СТАНОВИЩЕ

от д-р Светослав Христосов Енков – доцент в ПУ „Паисий Хилендарски“, ФМИ

на дисертационен труд за присъждане на образователната и научна степен **„доктор“**
по 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“

Научни ръководители: проф. д-р Елена Петрова Сомова и
доц. д-р Светослав Христосов Енков, ПУ „Паисий Хилендарски“- ФМИ

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 определен 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 от Тони Пламенов Каравасилев комплект материали на хартиен носител е в съответствие с Чл.36 (1) от Правилника за развитие на академичния състав на ПУ, включва всички изискуеми документи: молба до Ректора на ПУ за разкриване на процедурата за защита на дисертационен труд; автобиография в европейски формат; протоколи от катедрения съвет, свързан с докладване на готовността за откриване на процедурата и с предварително обсъждане на дисертационния труд и състав на научното жури; 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; 2 бр. протоколи от заседания на КС за удължаване за доразработване на дисертационния труд.

Всички документи ми бяха предоставени и в електронен вид и са в пълно съответствие с изискваните документи за процедура за придобиване на ОНС „Доктор“ съгласно сайта за процедури по РАСД на ПУ и ЗРАСРБ.

Докторантът Тони Каравасилев е роден през 1992 г., завършил е средно образование през 2011 г. в ГХП „Св. Св. Кирил и Методий“, гр. Пловдив и висше образование в ПУ – ФМИ, като и бакалавърската (2015) и магистърската (2016) степени са завършени с отличен успех 6.00 и златен медал (бакалавърската с отличен 6.00 с похвала). Имах удоволствието да познавам г-н Тони Каравасилев още от 1-ви курс на обучението му за бакалавър, бях много впечатлен от познанията му и работехме по научни статии, впоследствие беше и дипломант под мое ръководство за бакалавър и магистър. Тематиката на дипломните му работи беше „Разработване на криптографски софтуер TNTCrypter“ и „Разширяване на функционалността на криптографски софтуер TNTCrypter“ – впоследствие тези натрупани знания и умения бяха използвани в настоящата дисертационна разработка. Мога да споделя личното си мнение, че с Тони Каравасилев се работи много лесно и приятно, без конфликти, умее да търси бързо и да допълва сам нужната научна информация, както и че спазва изрядно всички стандарти за правопис и оформление на научни трудове и техническа документация. С докторанта имаме и общи научни статии, в процеса на тяхното разработване и публикуване нямаше никакви конфликти и проблеми. Приятно впечатление оставя и факта, че Тони Каравасилев разработи и води успешно 4 поредни години, при засилен интерес от страна на студентите, 2 избираеми дисциплини – „Приложна криптография с .Net“ и „Приложна криптография с PHP“. Друг важен факт от неговата автобиография е неговата работа в продължение на 2.5 години, още студент (12.2013-06.2016), като системен администратор във ФМИ, което допълнително спомогна за нашето взаимодействие и колегиалност (както и с целия колектив на ФМИ).

Тези негови разработки, умения и познания оказаха съществено и ползотворно влияние над разработката на настоящия дисертационен труд, те повлияха и на избора на тематиката.

2. Актуалност на тематиката

С оглед на съвременните тенденции за засилващото се влияние на криптовалутите, както и на постоянно увеличаващите се пробиви в сигурността на компютърните системи (предимно крипто-вирусите и кражбите на данни), по мое лично мнение, значението на познаването на процесите и компонентите в съвременните криптографски услуги и алгоритми представлява фундаментална част от защитата на

цифровите данни, както по време на преноса им, така и през периода на съхранението им.

При наличното изобилие от криптографски алгоритми и протоколи, доста програмни езици, софтуерни рамки и приложни библиотеки не поддържат унифициран набор от криптографски услуги, обектна йерархия или дори базов криптографски модел. Основната причина за този проблем е зависимостта на езиците за програмиране от библиотеки на ниско ниво, изградени изцяло в процедурен стил, както и липсата на реализации от високо ниво на стандартните протоколи за сигурност в обектно-ориентиран вариант.

