РЕЦЕНЗИЯ

на дисертационен труд за придобиване образователна и научна степен „Доктор“

Автор на дисертационния труд: маг. инж. Петко Генчев Генчев

Тема на дисертационния труд: „Подход за мониторинг на риска в системи за информационна сигурност“

Рецензент: доц. д-р инж. Росен Стефанов Радков, Технически университет - Варна

1. **Актуалност на разработвания в дисертационния труд проблем в научно и научно-приложно отношение. Степен и мащаб на актуалността на проблема и конкретните задачи, разработени в дисертацията.**

С повсеместното разпространение на Интернет, използването на IoT и все по-голямата зависимост на бизнес процесите от информационните технологии необходимостта от прилагане ефикасно управление на риска, свързан със сигурността на информацията е все по-належаща. Добра практика е внедряването и поддържането на системи за управление на сигурността на информацията, разработвани в съответствие с международния стандарт ISO/IEC 27001, при което като резултат от оценката на риска за сигурността на информацията се определят необходимите механизми за контрол.

В съвременния свят често в междуфирмените отношения се поставят изисквания за гарантиране на определено ниво на сигурност на обменяната/обработваната информацията. Един от най-добрите начини за доказване на съответствието с тези изисквания, е внедряване и сертифициране на система за управление на сигурността на информацията.

Поради това разработвания в десертацията проблем и решаваните задачи, свързани с предлагания подход за мониторинг на риска в системи за информационна сигурност са изключително актуални за практиката в световен мащаб. Хипотезата на дисертанта е, че с прилагането на такъв подход ще се постигне ефикасно управление на риска за сигурността на информацията, което да даде увереност на организацията, която го прилага, че наистина контролира и управлява риска.

Считам, че разработеният в дисертационния труд проблем, има своята актуалност в научно и научно-приложно отношение, а поставените цели и задачи са изпълнени в необходимия обем.

2. **Познава ли дисертантът състоянието на проблема и оценява ли творчески литературния материал.**

Дисертантът е извършил задълбочено проучване на проблемите, свързани процесите на идентификация, анализ и преценяване на риска, както и с проблемите за събиране на необходимите данни и методите за оценка на риска, като за целта е използвал 113 литературни източника, от които 99 са на латиница. Особено внимание е обърнато на анализа на вероятностните характеристики на измененията на рисковите фактори и определяне на периодичността на проверките на рисковите фактори. На базата на анализа на постигнатото в областта е изяснена нуждата от разработване на нови методи, които да подпомогнат определянето на периодичността на проверките и актуализация на състоянието на рисковите фактори, както и на алгоритми за ефективна организация на тяхното проследяване. Формулирани са някои от съществените проблеми, свързани с разработките в областта. Считам, че дисертантът е проучил добре изследвания проблем и е приложил творчесство за постигане на поставените задачи.

3. **Избраната методика на изследване може ли да даде отговор на поставената цел и задачи на дисертационния труд.**

В резултат от направения обзор и анализ е формулирана целта на настоящата дисертация: да се предложи подход и да се формулира задание за изграждане на информационна система с цел преодоляване на основните проблеми при оценка и мониторинг на риска в системите за информационна сигурност.

Във връзка с целта са формулирани следните задачи:

3.1. Да се направи анализ на вероятностните характеристики на измененията на рисковите фактори. Да се предложи начин за определяне на периодичността на проверките и актуализацията на състоянието на рисковите фактори.

3.2. Да се предложат алгоритми за ефективна организация на следенето на измененията на рисковите фактори и подпомагане на мониторинга на риска за сигурност на информацията.

3.3. Да се предложи форма на йерархичен контрол на реализацията и ефективността на мониторинга на рисковите фактори.

3.4. Да се предложи общ подход за преодоляване на основните затруднения и подпомагане на внедряването и експлоатацията на процеса за управление на риска за сигурност на информацията (УРСИ).

3.5. Използвайки предложения подход, да се дефинират функционални изисквания към изграждане на програмна система за реализация на УРСИ.

За решаването на поставените задачи са използвани математически модели за:

- изследване на промените на вероятността за инцидент;

- определяне на периодичността на проверките на рисковите фактори.

Изброеното по-горе е доказателство за добрата теоретична подготовка на автора и добрите му изследователски умения за избор на методи и средства за изследване.

4. Кратка аналитична характеристика на естеството и оценка на достоверността на материала, върху който се градят приносите на дисертационния труд.

