диска по 2 TB (един от тях ще се използва за Hotspare), които да бъдат в масив RAID 10, дублирано захранване (1200W), възможност за „гореща“ замяна на охлаждащите вентилатори, 2 LAN порта на дъното, допълнителна мрежова карта*. Към него задължително трябва да се закупи и UPS, който да поддържа функционирането на виртуалната среда при проблеми с централното електрозахранване.

От гледна точка на *платформа за виртуализация* се препоръчва използването на хипервайзора на компанията VMware, която е едни от лидерите в сървърната виртуализация. Вниманието е насочено към ***версията vSphere Essentials Kit*** като добро решение от гледна точка на установената ИИ в общината. vSphere Essentials Kit е най-евтината от платените версии на платформата vSphere с цена от *823 евро (≈ 1600 лв.) за 3-годишен период* за получаване на актуализации и нови версии на софтуера и *690 евро (≈ 1350 лв.) за 1-годишен период*. Лицензът за софтуера е доживотен и не изтича, като позволява инсталирането на платформата на *максимум три хоста с по две физически ядра всеки (6 CPU лицензa)*.

vSphere Essentials Kit е насочена към малки организации, които искат да осъществят консолидиране на сървъри с последващо централизирано управление, което се извършва посредством *vCenter Server Essentials*. Тази версия е подходяща за организации с малка ИИ (5-10 сървъра), което напълно отговаря на потребностите на общините, в които се регистрират ***между 3 и 7 физически сървъра***. Налична е възможност за създаване на резервни копия на виртуалните машини посредством инсталиране на инструмента *Veeam Backup & Replication*. Тъй като е безплатен, той позволява защитата на до 10 виртуални машини, но това е напълно достатъчно за нуждите на общината.

Понеже vSphere Essentials Kit лицензът покрива до три хоста, платформата може да се инсталира и на някой от физическите сървъри, които ще се освободят след консолидацията, стига техните параметри да го позволяват. Вторият хост ще е разположен в отдалеченото резервно сървърно помещение. На него ще се съхраняват последните резервни копия на виртуалните машини от основния хост, за да може при възникнали проблеми с последния, виртуалните машини да се стартират в средата на втория хост и за определено време да поемат натоварването. Предимството на това решение се изразява във възможността, бързо да се възстанови даден сървър и по този начин да има минимално прекъсване в предоставяните услуги и процесите, обслужвани от сървъра. Описаното решение е показано на Фигура 4.



Фигура 4. Концептуален модел на решение за възстановяване на ИИ на община

Отбелязано е, че в резервното сървърно помещение се съхраняват и копия на данните от различните виртуални и физически сървъри, по същия начин както към момента такива копия се правят и съхраняват на друг компютър или на външен хард диск. Възможно е, „транспортирането“ на резервните копия на данните от основното до резервното сървърно помещение да се реализира посредством *пренасяне на външен хард диск, използване на някаква форма на репликация на данните, изпълняване на някакви потребителски дефинирани скриптове* и т.н.

В края на изложението на трета глава са направени ***следните изводи***:

- Общините от изследваните категории разполагат със сравнително добре развита информационна инфраструктура, която обаче не е достатъчно добре подсигурена от гледна точка на възникване на непредвидено бедствие или авария, като се разчита основно на поддържането на резервни копия на основните масиви от данни.
- В общините липсва разработен и разписан план за възстановяване от бедствия и аварии, което неминуемо води и до факта, че масово не се прави оценка на рисковете и съответно липсва каталог, който систематизира критичността на информационните системи и услуги.
- Показана е последователността от действия, която трябва да се изпълни, за да се направи анализ на влиянието върху бизнеса за даден бизнес процес в общината и за да бъдат оценени рисковете, влияещи върху отделните компоненти на ИИ. Методиката е насочена към ИТ персонала в общините при осъществяването на подобни дейности, които са част от цялостната методология за изготвяне и поддържане на план за възстановяване от бедствия и аварии.
- Отсъствието на отдалечено място за възстановяване е сериозен недостатък, който ИТ специалистите в общините би следвало да обмислят. Предложеният концептуален модел на решение се базира именно на идеята за наемане на отдалечено резервно сървърно помещение, а с помощта на сървърната виртуализация е предвидена възможност за реализиране на успешно и бързо възстановяване на информационната инфраструктура на общината в случай на бедствие или авария.

