И К О Н О М И Ч Е С К И У Н И В Е Р С И Т Е Т – В А Р Н А

Стойчо Василев Стоев

Софтуерен модел за управление и оценка на ИТ риск

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 05.02.08

„Приложение на изчислителната техника в икономиката"

Варна

2017

Дисертацията е разработена в общ обем от 156 страници, в т.ч. основен текст – 156 страници, 51 фигури, 4 таблици, 93 литературни източника.

Защитата на дисертационния труд ще се състои на .. .. …. г. от ..:.. часа в зала … на Икономически университет – Варна на заседание на научно жури, назначено със Заповед …. от .. .. …. г. на ректора на Икономически университет - Варна.

Материалите по защитата са на разположение на интересуващите се на Интернет страницата на Икономически университет - Варна

www.ue-varna.bg

Стойчо Василев Стоев

Софтуерен модел за управление и оценка на ИТ риск

АВТОРЕФЕРАТ

на дисертационен труд
за присъждане на образователна и научна степен "доктор"
по научната специалност 05.02.08
„Приложение на изчислителната техника в икономиката"

НАУЧЕН РЪКОВОДИТЕЛ:
доц.д-р Тодорка Атанасова

НАУЧНО ЖУРИ

1. проф.д-р Емил Денчев	УНСС - София
2. доц.д-р Веселин Попов	СА „Д. А. Ценов" -Свищов
3. доц.д-р Ваня Лазарова	УНСС - София
4. доц.д-р Тодорка Атанасова	ИУ-Варна
5. доц.д-р Надежда Филипова	ИУ-Варна

Варна
2017

Дисертационният труд е обсъден и насочен за защита от катедра “Информатика” при Икономически университет – Варна.

Автор: Стойчо Василев Стоев
Заглавие: Софтуерен модел за управление и оценка на ИТ риск
Тираж: …..
Излиза от печат на .....
Отпечатан в Печатна база
На Икономически университет - Варна

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Актуалност на проблема (темата)

Нашето съвремие се характеризира с все по-взаимосвързани и по-взаимозависими процеси на развитие на информационните технологии и динамиката на бизнес средата. Тези два процеса са предизвикателство пред научните изследвания и практическите решения в съвременната икономика. Компютърната наука, като част от икономическото развитие на обществото, се стреми да следи или изпреварва тенденциите в икономическите процеси.

Конкурентната среда и технологичното развитие еволюционно изместват фокуса от проблема за оперативното развитие на бизнеса към перспективите за развитие и прогнозиране на бизнес средата при създаване и реализация на фирмените продукти и услуги. Ефективността на фирмената дейност е свързана с процеси по анализ и управление на риска. Сложните взаимовръзки между отделните източници на риск предполагат използване на адекватен модел за изграждането им и съответно софтуерна система за автоматизиране на етапите по обработка на рисковата информация.

Всяко внедряване на информационни технологии носи със себе си непосредствени рискове както за ИТ организациите, така и за потребителите на техните услуги. Следователно съвременното управление на компаниите трябва да анализира тези рискове, както и да планира мерки, които трябва да бъдат предприети за редуциране на въздействието им.

Целите пред фирменото управление на ИТ риска, могат да бъдат разгледани в две направления:

- повишаване на ефективността на проектите, реализирани от ИТ фирмите;

- адекватно ресурсно обезпечение на евентуалните загуби от рисковата среда.

Следователно необходимостта от подходящи ИТ решения в областта на управлението на риска при реализиран на ИС е обоснована и актуална.

2. Обект и предмет на изследване

Основните проблеми при осъществяване на управлението на риска за информационните системи са свързани с огромното количество информация, която трябва да бъде анализирана и обработена. Обемът на тази информация зависи както от потенциалните източници на риск, така и от непрекъснатия процес по нейното управление за предприемане на адекватни мерки за намаляване на щетите в ИТ организациите. Т.е. съществува необходимост от автоматизация на всеки един от етапите за оценка и управление на риска в информационните системи.

На тази основа предмет на изследването е автоматизирането на процесите по управление на риска при реализиране на информационни системи.

Обект на изследване е оценката на риска на информационните системи като съвременна тенденция от развитието на бизнес организациите.

3. Цели и задачи на изследване

Цел на дисертационния труд е изграждане на модел на система за оценка и управление на риска при създаване и внедряване на информационни системи, съответстваща на съвременните тенденции в научните изследвания и добрите практики. С реализиране на разработената система ще се подобри надеждността и ефективността на информационното осигуряване на бизнес процесите в процесите на разработване и внедряване на ИС.

За реализация на поставената цел предлагаме да бъдат решени следните задачи:

1. Изследване на същността на риска и спецификата му в информационните технологии.
2. Прецизиране на областта на приложение на информационните системи, подходящи за използване на системи за управление на риска.
3. Изготвяне на класификация на възможните източници на риск за ИС с цел създаване на регистър на ИТ рисковете за подпомагане на практическата оценка на заплахите.
4. Реализация на модел за управление на риска при внедряване и експлоатация на ИС проекти.
5. Разработване на информационна система за управление на риска за подпомагане на оценката и вземането на решения от ИТ бизнеса.

4. Теза

Основната теза на настоящата дисертация е необходимостта от разработване на приложение – система за оценка и управление на риска в процеса по внедряване на информационните системи (ИС), подпомагащо вземането на решения в ИТ сферата. В резултат очакваме повишаване на функционалността на ИС и подобряване на управлението като цяло в бизнес организацията.

5. Методология на изследване

При изследването на процесите по управление на риска са приложени сравнителният, историческият и системният подход. За реализиране на прототип на софтуерна система за обработка на риска са използвани методите на логическия анализ, моделиране и проектиране на информационни системи и др.

6. Апробация на дисертационния труд

По темата на дисертацията са публикувани два доклада и две статии.

Разработен е приложен програмен продукт за автоматизиране на процеса по изчисляване на основните характеристики на жилища от гледна точка на риска и на тяхна база да се състави оптимален (по съответен критерий) портфейл от избрани имоти.

Въз основа на предложените концептуален и логически модел е предложен прототип на система за информационно осигуряване на процесите по управление на ИТ риск на информационни системи. Прототипът на софтуерна система за оценка и управление на риска е разработена като специализирана ИС за подпомагане на управленческите дейности на ИТ фирма.

II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд има общ обем от 156 страници и се състои от предговор, изложение в три глави, заключение и списък с използваната литература от 93 източника. В основния текст са включени 4 таблици и 51 фигури.

Структурата на изложението е следната:

Въведение

Глава първа. **Управление и оценка на ИТ риска**

1.1. Същност и свойства на риска

1.2. Рискът в областта на ИТ

1.3. Управление на риска

1.3.1. Идентифициране на риска

1.3.2. Анализ на риска

1.3.3. Оценка на риска

1.3.4. Обработка на риска

1.3.5. Контрол и мониторинг

1.4. Основни методи и техники в процеса на управление на риска

1.4.1. Методи за оценка на вероятността от настъпване на събития

1.4.2. Методи за идентифициране на риска

1.4.3. Методи и техники за оценка на риска

Глава втора. **Модел за управление и оценка на риск в ИС**

2.1. Рискът при реализиране на ИС

2.1.1. Информационни нива за вземане на решение

2.1.2. Управление на риска в съответствие с обхвата на ИС

2.1.3. Разпределение на продуктовия риск

2.2. Бизнес концепция за източниците на риск за ИС

2.2.1. Трислоен профил на средата на ИС

2.2.2. Класификация на източници на риск за ИС

2.3. Логически модел

2.3.1. Принцип на изграждане на йерархична структура на източниците на риск

III. КРАТКО ПРЕДСТАВЯНЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Глава първа. Управление и оценка на ИТ риска

Изследването в първа глава е насочено към разглеждане и анализ на основните характеристики на риска и по-специално на ИТ риска. Разглеждат се основните етапи в процеса на управление на риска. Изследвани са съществуващите методи и са анализирани техните недостатъци за управление на ИТ риска.

Информационните технологии не остават изолирани от изследванията в областта на теорията на риска. Рискът се разглежда в няколко основни направления, в зависимост от направлението или обекта на приложение на компютърните технологии:

- Управление на риска в областта на сигурността на информацията.
- Анализ на риска при реализация на мрежова инфраструктура.
- Управление на риска при експлоатация на информационни системи.
- Информационни системи за управление на риска.

Приема се предложената категоризация на рисковете[1], която въпреки че е изведена от общата теория на риска и се отнася за всички области на човешката дейност, това деление на видове рискове е в голяма степен близко до рисковете, свързани с IT областта.

I. **По своята същност неизвестни** (inherently unknowable). Някои рискове по своята същност са непознаваеми. Това са истинските неизвестни, където несигурността е скрита в бъдеще, незабелязана, докато не възникне и прояви нейното въздействие – изненадата.

II. **Времево зависими** (time-dependent). Други рискове са зависими от времето и се появяват само с течение на времето. В процеса на

[1] Hillson, David, Exploiting Future Uncertainty : Creating Value from Risk. Ashgate Publishing Group, 2015

идентифициране на риска може да се анализира само ограничен период в бъдещето, което предполага че някои рискове съществуват под времевия хоризонт.

III. **Зависими от развитието** (progress-dependent). Някои пораждащи се рискове са непредвидими, защото са зависими от развитието. Те не могат да бъдат идентифицирани, докато не бъде постигнат определен напредък.

