СТАНОВИЩЕ

от доц. д-р Юлиана Пенева Пашкова

преподавател в Нов български университет, деп. “Информатика“

на дисертационен труд за присъждане на образователната и научна степен **'доктор'**

в област на висше образование 4.Природни науки, математика и информатика.

професионално направление *4.6 Информатика и компютърни науки*.

докторска програма *Информатика*

Автор: *Тони Пламенов Каравасилев*

Тема: *„Софтуерна рамка за криптографски услуги“*

Научен ръководител: *проф. д-р Елена Петрова Сомова*

доц. д-р Светослав Христосов Енков

Пловдивски университет „П.Хилендарски“

1. Общо представяне на процедурата и докторанта

Със заповед № Р33-5350 от 22.10..2021 г. на Ректора на Пловдивския университет „Паисий Хилендарски" (ПУ) съм определена за член на научното жури за осигуряване на процедура за защита на дисертационен труд на тема „Софтуерна рамка за криптографски услуги“ за придобиване на образователната и научна степен ‘доктор’ в област на висше образование 4. Природни науки, математика и информатика, професионално направление 4.6 Информатика и компютърни науки, докторска програма Информатика. Автор на дисертационния труд е Тони Пламенов Каравасилев – докторант в редовна форма на обучение към катедра Компютърна Информатика с научни ръководители проф. д-р Елена Петрова Сомова и доц. д-р Светослав Христосов Енков от ПУ „Паисий Хилендарски“- ФМИ.

Представеният комплект материали на хартиен носител е в съответствие с Чл.36 (1) от Правилника за развитие на академичния състав на ПУ, и съдържа:

- молба до Ректора на ПУ за разкриване на процедурата за защита на дисертационен труд;
- автобиография в европейски формат;
- протокол от катедрения съвет, свързан с докладване на готовността за откриване на процедурата и с предварително обсъждане на дисертационния труд;
- дисертационен труд;
- автореферат;
- списък на научните публикации по темата на дисертацията;
- копия на научните публикации;

- списък на забелязани цитирания;
- декларация за оригиналност и достоверност на приложените документи;
- справка за спазване на специфичните изисквания на съответния факултет;
- справка за спазване на минималните национални изисквания;

Докторантът е приложил 5 публикации.

Докторант Тони Каравасилев е завършила бакалавърска специалност „Информатика“ и магистърска специалност „Софтуерни технологии“ в ПУ „Паисий Хилендарски“ и двете с успех 6.00. В последните осем години Т.Каравасилев работи като системен администратор на компютърни системи, мрежи и бази данни в ПУ и като старши програмист в софтуерни компании. Има опит в разработването на уеб-базирани приложения, както и в системното администриране на компютърни мрежи, сървъри и системи.

2. Актуалност на тематиката

Защитата на цифровите данни от неправомерен достъп е от стратегическо значение при техния пренос и съхранение в съвременните компютърни системи с оглед осигуряване на точна, актуална и непротиворечива информация. Изискванията за информационна сигурност на разработвания софтуер водят до включването на множество криптографски процедури. Въвеждането на различни регулации, регламенти и стандарти за обработка на данни (напр. GDPR), както и провежданият при валидация задължителен одит на сигурността усложняват допълнително разработването на крайния продукт. Това оказва влияние както върху реализацията, така и върху поддържането на софтуерното решение. В същото време, поради различни причини повечето програмни езици, софтуерни рамки и приложни библиотеки не включват достатъчно пълен набор от криптографски услуги. Липсата на основен криптографски модел и унифицирани протоколи за сигурност усложняват изграждането на софтуерни или мрежови системи. Поради тези причини създаването на интегрален обектно ориентиран криптографски модел, предлагащ услуги, протоколи, примитиви е актуална задача.

Целта на дисертационното изследване е да се създаде софтуерна рамка за криптографски услуги, която да се прилага при разработването на софтуер. Тя предполага изграждането на общ модел и съставянето на работеща методика за защита на информацията. Въз основа на разработения модел са съставени унифицирани множества от специфични криптографски услуги, протоколи и примитиви. Реализацията им е интегрирана в софтуерна рамка за криптографски услуги, с което се създава предпоставка за повишаване на производителността и качеството на софтуерния процес. Поради това считам, че тематиката на дисертационния труд е особено актуална. Поставената цел и произтичащите от нея задачи са в съответствие със съвременността на проблема.

3. Познаване на проблема

Прегледът на цитираната литература (общо 117 заглавия, всички са на латиница, от тях 29 са интернет източници) позволява да се твърди, че докторантът е навлязъл достатъчно добре в проблематиката. Списъкът е представителен по брой и по разпределение на авторите, включени са публикации от последните 5 години (общо 71 източника, считано от 2016 г.), което е особено важно в областта “информатика”.

Изготвеният от докторанта обзор на съвременните международни стандарти за криптографски системи, качествени подходи за реализация на сигурна мрежова комуникация и добри практики за защита на информацията при пренос, съхранение и обработка показва задълбочено проучване на състоянието на изследванията в разглежданата област. Представени са основните понятия в областта на криптографията и е дискутирана приложимостта на генераторите на псевдо-случайни данни в информатиката. Акцентирано е върху еднопосочната криптографска обработка на данните и нейната приложимост в разработката на хардуерни и софтуерни решения. Изследвано е симетричното криптиране на големи количества от информация, което е особено важно при нейния принос и съхранение. Анализирани са асиметричните криптографски алгоритми и тяхното приложение зя реализирането на сигурна мрежова комуникация по публичен канал.

