РЕЦЕНЗИЯ

от ст.н.с. д-р Бончо Христов Балабанов
експерт към компания "КОМБАЛСАТ" оод,
„Комуникационна и компютърна техника"
за придобиване на научната степен „доктор" по професионално направление 5.3.
„Комуникационна и компютърна техника",
с кандидат **Кристиан Димитров Томов**
Тема на дисертационния труд**:**

Анализ и оптимизиране на вътрешни контролни системи в телекомуникационни структури

1. Значимост на изследвания проблем в научно и научно-приложно отношение.

Темата, на която е посветена дисертацията, е интересна и актуална. Дисертационният труд е посветен на оптимизиране на организацията на телекомуникационните предприятия с цел намаляване на рисковете и подбряване на надежността при предаване и обработка на информацията, което е област с важно значение за модерните телекомуникации и за информационните технологии. Целите и задачите, които си поставя докторантът са значими и комплексни, което прави работата му актуална.

Предложеният модел на Интегрирана вътрешна управленческа система (ИВУС) използва основните моменти във всеки стандарт и ги сравнява с други клаузи с подобната тематика. Моделът на **ИВУС**, разработен в настоящата работа за организации предимно в телекомуникационния сектор, е структуриран и изграден с крайна цел минимизиране или напълно отстраняване на част или всички проблеми, които често присъстват при организациите, опитващи се да се сертифицират по различни стандарти чрез отделни системи или използвайки неефективни методи за интеграция между различните стандарти.

Изграждането на ИВУС създава една цялостна прозрачна система, включваща ясни логически връзки, гарантираща управляема ефикасност и оптимална функционалност на процесите при максимална защита от рискове.

Моделът на ИВУС използва основните моменти във всеки стандарт, т.нар. клаузи за съответствие и ги съпоставя и сравнява с други клаузи с подобната или съща тематика. Това е основна приложна стойност на разработения модел на **ИВУС.**

2. Кратка аналитична характеристика на дисертационните резултати, върху които се базират научните приноси и образователната стойност на труда.

Дисертацията включва 119 страници в Увод и 5 глави с фигури и таблици. Приложени са 10 препоръки и 3 сертификата за внедряване на резултатите в България и в чужбина. В това отношение дисертационният труд в количествено отношение отговаря на изискванията за докторска работа.

В **Увода** са разгледани телекомуникационните структури и техните компоненти. Анализирано е предоставянето на информационни и комуникационни услуги чрез ресурсите на телекомуникационните компании. Посочена е необходимостта от интегрирани управленски системи (ИСУ). Показана е ролята на контролните

механизми в ИСУ. Засегнати са основните проблеми, които се разработват в дисертацията с цел подобряване на надежността на услугите.

В **Първа Глава** е направен обзор на специализираната литература и е анализирано съвременното състояние на изследваните проблеми. Разгледани са 103 литературни източника. Анализирани са стандартите за управление и сертифициране на телекомуникационните компании и внедряването им в областта на информационната сигурност. Посочено е, че прилагането на Директивите на Съвета на ЕС за управление на сигурността на риска при обмен на информация са задължителни. Разгледани са примери за правни изисквания при системите за управление. Посочен е регулаторният стандарт Базел III, който определя изискванията за финансовите институции и техния надзор. Регулаторните стандарти включват спецификация на системите за управление на риска в компаниите.

Системата за управление на информационната сигурност е подход за управление на чувствителната информация по начин, който съответства на нуждите на организацията и гарантира запазването на сигурността и цялостта на информацията, с която всяка организация оперира. Прилагането на стандартите гарантира, че информационният риск се управлява ефективно от гледна точка на съхраняване, както на собствената информация, така и на информацията, предоставена от различни други източници.

Интегрираните системи за управление (ИСУ) са утвърден подход за повишаване на информационната сигурност.

Кибератаките включват използването на вектори на атака, чрез които нарушителят може да придобие достъп до данни за онлайн самоличност, компютър или мрежов сървър, за да постигне злонамерен резултат. Често използвани вектори на атака са USB устройства, приложения в електронната поща, уеб страници, изскачащи прозорци, съобщения в реално време и измами от рода на атаки с фалшива самоличност.

В тази глава докторантът е определил целите и задачите на дисертацията.