IV. **Зависими от реакция** (response-dependent). Последната група от рискове, които могат да останат скрити в процеса на идентифициране, са зависими от реакция, известни също като вторични (следствени) рискове, които се проявяват само когато са предприети действия за реакция на съществуващ риск.

Обобщавайки изследванията в областта на риска, обособяваме следните характеристики на риска:

1. Рискът е комплекс от множество елементи, всеки от които притежава потенциални свойства, които го характеризират.
2. Случайността в същината на риска се изразява в момента и мястото на негово възникване.
3. Рискът е тясно свързан с динамиката на средата. По-динамичната среда предизвиква по-голяма вероятност от възникване на риск, включително и възможността няколко източника на риск да си въздействат по между си.
4. Количествената оценка на риска е възможност за неговото изучаване и анализ и задължително условие за компютърното му моделиране.
5. Рискът е явление, засягащо всяка област на съвременните социални, икономически, природни и други области, и не изключва влиянието му и върху информационните технологии.

6. Елементите, част от риск комплекса, се характеризират с продължителност и потенциална сила на въздействие.

В анализа на приложението на изследванията в областта на риска и прилагането им при компютърните науки, най-малко проучвания са извършени при изследване на риска при експлоатация на автоматизирани информационни системи (АИС). Като цялост авторите дефинират част от възможните рискови фактори за една АИС, предлагат методики за оценка на заплахите и уязвимостите, измерване на рисковете с оценка по два фактора, изброяват възможни подходи за управление на рискове.

В параграф 1.2 е предложено определение за риска в областта на ИТ бизнеса:

ИТ рисковете произтичат от спецификата на ИТ средата, предизвикващи негативни ефекти върху развитието на процесите в нея и по своята същност са познаваеми с потенциал за количествена оценка

За разлика от други цитирани автори не включваме **случайността** като елемент от разбирането на риска, защото в информационните технологии тя е синоним на поредица от действия, предизвикващи събития с определено въздействие, и не е точен термин за прецизиране на риска.

В определението се включва понятието **познаваеми**, защото само ако рисковете са известни, могат да се класифицират, оценят, да се предвиди техният ефект и съответно да се планират мерки за предотвратяването им. Следователно тяхната познаваемост дава възможност да се интегрират в система за управление на риска, включително и при компютърна реализация.

Друг важен акцент от предложеното определение е **количествената оценка** на риска. Тази оценка е възможност от една страна да се съпоставят различните източници на риск в процеса по управлението им и от друга страна да се сравнят различни рискови среди. Без наличие на

количествено оценяване на източниците на риск не може да се реализира ефективна компютърна система за управление на риска. Дори и в случаите, когато източниците на риска са оценени с грешка от действителните стойности, това е по-добър вариант от компютърно представяне във вида: има наличие на риск, липсва риск.

Понятието **процес** е включено в дефиницията по две основни причини: първо, защото дава по-общо възприятие на дейностите в ИТ областта; от друга страна е точно понятие за възможността за възникване на риск като следствие от последователност на действия.

От възможните последствия от риск – негативни или позитивни – значим е негативният ефект от риска, защото за разлика от сферата на инвестициите в ИТ областта не намира голямо приложение позитивният риск.

В параграф 1.3 се изследва процесът по управление на риска. Управлението на риска все по-често се разглежда като част от концепцията за устойчиво фирмено развитие и усъвършенстване. То представлява логичен процес или подход, който има за цел да премахне или поне да намали нивото на риска, съпътстващ реализацията на фирмената политика и достигане на организационните цели. Управлението на риска е част от управленската отговорност, която всеки ръководител на стопанска или публична организация носи [2].

В дисертацията се приема, че за ИТ риск важат "универсалните закони за управление на риска"[3], които са обобщени в следните четири акцента:

[2] Богданова, М., Е. Парашкевова, К. Павлова. Ефективно управление на оперативния риск в българските компании. // Диалог, ИНИ, Извънреден тематичен II, август 2012, с.172.

[3] Hillson, D. Exploiting Future Uncertainty Creating Value from Risk. Ashgate Publishing Group, 2010, p. 60.

I. Риска е несигурност. Рискът е нещо в бъдеще, което може или не може да се случи. Това е от жизненоважно значение за правилното разбиране на риска и неговото управление.

II. Определящи са риск целите. Не е възможно да има несъществен риск по дефиниция. Докато различни видове технологии за управление на риска се фокусират върху различни видове следствие, установено е общо мнение, че рискът трябва да промени нещо, тоест да повлияе на средата.

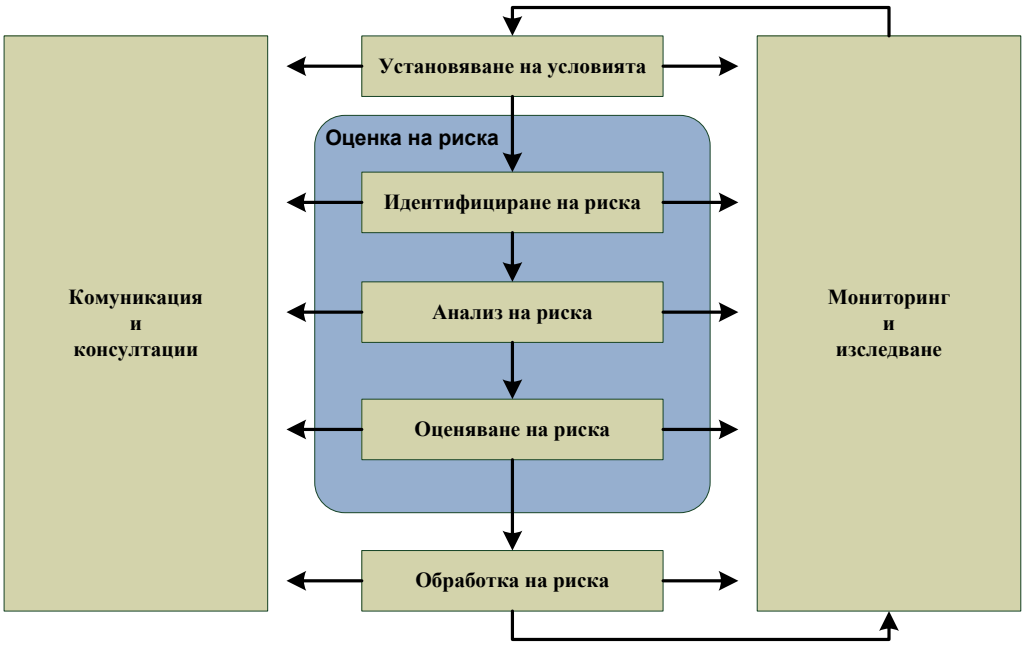
III. Управлението на риска е процес. Процесите по управление на риска могат да имат различни стъпки, но всички подходи към това управление осигуряват рамка, която има за цел да постигне оптималност между ефективност и ефикасност.

IV. Хората управляват риска. Човешките аспекти по управлението на риска са жизненоважни за успеха и ефективността. Хората установяват праговете на риска, идентифицирането на рисковете, оценка на степента на несигурност и размера на евентуалното въздействие, предлагат подходящи отговори и прилагат ответните действия.

Като база за изследване на етапите по управление на риска се приема стандартът ISO 31000[4]. ISO 31000 признава значението на обратна връзка чрез два механизма: това са „мониторинг и изследване" на резултатите и „комуникация и консултации" (фиг. 1). Механизмът за мониторинг и изследване гарантира, че организацията следи проявлението на риска и се учи от опита. Механизмът за комуникация и консултация е представен в ISO 31000 като част от процеса по управление на риска, но той може да бъде считан за елемент от подкрепящите инструменти.

Процесът по управление на риска се състои от няколко стъпки:

[4] www.iso.org/iso/home/standards/iso31000.htm (20.6.2015).



Фиг. 1. Процес за управление на риска (на базата на ISO 31000)[5]

Идентифициране на риска

Идентификация на риска е критичната първа стъпка в процеса по управление на риска [6] . Нейната цел е ранно и непрекъснато идентифициране на възможните рискове в рамките на проекта или външни за него. Тези рискове са събития, които, в случай че възникнат, ще имат отрицателно въздействие върху способността на проекта да постигне планираните резултати.

Анализ на риска

Процесът по анализ на риска включва: идентифициране и определяне на размера на несигурност; оценка на въздействието върху резултатите, които ни интересуват; изграждане на модел за анализ на риска, който изразява тези елементи в количествена форма. В последствие се изследва моделът, чрез симулация и анализ на чувствителността, както и вземане на

[5] A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. AIRMIC, Alarm, IRM. 2010, p. 8

[6] Garvey, P. R. Analytical methods for risk management: a systems engineering perspective. CRC Taylor & Francis Group. Boca Raton. 2009. p. 5.

решения за управление на риска; решения, които могат да ни помогнат рискът да се избегне, намали или да се справим с него по друг начин[7].

В хода на анализа на риска е необходимо да бъде събрана уместна и надеждна информация за евентуалните заплахи, идентифицирани и анализирани (въздействие, вероятност), а след това оценени. В този случай анализът на риска е насочен към картографиране на областите и процесите, които носят най-голям риск, и при определяне и оценка на рискове, присъстващи в организации, които могат да бъдат проверени. Ако анализът включва население (например институции, централни подсистеми, партньорства, частни лица) с голям брой елементи, ключовата цел на анализа на риска е да се подредят елементите, съгласно избраните критерии за риска, т.е. да се създаде един вид "риск класиране" в интерес на избора на рисковите елементи [8].