След направеното от докторанта проучване става ясно, че нуждата от подобна рамка за криптографски услуги е актуална и приложима.

3. Познаване на проблема

Докторантът детайлно е проучил и познава разглеждания проблем, за което може да се съди от проведения в Глава 1. Обзор на криптографската област, разглеждащ в детайли основните понятия и терминология, генераторите на данни, източниците на случайност и трите основни вида криптография – еднопосочна, симетрична и асиметрична, всичко това е използвано в описания в Глава 2. Криптографски обектно-ориентиран модел, който от своя страна е послужил за реализацията на Софтуерната рамка за криптографски услуги (описана в трета глава). В Глава 4. Методика за интеграция на криптографски услуги са представени детайлни алгоритми и диаграми за използването на реализираните криптографски услуги в практически проекти. Проведена е и анкета сред потребители, която потвърждава използваемостта и удовлетвореността от софтуерната рамка. Списъкът на използваната литература е обширен и актуален.

Изброеното затвърждава моето мнение, че разработката се базира върху сериозно проучване на съвременни и актуални публикации, книги и стандарти, надлежно описани и цитирани на мястото на използването им.

4. Методика на изследването

Дисертационното изследване е проведено по схемата: детайлно проучване на проблема и предметната област, конструиране на криптографски обектно-ориентиран модел, който от своя страна служи за реализацията на софтуерната рамка за криптографски услуги и накрая е разработена и методика за интеграция на криптографски услуги с помощта на рамката. Проведена е и анкета сред потребители, която потвърждава използваемостта и удовлетвореността от софтуерната рамка.

Това ми позволява да твърдя, че методиката на изследването е успешна и научно-обоснована.

5. Характеристика и оценка на дисертационния труд и приносите

Основният текст на изследването (общо 165 страници) е придружен от 9 приложения, разработени или подобрени в процеса на работата по дисертационния труд. Списъкът на използваната литература съдържа 117 заглавия, от които 0 на кирилица, 117 на латиница, включително и 29 уеб-базирани източници. За яснотата на изложението допринасят предвидените списъци на използваните съкращения, на таблиците и фигурите и на използваната литература. Приложени са резултати от анкети сред потребители на разработената рамка.

По-горе в т. 3 беше описана структурата на тезиса, която намирам за сполучлива и представяща в максимално добър вид извършената работа. За достоверността на материала, върху който се градят приносите на дисертационния труд нямам забележки и съмнения, участвал съм в процеса на разработка като втори научен ръководител.

7. Приноси и значимост на разработката за науката и практиката

В разгледания дисертационен труд е показано, че осигуряването на защитата на данните по време на пренос и съхранение чрез криптографски услуги става все по-важен и значим фактор при създаването на всички видове софтуерни продукти и представлява задължително изискване за голяма част от съществуващите регулации за обработка на информация. Успешно са създадени множество от методики за изграждане на цялостната защита на информационните системи и са предоставени съвети за практическата им реализация чрез дефинирани сигурни услуги, като част от изградения криптографски модел.

В рамките на дисертационното изследване са поставени и успешно решени следните задачи:

Задача 1. Проучване и анализ на теоретичните основи на криптографията и криптологията;

Задача 2. Проектиране на цялостен криптографски модел на базата на криптографски услуги, протоколи, примитиви и йерархии от обекти, както и на методика за интеграция на криптографски услуги в реална среда;

Задача 3. Изграждане на обектно-ориентирана софтуерна рамка за криптографски услуги на базата на дефинирания криптографски модел и софтуерни абстракции;

Задача 4. Тестване на изградената специализирана софтуерна рамка за съвместимост, производителност и качество, както и анализ на резултатите, включително спрямо съществуващите конкурентни решения или процедурни библиотеки.

