# Р Е Ц Е Н З И Я

върху дисертационен труд 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

**Автор на дисертационния труд:** Тихомир Димитров Тенев

**Тема на дисертационния труд:** „Разработване на йерархична таксономия от модели за подобряване на сигурността в информационните системи базирани на микросървисна архитектура“

**Рецензент:** проф., д-р Владимир Тодоров Димитров, ФМИ, СУ „Св. Климент Охридски“

## 1. Актуалност и значимост на разработвания в дисертационния труд проблем

Темата на дисертацията е в областта на компютърната сигурност и по-специално на компютърната сигурност в архитектурата на микроуслугите. Съгласно литературен източник [3] от дисертацията:

„Накратко, архитектурният стил на микроуслугите е подход в разработката на отделното приложение като набор от малки услуги, всяка от които изпълнява свой бизнес процес и комуникира с олекотени механизми, често пъти HTTP ресурс чрез API. Тези услуги са изградени около бизнес способности и независимо се разгръщат от изцяло автоматизирана машинария. Има минимално централизирано управление на тези услуги, които може да са написани на различни езици за програмиране и да използват различни технологии за съхранение на данни.“

Архитектурният стил е средство за реализация на архитектури. Например, чрез архитектурния стил на микроуслугите може да се реализира клиент-сървър архитектурата.

Заглавието на дисертацията указва към сигурността на информационните системи, но разглежданията не са свити само в това направление.

Изследванията в дисертацията са за разработване на йерархична таксономия от образци на сигурност. Получената таксономия не е задължително да е йерархична.

Темата на дисертацията определям по следния начин „Таксономизация на образци за сигурност в архитектурния стил на микроуслугите“. От тази отправна

точка разглеждам актуалността и значимостта на проблематиката на дисертационния труд.

На първо място, проблемите на компютърната сигурност в съвременното общество беше изместен по значимост единствено от COVID-19 пандемията. С всяка година нарастват провалите в сигурността на софтуерните системи, което е свързано със всеобхватното и дълбочинното им навлизане в ежедневието ни, а също така и с нарастващата сложност на приложенията.

На второ място е появата на новия архитектурен стил на микроуслугите. Този стил възникна от Линукс средата като средство за защита на пространствата на имената в операционната система.

По-долу ще използвам за по-кратко „архитектура на микроуслугите“ вместо „архитектурен стил на микроуслугите“.

Макар и съвсем нов стил, той намери бързо подкрепата на редица водещи доставчици софтуер. Причината за това се корени в демонстрираните предимства спрямо съществуващите архитектури и архитектурни стилове.

Концепцията на разглеждания архитектурен се характеризира с двойката контейнер-докер. Фактически микроуслугите са пакетирани в контейнери и се доставят на докерите за изпълнение. Последните могат да са разгърнати както върху физически така и върху виртуални машини. Контейнерите от своя страна са максимално компактни – съдържат само код на микроуслугите и описание на средата за изпълнение. Това прави контейнера стотици и дори хиляди пъти по-малък от виртуалната машина и лесно се прехвърля в мрежата от едно място на друго.

Архитектурната на микроуслугите е развитие на ориентираната към услуги архитектура (също архитектурен стил). Обхватът и приложимостта на архитектурата на микроуслугите поне за сега не е ясен, но очевидно е многообещаващ и има голяма вероятност да революционизира доставката на услуги.

За съжаление, всяка нова технология страда от липсата на сигурност – доставчиците бързат да доставят функционалността игнорирайки сигурността. Случаят с архитектурната на микроуслугите не е по-различен, което очертава актуалността на изследванията в дисертацията.

## 2. Обща характеристика и структура на дисертационния труд

Съгласно дисертацията „Целта на дисертационния труд е разработването на йерархична таксономия от модели за подобряване на сигурността в софтуерни системи базирани на микросървисна архитектура.“. Коментариите по-горе върху заглавието са валидни и за тази формулировка на целта, само ще добавя, че тук по-точно е отразен обекта на изследване, а именно „софтуерни системи“, а не „информационни системи“ както е в заглавието.

Поставените задачи за постигане на целта, съгласно дисертацията, са:

„1. Да се категоризира и гранулира софтуерна архитектура от ново поколение, наричана още Микросървисна архитектура, с цел представянето и под различни форми.

2. Да се направи анализ на заплахите за всяка една от представените категории на микросървисната архитектура.

3. Да се открият подходящи модели за сигурносткоито да влизат в обхвата на отделните категории, уповавайки се на анализът на заплахи.

4. Да се трансформират обосновките и решенията предоставени от различните модели за сигурност към контекста на мокросървисна архитектура.

5. Да се направи йерархичен модел на всички категории от микросървисната архитектура, който да служи като скелет при изграждането на подробна йерархична таксономия.

6. Да се открие и използва подходящ обектно ориентиран език за моделиране с цел привеждане на избраните модели за сигурност в четим вид, като се спазва йерархичността на отделните категории.

7. Да се трансформира езикът за моделиране, така че да може да бъде представен в графичен вид.

8. Да се намерят съвременни продукти с помощта на които може да се създаде устойчива среда за микросървисно приложение.

9. Да се направи изследване, кои от представените модели за сигурност могат да бъдат прилагани посредством избраните съвременни продукти за управление на микросървисни приложения, както и да се даде примерно решение.“

Ще анализирам всяка от задачите. Последните би трябвало да изглеждат така:

1. Изследване на архитектурата на микроуслугите и нейните реализации.
2. Анализ на заплахите общи и специфични за архитектурата на микроуслугите.