Оценка на риска

Оценката на риска [9] е процесът на идентифициране, оценка и приоритизиране на рисковете за информационната сигурност. Тя изисква внимателен анализ на заплахите и уязвимостта на информацията чрез определяне на степента, до която обстоятелства или събития биха могли да окажат отрицателно въздействие върху организацията и вероятността, с която ще възникнат такива обстоятелства или събития.

Оценките на риска[10] е прието да се прилагат за отделни области, процеси и процедури. Те са приемливи за прилагане, само когато са необходими за изпълнение на целите по конкретни оперативни причини. В допълнение рискове, предизвикани от промени в средата, рядко се идентифицират и трудно се управляват систематично.

[7] http://www.solver.com/risk-analysis-process (29.4.2015).
[8] Domokos, L. et al. Risk Analysis and Risk Management in the Public Sector and in Public Auditin. // Public Finance Quarterly, 2015, v.1, p.4
[9] Guide for Conducting Risk Assessments. National Institute of Standards and Technology, 2012, p. 6.
[10] Beauchamp-Akatova Elena, Curran Richard. From initial risk assessments to system risk management. // Journal of Modelling in Management, 2013, Vol. 8, №3 pp. 262 - 289.

Фазата на оценка на риска[11] включва критичен преглед на всички планове за действие, предложени в по-ранната фаза от гледна точка на ефективността за намаляване на общото ниво на индекса на опасност, размера на необходимите ресурси и степента на проектантски и инженерингови промени, необходими за избор на оптималния курс на действие за постигане на целите за безопасност и надеждност.

Изведени са три основни аспекта при оценката на риска:

а) скали и критерии, по които може да се измерва рискът;

б) оценка на вероятността за събитието;

в) измерване на рисковете.

Тяхната задача е да помогнат при изграждане на един специфичен модел за оценка на риска в определена област от бизнеса, в следствие от общата теория за управление на риска.

Обработка на риска

Планирането и действията, свързани с ограничаване на риска, често водят до допълнителни разходи. Екипът по управление на риска трябва да направи анализ на разходите/ползите, за да реши какви са възможните действия за обработка (третиране) на риска.

Приема се, че възможните реакции от възникването на риск са четири :

- **Намаляване на риска.** Нивото на риска трябва да бъде намалено чрез подбор на проверки, така че остатъчният риск да може да се преоцени като приемлив.
- **Запазване на риска.** Решението за запазване на риска, без по-нататъшни действия, трябва да се взема в зависимост от оценката на риска. Ако нивото на риска отговаря на критериите за

[11] Rao Tummala, V.M., Y.H. Leung. A risk management model to assess safety and reliability risks. // International Journal of Quality & Reliability Management, 1996, Vol. 13, №8 pp. 53 - 62.

приемливост, не е необходимо прилагането на допълнителни мерки за контрол и рискът може да бъде задържан.

- **Избягване на риска.** Когато установените рискове се считат за прекалено високи или разходите за изпълнението на други възможности за обработки на риска надхвърлят ползите, може да се вземе решение напълно да се избегне рискът.
- **Прехвърляне на риска.** Прехвърлянето на риска включва решение за споделяне на определени рискове с външни лица.

В параграф 1.4 са разгледани основни методи и процедури[12] за анализ на рисковете. В зависимост от избрания метод при една и съща ситуация е възможно да се изчислят различни оценки на риска. Целесъобразността на избрания метод зависи от наличната информация за определящия решението, от размера на бюджета и целите на вземащите решения. Всички те се основават на предпочитанията на вземащите решения за определен избор на конкретна алтернатива. Съществуват голям брой други методи за анализ на риска, въпреки че само част от тях са доказали популярност по отношение на практическото си прилагане.

Според приложимостта в отделни етапи от процеса по управление на риска смятаме, че методите могат да се класифицират в следните основни групи:

- методи за оценка на вероятността от настъпване на събития;
- методи за идентифициране на риска;
- методи и техники за оценка на риска.

Методите за оценка на вероятността от настъпване на събития се характеризират с два основни момента: резултатът от прилагане на метода е количествено изразяване на риска; изследват източниците на риск, а не

[12] Schubert, R. Analyzing and managing risks - on the importance of gender differences in risk attitudes. // Risk Management. Bradford: Emerald Group Publishing, 2006. ProQuest eLibrary. p.706.

толкова последствията от възникването им. Основните методи за оценка на вероятността от настъпване на неблагоприятни събития са следните[13]:

- метод на построяване на дърво на събитията;
- метод „Събитие-последствие”;
- метод на дървото на отказите.

След анализ на изложените методи стигаме до извода, че йерархичната структура е подходяща за обработка на ИТ риск. Недостатък на методите е логическата обвързаност на елементите в нея.

При методите за идентифициране на риска се изгражда информационен регистър на рисковете (понякога наричан „портфолио на риска”), които са известни и значими за системата.

Дефинирани са три основни метода за идентифициране на риска при анализ на конкретни процеси:

1. Метод на анализа на статистически данни от минали неблагоприятни събития.
2. Метод на теоретичния анализ на структурата на причинно-следствените връзки между отделни изследвани процеси.
3. Метод на експертния подход.

Изборът на метод за идентифициране на риска се основава на ресурсите, с които разполага фирмата и с наличието на достоверни данни от предишни или настоящи изследвания на риска в конкретна или подобна среда. Оптимално решение за оценката на риска е използването и миксиране на няколко метода за по-точни резултати.

От представените методи и техники за оценка на риска се стига до извода, че относно ИТ риска тяхното приложение е ограничено. Използването им е възможно като част от един по-общ йерархичен модел.

В заключение на главата се обосновава нуждата от разработване на нов модел за обработка на ИТ риска, обусловен от неговите специфики.

[13] Хохлов, Н.В. Управление риском. Москва: Юнити, 2001, с. 62.

Глава втора. Модел за управление и оценка на риск в ИС

В контекста на ИТ организацията [14] управлението на риска се представя като интеграция на хора, процеси и инструменти, които заедно осигуряват ранно и непрекъснато идентифициране и обработка на рисковете в или за организацията. В крайна сметка управлението на риска има за цел да създаде и поддържа цялостна информационна система за рисковете, така че възможностите и целите за изпълнение да постигнат желания ефект.

В управлението на риска при реализация на ИС дефинираме областта на приложение за модела. Предлагат се следните няколко направления:

- зависимост на управлението на риска от мащаба на ИС;
- разпределение на продуктовия риск ;
- ресурсна обезпеченост при управлението на риска.

От гледна точка на софтуерното производство видовете ИС, чрез призмата на управлението на риска, се обособяват в няколко категории:

- *Корпоративни ИС*.
- *Среднофирмени ИС.*
- *ИС за малък бизнес.*
- *Персонални ИС (ПИС).*

Следователно може да се отбележи, че от модел за управление на риска се нуждаят фирми, производители на ИС, насочени към втората категория софтуерно производство, а именно среднофирмени ИС. В тази категория добавената стойност от реализацията на ИС позволява да се постигнат следните основни цели:

- финансиране на процеса по управление на риска;

[14] Garvey, P. R. Analytical methods for risk management: a systems engineering perspective. CRC Taylor & Francis Group. Boca Raton. 2009. p.10.

- чрез управлението на риска да се оптимизират печалбите;
- намаляване на разходите на фирмата във фазите на внедряване и съпровождане на продукта;
- диференциране на източниците на риск, произтичащи от производителя и клиента;
- повишаване на функционалността на продукта, като се намалява влиянието на рисковите фактори.

При реализацията на конкретен продукт, във взаимоотношенията между производител и клиент, съществуват три множества от потенциални източници на риск (фиг. 2).

Фиг. 2. Разпределение на продуктов риск

Приема се, че възможните решения за управление на риска са:

- *Производителят поема управлението на продуктовия риск.*
- *Споделяне на продуктовия риск.*
- *Клиентът управлява продуктовия риск.*

Определят се специфичните характеристики на елементите в софтуерното производство, за които се смята, че са подходящи при изграждане на модел за управление на ИТ риск в реализацията на ИС и те са следните:

А) При реализация на средно големи ИС, при които добавената стойност позволява отделяне на ресурси за управление на риска.

Б) Средно големи фирми от ИТ бранша с цели за реализиране на един или няколко продукта.

В) Производителят поема отговорността за управление на продуктовия риск.

Г) Управлението на риска е част от стратегията на фирмата за оптимизиране на своята дейност.

В дисертацията се приема, че под ИТ риск се разбира множеството от източници на риск при внедряване и реализация на ИС.