С решаването на поставените задачи се постига основната цел на дисертацията – разработване на обектно-ориентирана софтуерна рамка за криптографски услуги. Създадената софтуерна рамка за криптографски услуги CryptoMañana и изграденият обектно-ориентиран криптографски модел дават възможност за практическа имплементация на дефинираните универсални методики за защитаване на информационни системи. В допълнение, те потвърждават използваемостта на проектирания криптографски модел, независимо от избрания език или платформа за реализацията му и успешно запълват липсата на такъв в езика за програмиране PHP.

Основните приноси на дисертацията могат да се характеризират като научни, научно-приложни и приложни.

Научният принос е: създаване на общ платформено независим криптографски модел за представяне на криптографски примитиви и услуги.

Научно-приложните приноси са: създаване на методики за осигуряване на защитата на информационни системи в различен приложен контекст; проектиране на софтуерната рамка за криптографски услуги; предложена е унифицирана архитектура за управление на криптографски услуги и примитиви чрез платформено независим подход за реализация.

Приложните приноси са: реализиране на софтуерната рамка за криптографски услуги; интегриране на криптографския модел в език за програмиране без наличието на вградена поддръжка на криптографски услуги и примитиви; тестване на създадената софтуерна рамка, автоматизирано и с реални потребители, и е направен анализ на получените резултати.

След анализ и оценка на изброените приноси, мога уверено да твърдя, че разработката има научен, научно-приложен и приложен аспект и ще бъде от полза за общността от разработчици на PHP (това се потвърждава и от проведените анкети).

6. Преценка на публикациите и личния принос на докторанта

Може да се счита, че резултатите, получени в дисертационния труд, са апробирани в достатъчна степен пред специализирана научна и потребителска аудитория, тъй като основните от тях са отразени в публикациите на докторанта и са използвани при разработването на софтуерната рамка и методиката за използването ѝ.

Резултатите от дисертационното изследване са представени в 5 (пет) публикации в трудовете на конференции (3 международни и 2 национални). Една от публикациите е публикувана и индексирана в Web of Science и Scopus. В публикациите е безспорна водещата роля на докторанта, в 4 от тях той е водещ автор.

В справката за цитиране се посочват данни за 4 (четири) цитирания на 2 (две) от публикациите по тематиката в 4 (четири) научни изследвания (4 (четири) от чуждестранни автори), от които 3 (три) са цитирани в статии, индексирани в световните бази от данни.

Основните резултати на изследването са докладвани на катедрени и докторантски семинари, на национални и международни научни форуми. Моделите, методиките и софтуерните средства, създадени в рамките на дисертацията, са използвани за създаване на учебни курсове в ПУ „Паисий Хилендарски“ (ФМИ). Приведените в приложения 8 и 9 анкети сред потребители потвърждават увереността в практическата нужда и използваемост на разработените рамка и методики.

Личното участие на докторанта е безспорно, имам лични наблюдения над обема и качеството на извършената работа. Нямам критични забележки и препоръки към проведеното изследване и тезиса.

7. Автореферат

Авторефератът е направен според действащите изисквания и адекватно отразява съдържанието, основните резултати и приноси на дисертационния труд.

8. Препоръки за бъдещо използване на дисертационните приноси и резултати

Мога да препоръчам разработената софтуерна рамка да се популяризира допълнително в Интернет (SEO) и да се осигури нейната поддръжка от докторанта (развитие при нови версии на PHP и отстраняване на новооткрити бъгове) за период от поне 5 години. Мисля че това е лесно постижимо, тъй като тя е публикувана в GitHub и е с open-source лицензи (рамката е с MIT лиценз, а документацията е с Creative Commons Zero v1.0 Universal лиценз), което позволява включването на допълнителни разработчици в нейното развитие. Методиката също е добре да се популяризира, може би с няколко допълнителни статии и публикации.

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 и компютърни науки, като демонстрира необходимите качества и умения за самостоятелно провеждане на научно изследване.

Поради гореизложеното, убедено давам своята ***положителна оценка*** за проведеното изследване, представено от обсъдените в становището 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.

18.11.2021 г. **Изготвил становището**: .....

(доц. д-р Светослав Енков)