От текста на дисертационния труд и свързаните с него публикации може да се отбележи, че докторантът познава много добре състоянието на проблема. Дисертационният труд е с обем от 146 страници и е оформен в четири глави. В първа глава, озаглавена „Системи за управление на риска и сигурността на информацията“, е направен обзор на изискванията на международните стандарти, разработени от ISO, по отношение на управлението на риска, свързан със сигурността на информацията и са формулирани задачите, които трябва да бъдат решени. Във втората глава, озаглавена „Модел за определяне на периодичността на проверките на рисковите фактори“, се прави анализ на вероятностните характеристики на измененията на рисковите фактори. На базата на направения анализ, са изведени математически изрази, за изчисляване на интервала от време до следваща проверка, за да се отчетат настъпилите промени и се изчисляват нови стойности на риска за сигурността на информацията (СИ). В трета глава, „Формулиране на подход за облекчаване на управлението на риска за СИ“, е описан предлаганият подход. Четвърта глава, озаглавена „Изследване на възможностите на предложения подход чрез изграждане на програмна система за оценка и мониторинг на риска за сигурността на информацията“, е посветена на описание на примерна реализация на информационна система за обслужване на оценката и мониторинга на риска за сигурността на информацията в една организация с внедрена система за управление на сигурността на информацията (СУСИ). В нея са реализирани голяма част от препоръките на предлагания подход. Направен е анализ на възможностите с прилагане на предлагания подход и препоръките, включени в него, да се постигне ефикасно управление на риска и да се оценят неговите предимства.

5. Научни и научно-приложни приноси на дисертационния труд. Значимост на приносите за науката и практиката.

Приемам декларираните от докторанта приноси, като според мен те могат да бъдат преформулирани според степента си на важност така:

Приноси с научно-приложен характер:

1. Предложен е подход за ефикасно управление на риска за сигурността на информацията, чрез въвеждане, обработване на данни рисковите фактори и прилагане на динамична система за тяхното регулярно наблюдение, както и на стойността на риска

2. Изведени са математически изрази за определяне на периодичността на проверките на рисковите фактори и за определяне на текуща стойност на вероятността за инцидент между две проверки на рисковите фактори
3. Предложен е алгоритъм за оценка на периодичността на проверките за риска на информационен актив
4. Предложен е алгоритъм за йерархична организация на контрола на извършваните проверки за риска на информационен актив

Приноси с приложен характер:

5. Разработена е примерна информационна система за управление на риска за сигурността на информацията в една организация с внедрена СУСИ. Формулирани са предложения за генериране на добре структурирани справки за работата на системата и измененията на риска

6. Може ли да се оцени в каква степен дисертационния труд и приносите представляват лично дело на дисертанта?

Представеният ми за рецензия дисертационен труд, информацията, с която разполагам, както и публикациите по темата на дисертацията ми дават увереност да смятам, че основните резултати от дисертационния труд са лично дело на инж. Петко Генчев, разбира се под ръководството на научния му ръководител доц. д-р инж. Милена Карова.

7. Преценка на публикациите по дисертационния труд: брой, характер на изданията, в които са отпечатани.

Основните резултати от дисертационния труд са представени в 4 доклада (2 в съавторство с научния ръководител) от международни конференции и две статии (в съавторство) в списание. Два от докладите са индексирани в базата данни Scopus. Към днешна дата не са отбелязани цитирания на публикациите в базата данни Scopus.

В представените научни публикации са публикувани основни части от дисертационния труд, което доказва, че основните резултати от него са добре предствени на редица национални и международни форуми и са станали известни на научната общност.

8. Резултатите от дисертационния труд използвани ли са вече в научната и социалната практика?

Не са представени доказателства за внедряване на резултатите на дисертационния труд.

9. Мотивирани препоръки за бъдещо използване на научните и научноприложните приноси: какво и къде да се внедри.

Като бъдеща работа в тази област и продължение на настоящата разработка, би могло да се помисли за реализиране на програмна система и експериментиране и апробиране на предлагания подход в реална бизнес среда.

10. **Авторефератът направен ли е съгласно изискванията, правилно ли отразява основните положения и научните приноси на дисертационния труд?**

Авторефератът е разработен съгласно изискванията на ТУ-Варна. В него достатъчно подробно и точно, но в кратък вид, се отразява същността на дисертационния труд, неговите резултати, поставени задачи и приноси.

11. **Критични бележки по дисертацията, включително и по литературната осведоменост на кандидата.**

Съществени забележки и препоръки към дисертационния труд нямам. Като изготвящ мнение на дисертационния труд, преди да бъде представен за предварителна защита, бях отправил няколко конкретни забележки и препоръки за подобряване на представения материал.

Прави впечатление, че инж. Петко Генчев, се е съобразил с голяма част от направените критични бележки по представения за предварителна защита материал. Повечето отбелязани пропуски от редакционен характер са своевременно коригирани. Добре щеше да бъде ако бе направен по-подробен преглед на конкретни реализации на УРСИ.

ЗАКЛЮЧЕНИЕ

На базата на изложените по-горе анализи на предоставения за рецензия дисертационен труд, задълбочените изследвания в него и оценка на резултатите от разработката, тяхната актуалност, оригиналност, значимост за науката и практиката смятам, че дисертационният труд **„Подход за мониторинг на риска в системи за информационна сигурност“,** отговаря на изискванията на ЗРАСРБ и Правилника за неговото приложение за придобиване на образователна и научна степен “доктор”. Това ми дава основание и давам положителна оценка на дисертационния труд и предлагам на членовете на уважаваното научно жури да гласуват за придобиване от **маг. инж. Петко Генчев Генчев** на образователна и научна степен „**доктор**” по докторска програма „Системно програмиране“ към професионално направление: 5.3 „Комуникационна и компютърна техника.

гр. Варна Рецензент:……

30 Декември 2022 /доц. д-р инж. Росен Радков/