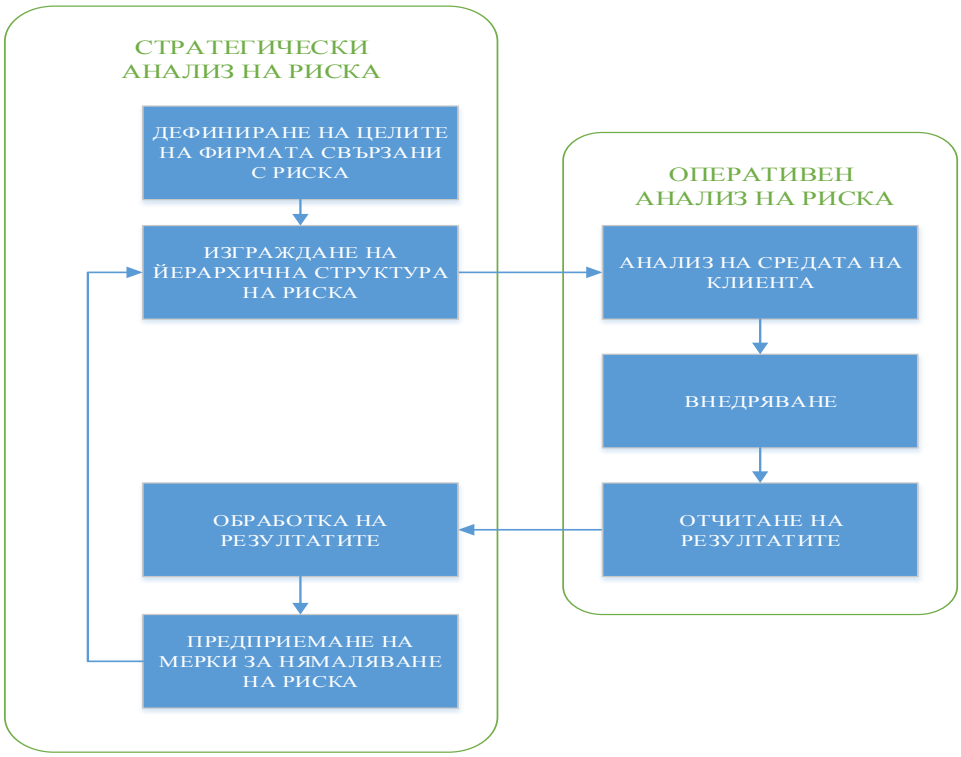
В параграф 2.2 се изследва зависимостта между целите на фирмата във връзка с управлението на риска, като основен етап от цялостното управление не само на риска, но и на организацията на работа в самата фирма и нейните връзки с клиентите. От гледна точка на източниците на риск дефинирането на основните цели за фирмата ще спомогне да се определи кои източници на риск са значими и кои не са, и ще даде възможност за приоритизиране на основните източници.

При компаниите от областта на софтуерното производство фирменото развитие преминава през няколко фази:

1. Създаване и разпространение на първоначален продукт – ИС.
2. Създаване и разпространение на съпътстващи модули, интеграционно свързани с първоначалния продукт, с цел по-пълно задоволяване на нуждите на клиента или
3. Създаване и разпространение на концептуално нови продукти в други сфери на приложение.

В рамките на софтуерната фирма са дефинирани две основни направления за управление на риска (фиг. 3):

- Стратегическо управление на риска (СУР).
- Оперативно управление на риска (ОУР).



Фиг. 3. Общ модел на фирменото управление на риска

Връзката между стратегическото и оперативното управление на риска е пряка и взаимосвързана. Докато стратегическото управление изследва общия замисъл на риска и тенденциите в неговото изменение, то оперативното касае конкретен случай и конкретна среда. Получените резултати се обработват и имплементират в базата от данните на СУР. Така с всяко ново внедряване се постига актуализация и допълване на общата база от данни на източниците на риск за дадената фирма и нейните продукти.

В параграф 2.2.1 се предлага трислоен модел на средата на ИС (фиг. 4).

Фиг. 4. Общ модел на източниците на риска в ИС

Определя се, че основна цел при изследване на риска в трислойния модел е анализът на най-динамичната част от източниците на риск, а именно взаимовръзката между ИС и средата на клиента.

В процеса на управление на риска при реализация на ИС се приема, че от съществено значение е познаването на източниците на риск. В този смисъл се предлага класификацията им в три основни разреза:

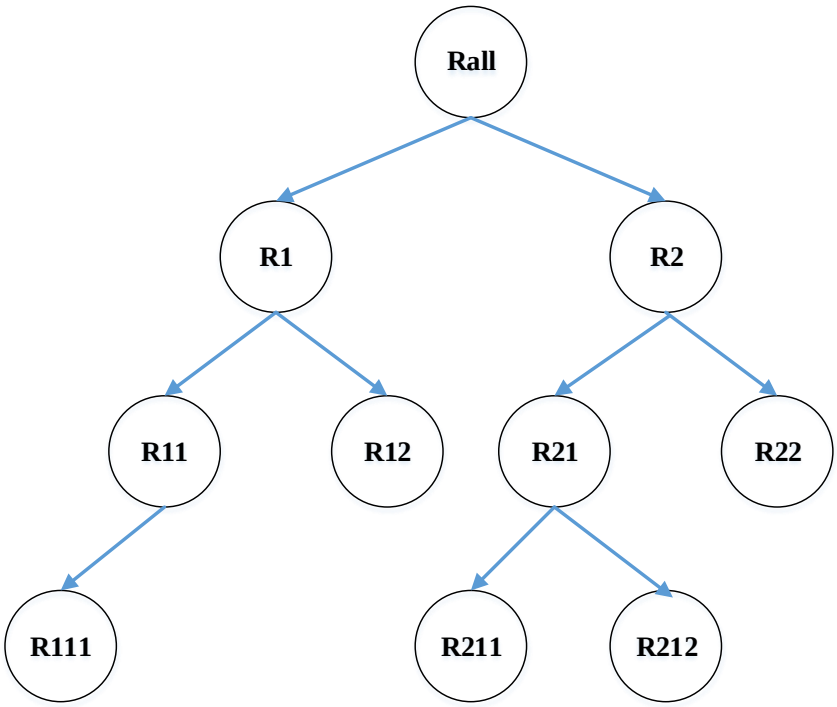
- класификация на източниците на риск в зависимост от жизнения цикъл на ИС;
- класификация на източниците на риск в зависимост от функционалните компоненти на ИС;
- класификация на източниците на риск в зависимост от архитектурата на ИС.

Избраната класификация дефинира основните направления, в които е удачно да се търсят потенциални източници на риск.

Логически модел

От съществено значение за концептуалния модел на предлаганата система е видът и връзките между елементите в общата структура. Изборът на структура определя в последствие логиката за обработката и анализа й. Дефинирани са изискванията, на които тя трябва да отговаря за целите на изследването:

- *структурната схема има йерархичен характер*;
- *структурата отразява моментна снимка на риска*;
- *сложна логическа връзка между отделните елементи;*
- *връзка с методите за количествена оценка на факторите на риск.*



Фиг. 5. Модел на релацията между източниците на риск

Подходящ модел за реализиране на структурна схема на връзките при елементите на риска е дървовидната структура и по-точно двоичното дърво. На първо място тя позволява по-опростено взаимодействие на елементите два по два, които могат да се свържат с по-прости логически връзки. На второ място дървото е добре изявената йерархична структура, която ясно визуализира данните в нея, лесно и подредено се изгражда като структура (фиг.5).

Общото наличие на риск изчисляваме по формулата:

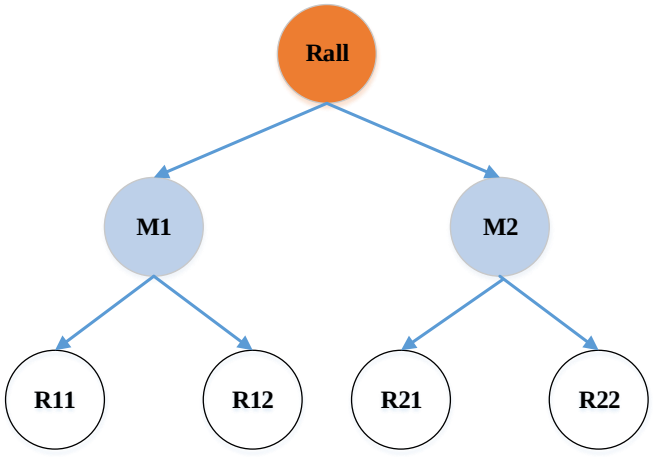
$$R_{all}=\sum Ri,$$

където R_{all} е резултатът от сумирането на всички възли в дървото.

Възлите в дървото са дефинирани като два основни типа:

- **Информационни възли.** Съдържат конкретна стойност за конкретен източник на риск. Като информационен носител те съдържат информация за вида на източника на риск и неговото количествено изражение. Най-често тези възли са крайни елементи наречени листа.
- **Възли – мултиплексор.** Общата дефиниция за мултиплексор е ”комбинационна логическа схема с два вида входове и един изход, който осигурява свързване на няколко източника на сигнал към един приемник[15]”. По своята същност това са свързващи възли, йерархически са поне едно ниво над листата и тяхната роля е да позволят да се изгради по-сложна логика между подчинените възли.

Връзката между двата типа възли в дървовидния модел представяме чрез фиг. 6.



Фиг. 6. Връзка между информационни възли и мултиплексори

15 http://rechnik.info/%D0%BC%D1%83%D0%BB%D1%82%D0%B8%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BE%D1%80 (4.6.2015).