Във **Втора Глава** се въвежда и описва Интегрирана вътрешна управленческа система **(ИВУС)** и Моделът на **ИВУС.** Дадени са предварителни сведения и са разгледани предпоставките за разработка на Модел и Алгоритъм като схема за реализиране на **ИВУС.**

ИВУС се използва за управление на телекомуникационната структура за подобряване на качеството, на безопасността по време на работа, на експлоатационните процеси и на сигурноста. Моделът на **ИВУС** включва организационни (административни) и технически, превантивни, детективни и коригиращи изисквания (механизми за контрол) спрямо телекомуникационната структура, както и препоръки за изпълнението им. Анализирана е ефективността на предприятието и ефективната му оперативна дейност в контекста на **ИВУС**. Определена е надеждността като способност на обекта да запазва във времето стойностите на всички параметри в установените граници.

В **Трета Глава** е разгледано управлението на риска при **ИВУС** и значението на управлението на риска в телекомуникационните компании.

Рискът R е от категорията на статистическите оценки и по същество представлява вектор с многокомпонентни величини.

Развиването на успешна дейност в каквато и да е област е в пряка зависимост от идентифицирането, поемането и управлението на различните видове риск - оперативен, организационен, както и риска от използване на информационните системи.

Рисковете свързани с информационната сигурност имат ефект върху множество бизнес процеси:

–спечелване и запазване на потребителското доверие;

–защита на личната информация на клиентите;

–създаване, запазване, и увеличаване на репутацията;

–увеличаване на печалбата и на цената на акциите/дяловете;

–увеличаване на размера на пазарният дял, който компанията владее;

–намаляване на времето необходимо за изкарване на нови продукти на пазара;

–разрастване на бизнеса;

–формулиране и изпълнение на мисията;

–привличане и запазване на компетентен персонал; и т.н.

Оценката на риска трябва да се задейства в рамките на работния процес, когато възникват особени обстоятелства извън текущия бизнес цикъл.

Анализиран е моделът "Оценка на риска" и е описано предпазването от кибер атаки и защитата на информационните системи.

Създаден е Модел и Алгоритъм за оценка на корпоративния риск като част от ИВУС

В **Четвърта Глава** е разгледана оперативната ефективност на ИВУС и е предложен Модел и Алгоритъм за оценка на оперативната ефективност на ИВУС.

Предложено е създаването на контролни групи, които съдържат определени контролни механизми, всеки от които е в съответствие с типа на контролата (превантивна, детективна и коригираща). Контролни групи се създават за всяка заплаха (списък рискове), описани съгласно конкретния случай на приложение.

Описана е методика за определяне на оперативната ефективност в аналитичен вид за различните случаи.

В **Пета Глава** се предлагат Методики и Алгоритми за използване на модела на **ИВУС** в съответствие с практиката за управление. Въвеждането на **ИВУС** позволява на организациите да решат проблемите, които често възникват при паралелно или последователно независимо внедряване на няколко СУ според международните стандарти. Моделът на **ИВУС**, разработен в настоящата работа за организации предимно в телекомуникационния сектор, е структуриран и изграден с крайна цел минимизиране или напълно отстраняване на част или всички от изброените по-горе проблеми, които често присъстват при организациите, опитващи се да се сертифицират по различни стандарти чрез отделни системи или използвайки неефективни методи за интеграция между различните стандарти. Моделът на ИВУС използва основните моменти във всеки стандарт, т.нар. клаузи за съответствие и ги съпоставя и сравнява с други клаузи с подобната или съща тематика.

Това е основна приложна стойност на разработения модел на **ИВУС.**

3. Цели и задачи на дисертацията.

В съответствие с резултатите от литературния обзор и направения критичен анализ на приложението и ефективността на управленческите системи на

телекомуникационните структури, целите на дисертационния труд са формулирани така:

- Изследване и анализ на необходимостта от ИВУС (Интегрирана Вътрешна Управленска Система).
- Разработка на модел на ИВУС на база управление на качеството, околна среда, сигурността по време на работа и информационна сигурност и разработка на съответен алгоритъм за управление на риска и изследване на параметрите на оперативната ефективност на ИВУС.
- Анализ и разработка на модел и алгоритъм за внедряване на ИВУС.

За постигане на тези цели са изпълнени следните задачи:

❖ Изследване на необходимостта от ИВУС.

❖ Разработване на модел на ИВУС и алгоритъм като схема за създаване на ИВУС.

❖ Разработване на модел и алгоритъм за оценка на риска и управлението му, включващ идентифициране на критични активи, групиране на активи, прилагане на стандартен списък от контроли чрез анализ на необходимостта от защита на активите, както и създаване на разширена методика за оценка на риска, въз основа на модела на ИВУС.