В **заключението** на дисертационния труд са систематизирани проблемите, решенията, които се предлагат, а така също са отбелязани и основните му приноси от научна и научно-приложна гледна точка.

Планирането и организацията на дейностите по възстановяване от бедствия и аварии има потенциала да гарантира високо ниво на сигурност и поверителност на данните, постоянен достъп до критичните бизнес приложения и услуги и съответно непрекъснато функциониране на критичните бизнес процеси.

IV. СПРАВКА ЗА ОСНОВНИТЕ ПРИНОСИ В ДИСЕРТАЦИОННИЯ ТРУД

Теоретичната и практическа значимост на труда и неговите ***основни приноси*** се изразяват в следното:

1. Направен е анализ на ролята и значението на възстановяването от бедствия и аварии в съвременните организации и са разгледани задълбочено показателите, използвани за определяне на способността за възстановяване.
2. Извършен е критичен анализ на особеностите на различните архитектурни и стратегически подходи за възстановяване от бедствия и аварии.
3. Проведено е анкетно проучване за състоянието на информационната инфраструктура на българските общини от категория 2 и 3 и възможностите за бързото й възстановяване, като се доказва липсата на разписан план за възстановяване от бедствия и аварии и използването на съвременни решения за възстановяване.
4. Разработена е и е приложена методика за оценяване на критичността на компонентите на информационната инфраструктура в общините на базата на приложение на методите за анализ на влияние върху бизнеса и оценка на риска.
5. Предложен е концептуален модел на решение за възстановяване на информационната инфраструктура на българските общини от изследваните категории чрез използване на отдалечен резервен център и технология за сървърна виртуализация.

V. СПИСЪК НА ПУБЛИКАЦИИТЕ, СВЪРЗАНИ С ДИСЕРТАЦИОННИЯ ТРУД

Статии:

1. **Божиков, А.** Репликация на данните - в служба на контролинга. // Европейските измерения на правото, контрола и екологията: Статии, АИ Ценов, Свищов, 2008, с. 76-84.

Доклади:

1. **Божиков, А.** За важността на възстановяването от ИТ бедствия и аварии и връзката с поставените бизнес цели. // Икономическо благосъстояние чрез споделяне на знания : Международна научна конференция - Свищов, 9-10 ноември 2016 г., АИ Ценов, 2016, т. 3, с. 358 – 362.
2. **Божиков, А.** Облачни услуги и възстановяване от ИТ бедствия и аварии. // Информационните технологии в бизнеса и образованието : Международна научна конференция - Варна, 17 октомври 2014 г., Издателство „Наука и икономика“, 2014, с. 493- 499.
3. **Bozhikov, A.** Disaster Recovery Planning – the obvious that we miss or underrate // Securitatea informationala 2012 : IX-a Conferinta internationala, Chisinau, 2012, pp. 69 -72.
4. **Божиков, А.** Аварийно възстановяване на данните и клауд компютинг. // Приложение на информационните и комуникационните технологии в икономиката и образованието : Международна научна конференция - София, 2-3 декември 2011 г., , 2011, с. 513-519.
5. **Божиков, А.** Планът за възстановяване от бедствия и аварии в малките и средните предприятия. // Системи за управление на бизнеса в малки и средни предприятия : Международна научна конференция - Свищов, 23-24 април 2010 г., АИ Ценов, 2010, с. 256-261.

ДЕКЛАРАЦИЯ ЗА ОРИГИНАЛНОСТ И ДОСТОВЕРНОСТ

от Асен Петров Божиков

Във връзка с провеждането на процедура за придобиване на образователна и научна степен „доктор“ по научната специалност „Приложение на изчислителната техника в икономиката“ декларирам:

1. Резултатите и приносите в дисертационния труд на тема: „Възстановяване на информационната инфраструктура при бедствия и аварии“ са оригинални и не са заимствани от изследвания и публикации, в които авторът няма участия.
2. Представената от автора информация във вид на копия на документи и публикации, лично съставени справки и др. съответства на обективната истина.
3. Резултатите, които са получени, описани и/или публикувани от други автори, са надлежно и подробно цитирани в библиографията.

гр. Свищов Д Е К Л А Р А Т О Р:…….

/Асен Божиков/