Изграждането на дървото зависи от функционалната обвързаност на източниците на риск. Предложени са следните варианти:

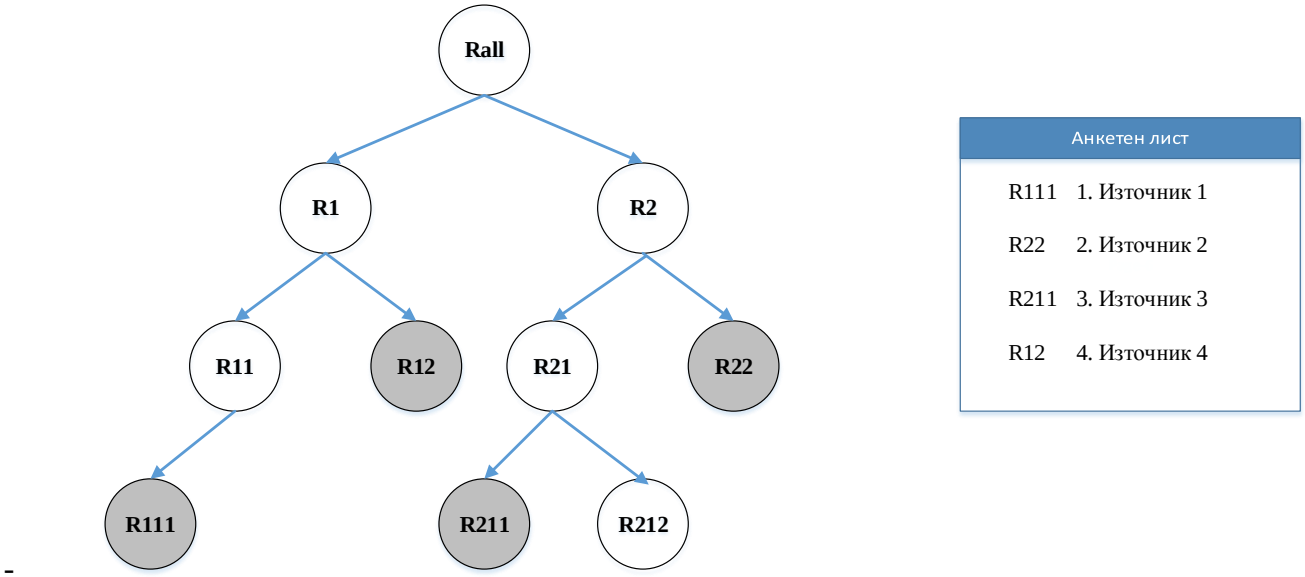
- в зависимост от динамиката на източниците на риск;
- трислойно разпределение;
- според фазите на жизнения цикъл на ИС;
- функционално разпределение.

Основната цел на модела е да определи потенциалният риск при условията на конкретен клиент за устойчивостта на ИС в процеса на внедряване и експлоатация от жизнения цикъл на системата. На фиг. 7 е демонстрирана връзката между структурата на риска за ИС и входящата информация за средата на клиента.

От общата структура на риска се избират тези елементи, касаещи информационната среда на клиента в отделен модул, преобразуван като „Анкетен лист“. Данни в „Анкетния лист” се попълват в процеса на проучване на рисковата среда при внедряване на конкретна ИС за конкретен клиент. Крайната цел е получаването на количествени стойности за изброените в „Анкетния лист“ източници на риск за конструирането на специфичен модел на риска за конкретния клиент.

Данните в „Анкетния лист“ са особено важни за изчисляване на общия риск на системата, тъй като влияят върху променливите стойности в общата йерархия. Начина на конструиране на тези данни зависи от наличието на риск експерт в развойната фирма. Предлага се избор от три основни метода:

- *Попълване на конкретни стойности.*
- *Чрез диапазони на възможните стойности.*
- *Смесен подход.*



-

Фиг. 7. Връзка между източниците на риск от данните за определен клиент и общия риск на ИС

Изграждането на система за управление на ИТ риска е сравнително сложен проблем, който зависи до голяма степен от информационните процеси в бизнес средата. Известно е, че всяка фирма се нуждае от интегриране на процеса по управление на риска в общата стратегия за бизнес развитие. От концептуална гледна точка е необходимо да се дефинира общ алгоритъм за управление на риска. Такъв тип алгоритми са необходими като основа за адаптиране и развитие на управлението на риска в конкретните условия, както на ИТ фирмите, така и на фирми с друг предмет на дейност. Анализът на основните етапи от управлението на риска, взаимствани от теорията на риска, предопределя развитието на процеса чрез добавяне на нови стъпки към разработения модел. Целта е да се създаде по-рационален и практически насочен процес.

Отделните стъпки, свързани с управление на риска в ИТ фирма, следва да бъдат следните:

1. Идентифициране на източниците на риск за ИС.
2. Приоритизиране на риска.

3. Отделяне на значимите източници на риск.
4. Изграждане на структурна схема на източниците на риск.
5. Свързване на източниците на риск чрез мултиплексори.
6. Задаване на стойности за отделните източници на риск.
7. Тестване на изградената структура.
8. Извличане на част от структурата, касаеща конкретен проект.
9. Трансформиране на данните във вид на „Анкетен лист”.
10. Оценка на източниците на риск за конкретната среда.
11. Внедряване.
12. Анализ на предварителната оценка на източниците на риск.
13. Анализ на нововъзникнали източници на риск.
14. Обработка на новопостъпилите данни към общата структура на източниците на риск за фирмата.

Предложеният йерархичен модел на двоично дърво позволява изграждане на сложна структура от различни източници на риск. Съчетаването на възли от типа мултиплексор и информационни възли разрешава свързване на различни по вид и логика ИТ рискове. Възможността за реализация на количествени диапазони в информационните елементи, по подобие на **метода на индексите на опасностите**, улеснява процеса по оценка на отделните източници на риск.

Глава трета. Софтуерна система за управление и оценка на ИТ риск

Идеологията на системата за управление и оценка на риска се определя от вида на входящите потоци от данни. Първичната информация зависи от два основни фактора: метод на постъпване и вид на източниците на риск.

Според метода на постъпване (времева зависимост) се определят два вида потоци от данни:

- *Извличане на данни в реално време*.

- *Извличане на данни в конкретен момент.*

Като основа при изграждането на софтуерната система е разбирането, че за оценка на източниците на риск трудно могат да се осигурят достатъчно източници на данни в реално време. По-точно системата ще се базира на *източници на данни в конкретен момент*.

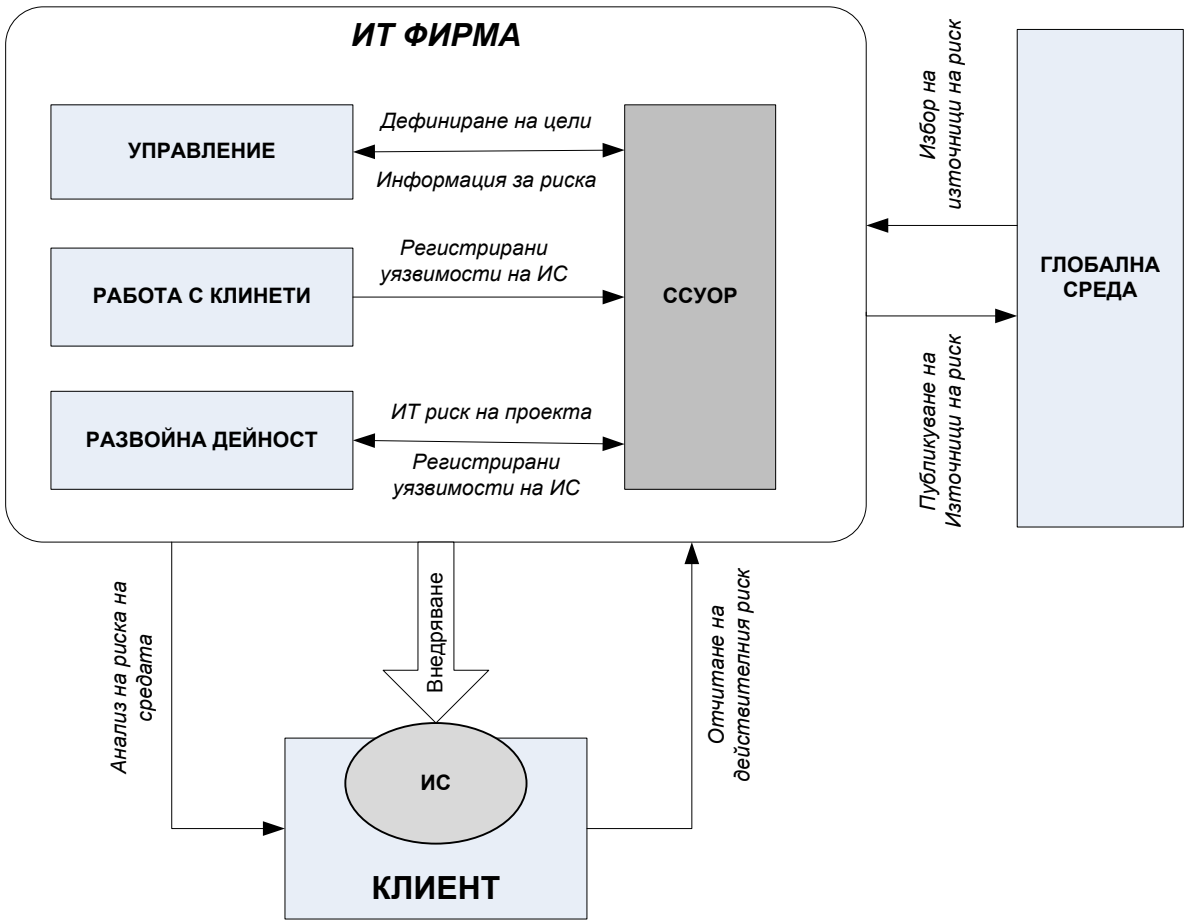
При изграждането на софтуерната система ръководни са следните цели:

- системата да е адаптивна, тоест да позволява приспособяване към нуждите на която и да е фирма в областта на ИТ сектора;

- минимизиране на ограниченията за избор, съчетаване и описване на източниците на риск – тоест да бъде универсална.