4. Методика на изследването

Методиката, приложена от докторант Тони Каравасилев, произтича от поставените цели и обособените изследователски задачи. Налице са методическите компоненти на дисертационна разработка с практическа насоченост: анализ на състоянието, теоретичен модел, софтуерна реализация, експеримент за прилагането ѝ, отзиви от потребителите. След проведеното проучване в областта и дефиниране на проблема е разработен подходящо обоснован модел за криптографски услуги. Предложена е специализираната софтуерна рамка, публикувана онлайн под името CryptoMañana, която предоставя тези услуги, с цел интегриране на мерките за мрежова и информационна сигурност при създаването на софтуер. Тази рамка е тествана за съвместимост с различни платформи, както и за съответствие между реализирана и проектирана функционалност. Планирани са съответни експерименти, за да се оцени практическата приложимост на разработката, проведено е анкетиране на потребителите, количествен и качествен анализ на получените резултати. Може да се твърди, че докторантът Тони Каравасилев е приложил методически похвати, присъщи на коректно научно изследване.

5. Характеристика и оценка на дисертационния труд и приносите

Дисертацията с общ обем от 165 страници съдържа следните компоненти: увод, четири глави и заключение, списък на използваната литература, 9 приложения, списък на авторските публикации по темата и декларация за оригиналност Работата е илюстрирана с подходящо избрани фигури (общо 46) и таблици (общо 10), и като обем е напълно в нормите.

Формулираните четири задачи произтичат от целта на дисертационното изследване: да се създаде софтуерна рамка за криптографски услуги, която да се прилага при разработването на софтуер. Приносите са научни, научно-приложни и приложни, като обхващат: разработване на унифициран, платформено независим модел на криптографски услуги; съставяне на подходяща методика за защита на информацията; проектиране на архитектура за управление на криптографски услуги и примитиви, реализиране на софтуерна рамка като приложен инструмент за създаване, управление и конфигуриране на сигурни софтуерни услуги и среди. Основен извод от извършените проучвания и проведения експеримент е, че предложената софтуерна рамка и нейният криптографски модел осигуряват необходимите услуги, свързани с информационната сигурност при създаването на софтуер. Резултатите от проведено анкетиране на крайна потребители потвърждават нейната приложимост и ползваемост.

Перспективите за развитие на тематиката обхващат: доуточняване на предложения обектно ориентиран криптографски модел и разширяване на софтуерната рамка с нови услуги и протоколи.

6. Преценка на публикациите и личния принос на докторанта

Докторантът е представил списък от пет публикации по дисертационното изследване. В тях са отразени основните резултати, получени в дисертационния труд. Докладвани са на катедрени и докторантски семинари, на национални и международни научни форуми. Резултатите са представени в достатъчна степен пред специализирана научна аудитория. Като брой публикациите са достатъчни. Изпълнени са специфичните изисквания на ФМИ. Четири от публикациите са в съавторство, една – самостоятелна, всички са на английски език и в трудове на конференции (две национални и три международни). Самостоятелната публикация е индексирана в световноизвестните бази от данни Web of Science и Scopus, и има SJR=0,198. Тематиката на публикациите подчертава личното участие на докторанта.

Авторът е представил списък от 4 (четири) цитирания на 2 (две) от публикациите по темата в 4 (четири) научни изследвания от чуждестранни. автори. Три от тях са цитирани в статии, индексирани в световните бази от данни.

7. Автореферат

Авторефератът е съставен според изискванията и отразява достатъчно пълно всички аспекти на дисертационното изследване. Обобщени са основните постигнати резултати и приносите на автора.

8. Препоръки за бъдещо използване на дисертационните приноси и резултати

Дисертационните приноси и резултати могат да се използват при осигуряване на защита на данните от неправомерен достъп в реална среда чрез интеграцията на криптографски услуги при разработването на софтуер. С помощта на предложената софтуерна рамка, представляваща приложен инструмент за създаване, управление и

конфигуриране на сигурни софтуерни услуги и среди, става възможно лесното вграждане на мерките за мрежова и информационна сигурност при създаването на различни приложения.

ЗАКЛЮЧЕНИЕ

Дисертационният труд ***съдържа научни, научно-приложни и приложни резултати, които представляват оригинален принос в науката*** и **отговарят на всички** изисквания на Закона за развитие на академичния състав в Република България (ЗРАСРБ), Правилника за прилагане на ЗРАСРБ и съответния Правилник на ПУ „Паисий Хилендарски“. Представените материали и дисертационни резултати **напълно** съответстват на специфичните изисквания на Факултета по математика и информатика, приети във връзка с Правилника на ПУ за приложение на ЗРАСРБ.

Дисертационният труд показва, че докторантът Тони Пламенов Каравасилев **притежава** задълбочени теоретични знания и професионални умения по научна специалност информатика като **демонстрира** качества и умения за самостоятелно провеждане на научно изследване.

Поради гореизложеното, убедено давам своята ***положителна оценка*** за проведеното изследване, представено от рецензираните по-горе дисертационен труд, автореферат, постигнати резултати и приноси, и ***предлагам на почитаемото научно жури да присъди образователната и научна степен 'доктор'*** на Тони Пламенов Каравасилев в област на висше образование: 4. Природни науки, математика и информатика, професионално направление 4.6 Информатика и компютърни науки, докторска програма „Информатика“.

24.11.2021 г. **Изготвил становището**: .....

Доц. д-р Юлиана Пенева