❖ Разработване на модел и алгоритъм за измерването на оперативната ефективност на ИВУС, включващ критерии за оценка на оперативната ефективност на ИВУС на база на примерни контролни групи и контролни механизми, взети под внимание в процеса на третиране на рисковете след извършване на разширената им оценка.

❖ Разработване на метод и алгоритъм за внедряване на ИВУС, въз основа на подход, включващ система за управление на качеството, система за управление на информационната сигурност, система за управление на здравословните и безопасни условия на труд и система за управление на околната среда.

4. В дисертацията са разработени модели и алгоритми и е избрана методология и методика на изследване, които съответстват изцяло на поставената цел и задачи. ИВУС е отговорна за управлението и надзора на комплексни организации. Тя включва поредица от процеси и интегрира всички аспекти на бизнеса, като управление на тези процеси, осигуряване на качеството, опазване на околната среда и безопасност на труда, управление на извънредни ситуации, сигурността, както и много други, събрани в единна управленска структура. Изследванията са проведени чрез създаване на модел на ИВУС, с отчитане на условията на функциониране, като е предвидена възможността за използване на различни варианти.

Моделът на ИВУС е схема по която се разработва ИВУС в корпоративни структури и включва различни модули. Това позволява непрекъснато разширение на ИВУС. Количеството на системите в ИВУС зависи от нуждите на съответната организация. Тя се състои от общи и от специфични модули, но може в допълнение да се включат и други изпитани и проверени системи за управление, съдържащи и други области. Процесът на създаване и изследване на приложимостта на **ИВУС** представлява анализ и оптимизиране на вътрешните контролни системи в телекомуникационни структури.

5. Авторът е показал основно познаване на състоянието на проблема в резултат от професионалната си практика. Разгледани са по-важните литературни източници в областта на теорията на системите, теорията на управлението и информационната сигурност.

6. Разработени са и са анализирани обоснавани теоретични модели и алгоритми на Интегрирана вътрешна управленческа система (**ИВУС**), за оценка на корпоративния риск като част от ИВУС, за оценка на оперативната ефективност на ИВУС и методика и алгоритъм за използване на модела на **ИВУС.** Алгоритъмът представя логическия процес по който се реализира и функционира моделът. Това показва наличие на обоснован и разработен теоретичен модел на изследването.

7. Избраната методология и методика на изследване съответства на поставените цели и задачи на дисертационния труд. Всички поставени задачи са решени и целите на дисертацията са постигнати.

8. Собственият принос при събирането и анализирането на емпиричните данни се доказва от постигнатите резултати и от приложените документи за внедряване, препоръките и сертификатите.

9. Докторантът е отлично запознат с областта, към която се отнася темата на дисертацията. Изборът на целите и задачите на изследването са свързани с практически значими проблеми, които са формулирани компетентно и ясно. Това е позволило да се извърши задълбочен и детайлен анализ на проблемите и да се постигнат целите на дисертацията.

Дисертационният труд е разработен самостоятелно, което проличава от приложените документи за внедряване, препоръките и сертификатите. Те доказват и компетенциите на докторанта в областта на дисертационната тема.

10. Между темата на дисертацията и методиката за изследване има пълно съответствие. Това се доказва с постигнатите резултати и с тяхната приложимост.

11. Научно-приложни приноси

Дисертационният труд съдържа научно-приложни приноси. Могат да се признаят следните по-важни научно-приложни приноси:

11.1. Направен е критичен анализ на въпросите свързани с управленски системи въз основа на разгледаната литература.

11.2. Разработен е модел на ИВУС, въз основа на приети ограничителни условия и са предложени структура, дефиниции и параметри на модела на ИВУС.

11.3. Предложен е модел и алгоритъм за управление на риска като част от ИВУС.

11.4. Синтезиран е модел и алгоритъм за измерване на оперативната ефективност на ИВУС и са дадени контролните изисквания за прилагане на алгоритъма, както и примери за прилагането му.

11.5. Определени са типовете контроли и измерителите за ефективност на всеки от контролите, въз основа на примерни инциденти.

11.6. Описани са основните ползи при интеграция на стандартите в единна система при използване на модела на ИВУС.

11.7. Предложен е метод за внедряване на модела на ИВУС, като са представени основните пет етапа, базирани на цикъла на Деминг, при реализация на цялостно решение по разработване и внедряване на ИВУС.

Получените приноси изцяло съответстват на поставените задачи и цели на дисертацията.