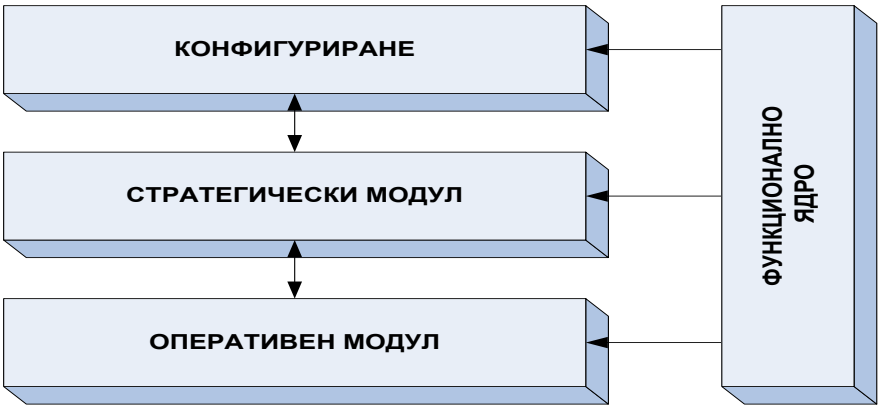
Информационните потоци в софтуерната система за управление и оценка на риска (ССУОР) са показани на фиг. 8. Оформени са два основни субекта: ИТ фирма и клиент при свързващ елемент – ИС.

В субекта "ИТ форма" потоците от информация се определят от трите дейности, свързани с управлението на риска: управление, работа с клиенти и развойна дейност.



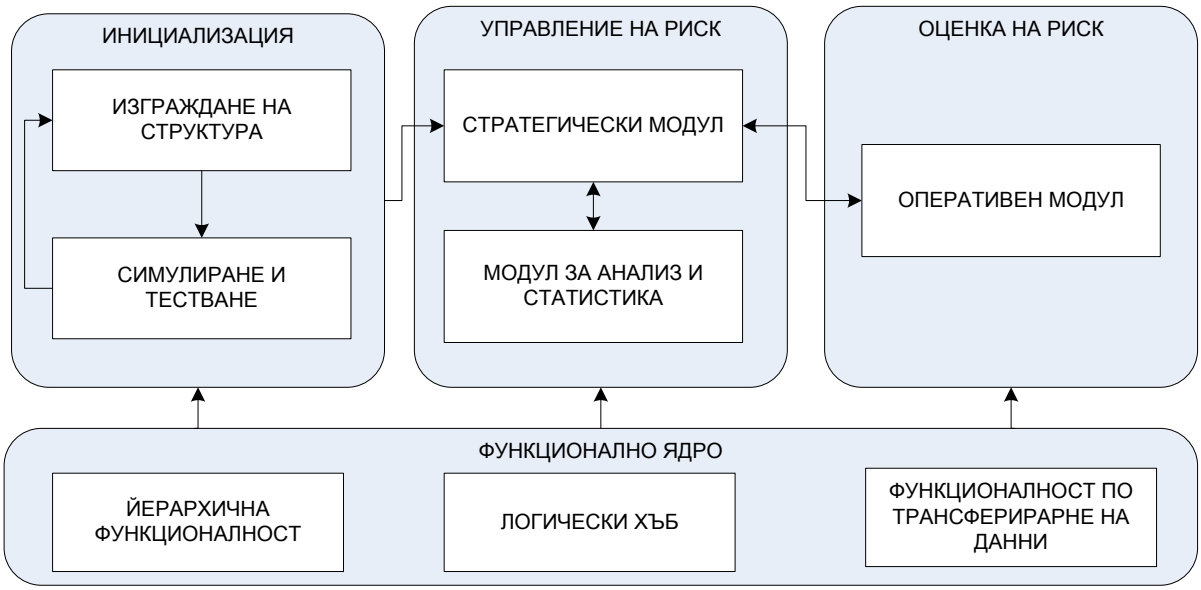
Фиг. 8. Информационни потоци в ССУОР

Технологичната йерархия на отделните модули е представена на фиг. 9 и определя зависимостта на използване на отделните модули в ССУОР от реализация на алгоритъма на концептуалния модел. Всеки следващ модул става функционален след завършване на дейността по предишния.



Фиг. 9. Йерархия на модулите в системата

Концептуалният модел на системата е представен на фиг. 10 и проследява логическите връзки между отделните компоненти.



Фиг. 10. Концептуален модел на ССУОР

Модул „Инициализация”

Модулът „Инициализация” е основният елемент от структурата на софтуерния модел, тъй като дефинира общата ефективност на приложението. Основната му задача е изграждане и симулиране на йерархичната структура на източниците на риск и логическата връзка между тях. Модулът се характеризира със следните функционалности:

- Създаване и актуализиране на номенклатурата на източниците на риск.
- Изграждане на двоично дърво на модела за управление на риска, отговарящо на фирмените цели.
- Задаване на основните характеристики на всеки източник на риск.

- Симулиране на резултатните стойности за риска чрез калкулиране на минимални, средни и максимални, както за цялата дървовидна структура, така и за отделни нейни подмножества.

Оперирането с този елемент от структурата е от фундаментално значение за общата функционалност на системата. Всички последващи модули зависят от правилното задаване на основните параметри на елементите от дървото. Пренастройване на характеристиките на отделните елементи е необходимо при добавяне на нови или премахване на стари източници на риск.

Модул „Управление на риска”

Модулът „Управление на риска” предоставя следващите етапи от технологията за работа със системата, след настройка на общата структура на източниците на риск от модул „Инициализиране”. Предлага се модулът да се раздели на два основни компонента: „Стратегически” и „Анализ и статистика”. Съответно задачите, поставени пред тях, са следните:

Компонент „Стратегически”:

- Дефиниране на проектите, разработвани и реализирани от фирмата.
- Определяне на ресурсната обезпеченост на всеки проект.
- Обобщаване на данните за отделните реализации по конкретен проект.
- Отчитане на ресурсите, прогнозирани при реализация и отчитане на действителните разходи.

Компонент „Анализ и статистика”. Освен представяне на обобщените резултати от данните за различните проекти в числов вид се предвижда визуализация на информацията по графичен път:

- Следене на източниците на риск, превишаващи средните стойности за реализацията на конкретния проект.

- Следене изменението на конкретен източник на риск, отчетен в различни реализации на един продукт.
- Диференциране на източниците на риск, присъщ за продукта, и тези, зависими от средата.

Модул „Оценка на риска”

Модул „Оценка на риска” обслужва подготовката и отчитането на всяка реализация към клиент. Дефинирани са следните функционалности за този модул:

- Копиране на структурата на конкретен проект за предстояща оценка на риска.
- Регистриране на клиент с прогнозна ресурсна обезпеченост.
- Експортиране на анкетен лист за предварителна оценка на източниците на риск в системата „Продукт - среда - клиент”.
- Отразяване на количествените показатели на риска в софтуерната система.
- След внедряване се отчитат действителните нива на рисковите източници и се определят разликите в прогнозните и действителните стойности.

Функционалното ядро (фиг. 10) не притежава самостоятелен интерфейс, а осигурява основните функционални възможности на системата. Всеки от трите модула на ядрото предлагат набор от функции, използвани при изграждане и осигуряване на обща функционалност на интерфейсната част.

Задачата на логическия хъб е да реализира изчисленията в логическите възли. Всяка от функциите, съдържащи се в хъба, осъществява операция между две входни данни ‘a’ и ‘b’ и като резултат връща стойност, изчислена в зависимост от вида операция между тях:

$$R = a \ ? \ b.$$

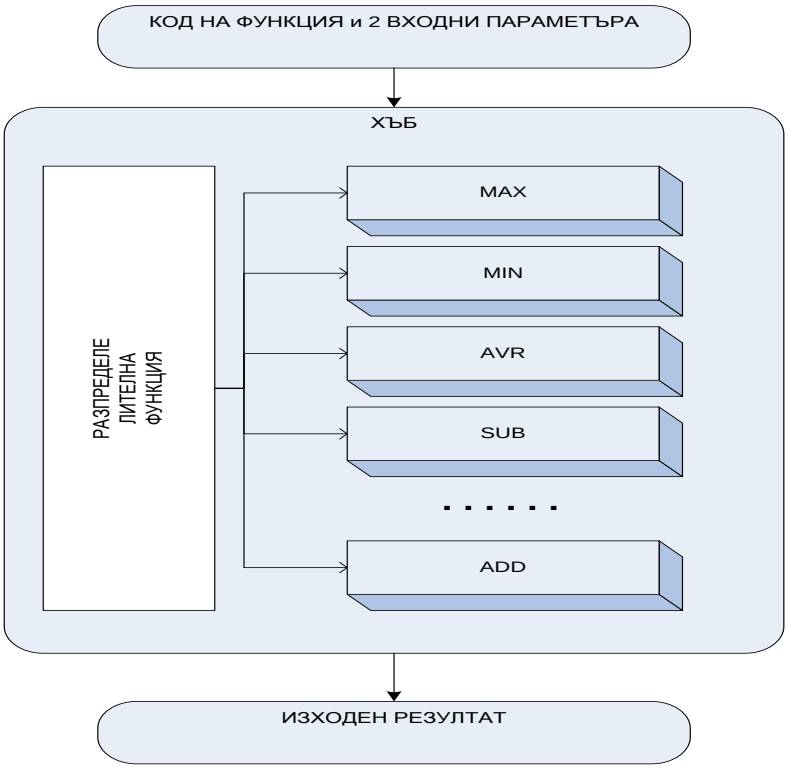
В обобщение хъбът прави пренос на функционалност от базата данни към вътрешния код на приложението за коректно изчисляване на връзките между източниците на риск.

Структурата на хъба е демонстрирана на фиг. 11, а функционалността му се осигурява в следните стъпки:

1. Подготвят се данните за двата входни параметъра. Както е показано на фиг. 11, това са данни или от конкретен източник на риск, или в резултат от изчисление на определен логически възел.
2. От базата данни се извлича кодът на необходимата операция и се подава към логическия хъб.
3. Хъбът превключва логиката към желаното изчисление.
4. Като изход се подава резултатът от операцията.

За реализиране на функциите от логическия хъб е необходимо да се въведат следните ограничения:

- двата входни параметъра да са от един и същи тип;
- всички логики да работят с еднакъв тип данни;
- типът на резултата от изчисленията да е подходящ за последваща обработка.



Фиг. 11. Структура на логическия хъб

Логическия хъб е подсистема на йерархичната функционалност за цялостна обработка на дървовидната структура.

В параграф 3.2 се предлага прототип на ССУОР, базиран на предложения модел. Използваните развойни средства са база данни Firebird с реализиран интерфейс чрез средата Delphi. Представен е моделът на използваната база от данни. В следващия параграф е описан изграденият интерфейс с кратко представяне на функционалните му възможности.

Ефективността на ССУОР се разглежда в следните три функционалности:

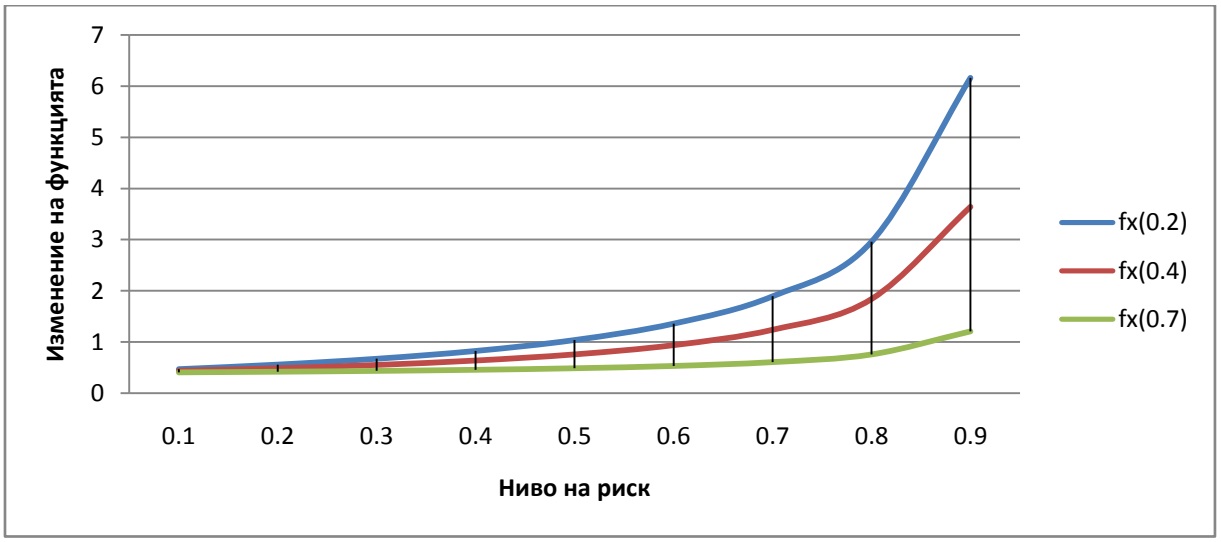
- ресурсна обезпеченост на риска;
- обусловеност на развойния и реализационния риск;
- импорт/експорт на структури.

Една от задачите, които задаваме пред ССУОР, е да се изгради релация между риска и ресурсната му обезпеченост. Като основа се приема фактът, че в повечето случаи, при разпределение на продуктовия риск, по-голямата тежест се поема от фирмата производител.

Основният смисъл на ресурсната обезпеченост е в това, че с растежа на нивата на риска се увеличава и обемът на необходимите ресурси за потискане на отделни източници на риск и респективно на цялостния риск. В процеса на определяне на ресурсната обезпеченост се предлага функционална зависимост, изчислена от формулата:

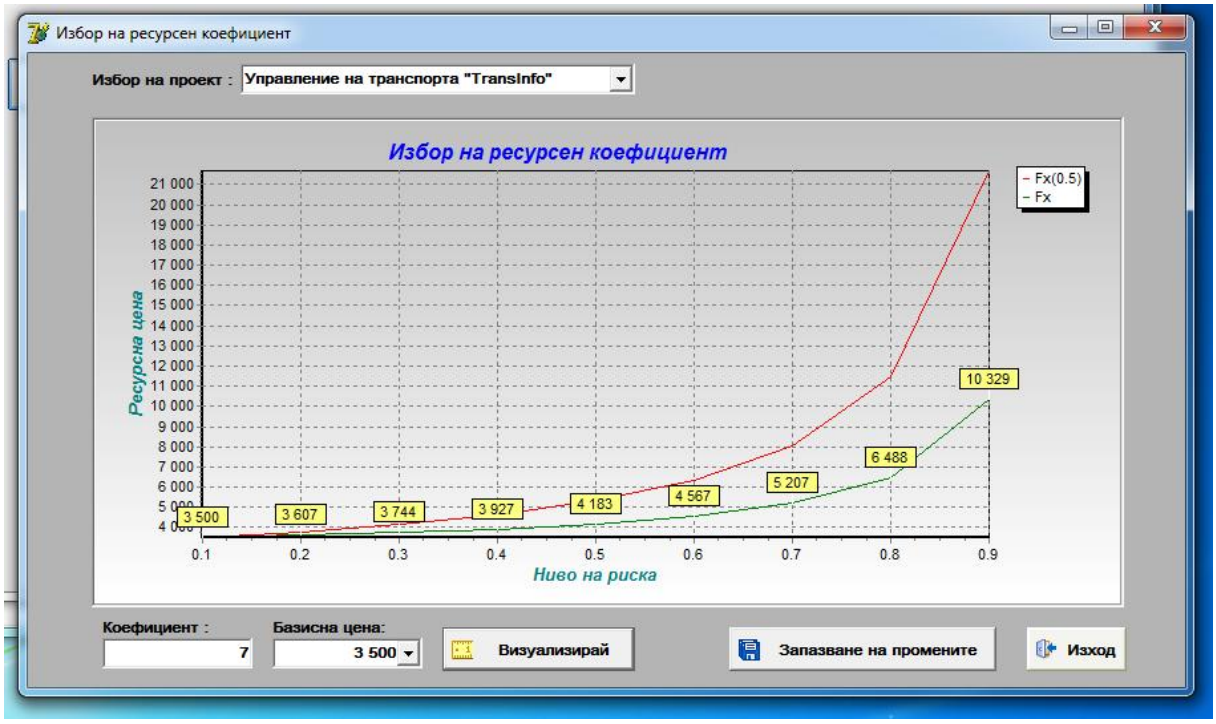
$$f(x) = a + \frac{(1-b)^2 x}{1-x} \quad (0 \le a \le 1, 0 \le b < 1).$$

Основна роля при определяне на зависимостта се отрежда на коефициента ***b***, от който зависи скоростта на растеж на зависимостта. Препоръчителните стойности, в които се изменя коефициентът, са от 0 до 1. На фиг. 12 са визуализирани три примерни криви при три различни коефициента (при стойности 0.2, 0.4 и 0.7). Може да се отбележи, че с намаляване на стойностите на коефициента, при нива на риск в критичната зона 0,7 – 0.9, функцията прогресивно расте.



Фиг. 12. Влияние на коефициент *b* за изменение на функцията

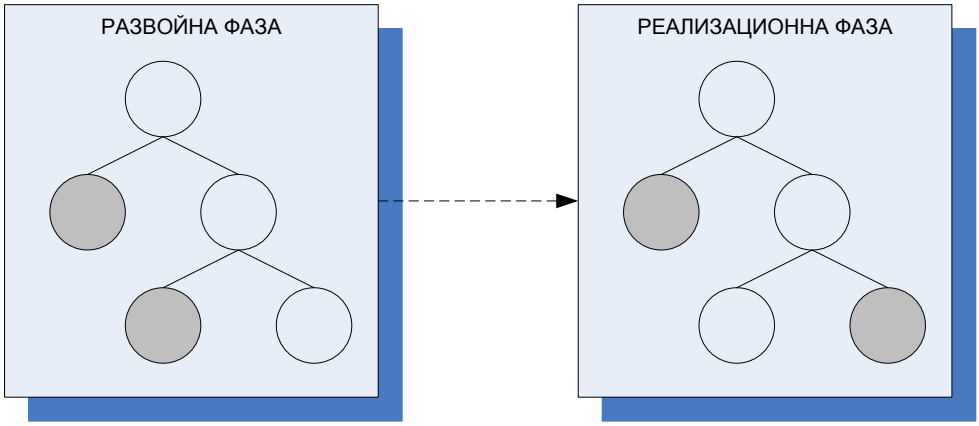
В системата за управление на риска гореизложената зависимост е реализирана чрез интерфейса, показан на фиг. 13. Основните моменти в интерфейса са изборът на проект, за който е предназначена конкретната зависимост, стойностите на коефициента ***b***, зададен в цели стойности от 1 до 9 (отговарящи съответно на 0.1 – 0.9), и базисна цена на ИС за изчисляване на относителната цена при определеното ниво на риск.