12. Оценка на съответствието на автореферата с основните положения и приносите на дисертационния труд.

Авторефератът отразява съдържанието на дисертацията и съответства на основните положения и на приносите на дисертационния труд.

13. Преценка на публикациите по дисертационния труд: брой, характер на изданията, в които са публикувани.

Авторът на докторската работа има 10 публикации свързани с дисертационния труд, от които От тях 4 са изнесени на национални конференции с международно участие (в Телеком 2012 - 1 публикация, в Телеком 2013 - 2 публикации и в АСТЕЛ 2013 - 1 публикация), 1 публикация е изнесена на регионална конференция на ITU, 2 публикации са направени в международно електронно научно списание (http://www.all-about-security.de) и 3 публикации са в Годишник на департамент „Телекомуникации". Представените публикации са на български, английски и немски език. Тези материали отразяват основни моменти на изследванията свързани с представената докторска работа.

14. Цитиране от други автори, отзиви в научния печат и др.

Има едно забелязано цитиране на научна публикация на Кристиан Томов. Има приложени официални отзиви от специалисти и водещи фирми в областта. В процеса на работа над дисертацията има направени допълнително две публикации в областта на телекомуникациите.

15. Забележки към дисертационният труд

15.1. В дисертацията не са посочени конкретни примери за предотвратяване на хакерски атаки.

15.2. При анализа на информационната сигурност не е описана ситуацията в България.

15.3. Разглеждат се задълженията на фирмите, но не е ясно какви са изпълненията им и дали има проблеми при предотвратяване на рисковете.

15.4. Номерацията на литературата е по глави, което прави цитирането неясно.

16. Препоръки за бъдещо развитие на тематиката

Представените резултати в разработката могат да бъдат широко приложими и да позволяват оценка на оперативната ефективност на ИВУС спрямо изискванията към нея и вложените в нея инвестиции. Такива системи са вече внедрени в частния сектор, както и в организации от публичния сектор.

Като една възможност за продължение на тази разработа може да се предложи приложението на алгоритъма и доказване на ефективността в реални условия. В практиката на изследване, анализ и одитиране на ИВУС се използват много практически подходи, базирани на съответните стандарти.

Препоръчвам авторът да подготви учебно пособие за програмите на НБУ в областа на информационната сигурност.

17. Заключение и общи изводи от изследванията

В настоящата разработка е предложен обоснован модел на ИВУС, описана е методика и е предложен алгоритъм за оценка на нейната оперативна ефективност, пряко свързан с оценката на нейното функциониране. Използван е модулен подход и са дадени ограничителни условия.

Представените резултати в разработката могат да бъдат широко приложими и да позволяват оценка на оперативната ефективност на ИВУС спрямо изискванията към нея и вложените в нея инвестиции.

Като съществен фактор от анализа на риска могат да се изтъкнат кибер атаките. Те са динамични и представляват съществена заплаха за информационната и финансовата сигурност на всяка система за управление. По тази причина анализът на тенденциите в усъвършенстването и разпространението на кибер атаките е ключов за сигурността в изследвания модел.

Направеният компетентен и коректен преглед на 103 литературни източника се свежда до разглеждането на най-важните и актуални проблеми в областта на информационната сигурност. Отбелязва се, че за тяхното разрешаване възникват много практически проблеми при организацията управлението на компаниите, свързани с необходимите минимални ограничения относно обмена и обработката на информацията.

Въз основа на тази констатация е формулирана основната цел на дисертационния труд:

Разработка на модел на ИВУС на база управление на качеството, околна среда, сигурността по време на работа и информационна сигурност и разработка на съответен алгоритъм за управление на риска и изследване на параметрите на оперативната ефективност на ИВУС.

Дисертационният труд показва, че кандидатът притежава задълбочени теоретични знания по съответната специалност и способности за самостоятелни научни изследвания.

Конкретната програма на научно-приложните изследвания е изградена от обективно очертаните от докторанта общи проблеми за решаване в областта на темата. Тази програма е изпълнена и е довела до съществени резултати при проектите, по които е работил докторанта.

Направените забележки и препоръки не подлагат на съмнение получените резултати.

Представеният дисертационен труд отговаря на изискванията определени от закона за развитие на академичния състав за получаване на образователна степен „Доктор".

Предлагам на уважаемото научно жури да присъди образователна и научна степен „Доктор" на **Кристиан Томов** по научно направление:

5.3. „Комуникационна и компютърна техника"

12.6.2016г. Рецензент:

/ст.н.с. д-р Б. Балабанов/