Фиг. 13. Интерфейс за избор на ресурсната обезпеченост в зависимост от нивото на риска

Изборът на стойност за коефициента ***b*** се основава на стремежа на фирмата да компенсира разходите по мерки за намаляване на риска и гарантиране на целевия обем приходи.

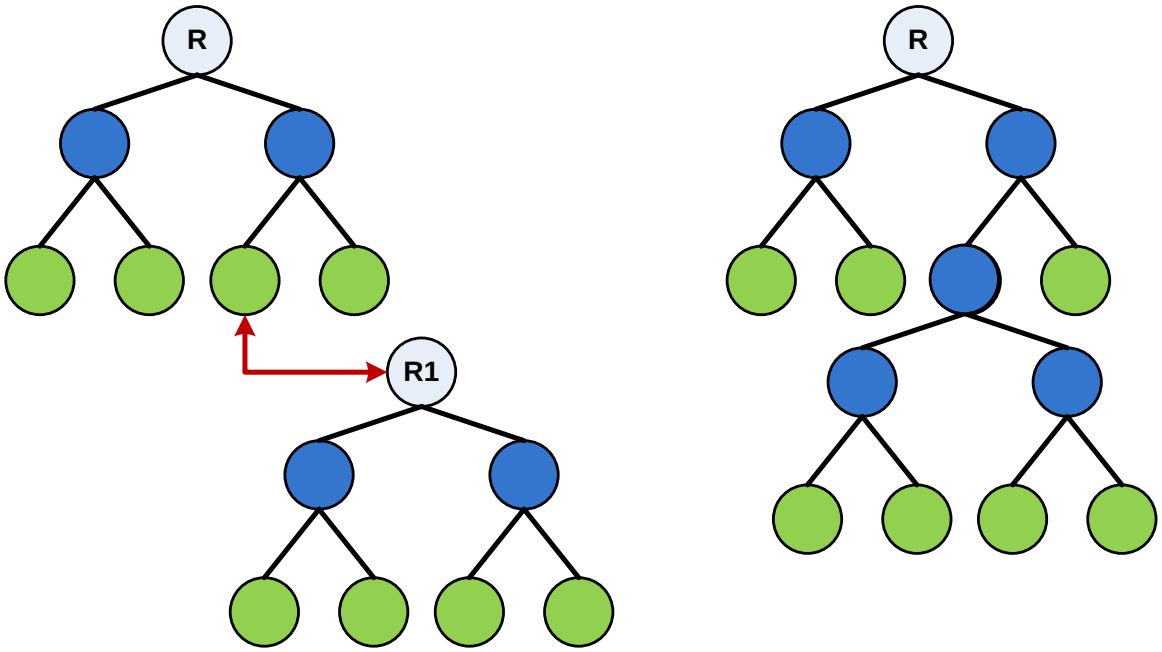
Ефективността на ССУОР се повишава значително, ако се осъществи релация на инженерните и управленските източници на риск. Добра практика е реализирането на миграция на източниците на риск (фиг. 14).



Фиг. 14. Миграция на източниците на риск

Идеята е двете групи източници на риск да не са независими една от друга. Целта е да се изследват двете множества от рискови фактори и да се търси общо подмножество. Този процес ще пренесе опит и знания от едно направление на фирмената дейност към друго, повишавайки достоверността на използваните данни за риска.

Дървовидната структура на модела позволява лесно импортиране на частична или на цяла външна структура към текущата за реализиране на по-сложен модел на средата. На фиг. 15 са демонстрирани етапите по свързването на двете структури. На първия етап коренът на втората структура (общ риск) се реорганизира с желан мултиплексор, след което на втора стъпка се заменя избран източник на риск от първото дърво с цялата втора структура.



Фиг. 15. Експортиране/импортиране на структура

Друга възможност е част от дървовидната структура да се експортира към външен текстови файл. От една страна това позволява изграждане на различни дървовидни структури, съдържащи общи подйерархии. От друга страна е възможност за съхранение или архивиране на вече изградени дървета с цел бъдеща актуализация.

Предложеният прототип на софтуерна система за управление и оценка на риска (ССУОР) цели да реализира универсален подход за наблюдение, оценка и анализ на източниците на риск, който позволява адаптирането на системата към конкретните нужди на ИТ фирмата. Нейната целесъобразност се конкретизира в следните основни моменти:

- ИТ фирмата самостоятелно избира значимите източници на риск, като ги отчита в ССУОР. Те са следствие от вътрешнофирмения експертен анализ на отделени фактори на средата, отчитане на резултатите от дейността на ССУОР или при обмен на информация с други фирми, или организации в областта.

- Широк диапазон от възможности за логически синтез на отделните рискови фактори в една цялостна система според стратегията по управление на риска, изградена в ИТ фирмата. Моделът на йерархична структура на общия риск е отворена система, която позволява конфигуриране на източниците на риск и мултиплексори с висока вариативност.
- Позволява количественото изражение на риска в отделните източници, включително модифициране на отделни характеристики според нуждите на фирмата. ССУОР допуска да се дефинира диапазон за изменение на стойностите на всеки източник на риск, промяна на скалата за избрания диапазон или вида на текстовото представяне на количествените нива.
- Автоматизира процесите по анализ на източниците на риск и анализ на оценката на потребителя.

Реализира се функционалност по ресурсна обезпеченост на риска. Предложен е интерфейс за динамична финансова обезпеченост при реализиране на приложения в средата на клиента, в зависимост от нивата на общия риск.

Основните резултати от направеното изследване могат да се обобщят по следния начин:

1. Основните методологии за управление на риска сами по себе си не са достатъчно ефективни при използване в ИТ областта. Съчетаването на отделни елементи на различни модели и интегрирането им в нов модел ще позволи адекватен отговор на проблемите, свързани с източниците на риск в ИТ фирмите.
2. Процесът по управление на ИТ риска в световен мащаб и в частност в България е свързан с използване на традиционни инструменти за обработка на данните като офис пакети. Не се прилагат специализирани

информационни системи или поради липса на такива, или поради разминаване на възможностите на ИС и нуждите на фирмите.

3. От направеното изследване проличава, че съществуват множество теоретични разработки в областта на управлението на риска, но налице е недостиг на приложни ИС, специализирани в тази област.

4. В областта на информационните системи за управление на риска стигаме до извода, че има необходимост от концепция за софтуерно приложение, което да предлага универсалност и съответно да повиши ефективността на фирмите в ИТ сектора.

5. Решенията в областта на управление на ИТ риска, когато съществуват такива, са капсулирани в рамките на ИТ фирмата. Реализирането на по-глобална концепция за обмен на информация и решения при управление на риска оптимизира процесите по анализ и оценка на източниците на риск от една страна, а от друга повишава квалификацията на експертите по вземане на решения.

IV. СПРАВКА ЗА ПРИНОСИТЕ В ДИСЕРТАЦИОННИЯ ТРУД

В дисертационния труд се съдържат следните основни приносни моменти с научен и научно-приложен характер:

1. Направено е проучване и критичен анализ на съществуващите модели за управление и оценка на риска при отчитане на спецификите на ИТ сектора.

2. Предложена е класификация на източниците на риск за информационните системи в три основни направления. Предложен е модел на йерархична структура на източниците на риск с отчитане на спецификите на ИТ областта.

3. Представен е трислоен модел на средата на приложение на ИС с групиране на източниците на риск и формулиране на количественото изражение на общия риск за системата.

4. Предложен е модел на система за управление на риска в ИТ сферата с идея за глобализиране на информацията. Изграден е прототип на ССУОР, реализиращ основните функционалности на предложения модел.

5. Реализирана е приложна интерфейсна част за ресурсна обезпеченост на риска, в която чрез математически модел се цели минимизиране на загубите от възникване на риск.

V. СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД

Научни статии:

1. Стоев, Ст. Нов йерархичен модел за обработка на източниците на риск. // списание Известия - Икономически университет - Варна, 2016, том 60/4, с. 491-504.

2. Стоев, Ст. Разпределение на продуктовия риск при внедряване на ИС. // Известия на съюза на учените - Варна, Серия "Икономически науки", №2, 2016, с.109-116.

Доклади:

1. Стоев, Ст. Прототип на информационна система за обработка на източниците на риск в процеса на фирменото управление. // Сборник с доклади от конференция на младите научни работници. Варна: Наука и икономика, 2016, с.168-177.

2. Стоев, Ст. Класификация на източници на риск за ИС. // Юбилейна научна конференция "Предизвикателства пред информационните технологии в контекста на "Хоризонт 2020". Свищов, 2016, с. 298-305.