3. Събиране на образци на сигурност приложими за архитектурата на микроуслугите. Избор на система на заплахите. Систематизация на образците на сигурност по системата на заплахи.
4. Формулировка на образците на сигурност в термините на архитектурата на микроуслугите.
5. Изграждане на таксономия на образците на сигурност за архитектурата на микроуслугите.
6. Избор и прилагане на език за описание на таксономията. Последният трябва да има възможности за графична визуализация.
7. Графична визуализация на таксономията.
8. Подбор на среда за разработка на примерно решение с архитектурата на микроуслугите. Разработка на примерното приложение.
9. Прилагане на образците за сигурност към примерното решение.

По-просто казано:

- да се изследва архитектурата на микроуслугите;
- да се съберат образците за сигурност приложими за нея и да се преформулират в нейните термини;
- да се подбере система за класификация на образците и последните да се класифицират по нея;
- да се избере език за описание на таксономията позволяващ графична визуализация;
- да се визуализира графично таксономията; да се подбере среда и примерно приложение за архитектурата на микроуслугите;
- и да се приложат образците за сигурност към примерното приложение.

Уводът, по същество, съдържа кратко описание на главите от дисертацията.

Глава 1 е увод с препратки към литературни източници за архитектурата на микроуслугите. Изложението е неформално и с различни нива на абстракция. Тук е представено виждането на автора за архитектурата.

В тази глава е посочена системата за класификация на заплахите STRIDE. Това е системата на Microsoft за класификация на заплахите по категории приложения разработвани от компанията.

В тази глава е посочено и средството за описание CIM. Това е средство за описание и управление на обекти в информационно-технологични среди.

Визуализацията на CIM описанията е посочено да се извършва с UI Wireframing. Графично представяне на CIM модели е предвидено по стандарт да се осъществява във вид на UML диаграми, за което е разработен съответния стереотип.

Накрая на главата са формулирани цел и задачи на дисертацията, които бяха коментирани по-горе.

Следващите глави, от 2 до 6, разглеждат образците за сигурност в следните проектни (архитектурни) образци: сметка и идентичност, комуникация, постоянни данни, среда, доставчици - трети страни.

Всяка от тези глави започва с неформално описание на проектния образец и се дискутира спецификата на заплахите по STRIDE. След това следва препратка към публикация, в която са събрани образците на сигурност по дадения проектно-технологичен образец. Това е препратка към публикация на докторанта (съвместна с научен ръководител или самостоятелна). Следва коментар за всеки образец на сигурност в посока STRIDE.

Накрая главата завършва със заключение.

Коментарите по образците на сигурност са по предложената от автора архитектура.

Глава 7 дава кратко описание на CIM. Идеята е образците на сигурност да бъдат описани с CIM като обекти.

Таксономията е представена като йерархия, която е организирана по предложената архитектура.

Визуализацията на таксономията е направена във вид на таблици. Първото измерение са образците на сигурност, а второто е по STRIDE. За всеки проектно-технологичен образец е изведена по една таблица.

Образецът на сигурност е описан с атрибутите Pattern (има на образеца на сигурност), Context (контекст на приложение), Solution (описание на решението), STRIDEAccronim (класификация на заплахата или заплахите по STRIDE) и Reference (източник на образеца на заплаха).

В Глава 8 се прилага таксономията към детайлизираната архитектура на прототипното решение. Тук образците на сигурност по проектните образци са свързани с конкретни софтуерни компоненти на софтуерното решение. Представени са конкретните разработки по образците на сигурност.

Глава 9 е заключение на половин страница.

Глава 10 е за приносите на дисертационни труд. Изброени са 6 такива, които коментирам в съответния раздел на рецензията.

Глава 11 е декларация за оригиналност.

В Глава 12 е приложен пълният текст на таксономията в CIM.

Глава 13 е за използваната литература. Това са 111 източника предимно от Интернет.

**3. Степен на проникване в проблема и оценка за състоянието на решаването му към настоящия момент**

Архитектурата на микроуслугите е твърде нова и вижданията за нея на различните автори значително варират.

Класификацията STRIDE на Microsoft не е единственият подход към заплахите – нивото е твърде високо. Най-общо заплахите се детайлизират като уязвимости, слабости и образци на атаки. При това уязвимостите се „типизират“ по слабостите, а за слабостите и атаките има силно развити и утвърдени таксономии по назначение.

Получените резултати в дисертацията са валидни за разглежданата архитектура (не за архитектурния стил на микроуслугите). Те не могат да бъдат обобщени за архитектурата на микроуслугите. Предлаганите в дисертация решения са частни.

**4. Относно избраната методика на изследванията**

В дисертацията няма формулирана методика на изследванията. Подходът към изследванията е чисто инженерен.

Представена е архитектура с определени проектни образци и за нея са приложени образци на сигурност. По проектните образци са класифицирани образците на сигурност и последните са характеризирани по заплахите от STRIDE. Образците на сигурност са приведени към проектно – технологичните образци. Накрая е детайлизирана архитектурата до проект с конкретни софтуерни компоненти като при детайлизацията образците на сигурност са конкретизирани до код.

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

Дисертацията е от 151 страници. Състои се от увод, 8 глави, заключение, приноси, декларация за оригиналност, приложения, използвана литература и списък

с публикациите по дисертацията. Използваната литература включва 111 заглавия на английски език. От публикации 49 са от материали от конференции и публикации, останалите 52 са от Интернет източници.

Уводът е от 2 страници, Глава 1 – 11, Глава 2 – 12, Глава 3 – 20, Глава 4 – 7, Глава 5 – 10, Глава 6 – 8, Глава 7 – 15, Глава 8 – 15, Заключение – 1, Приноси – 1, Декларация за оригиналност – 1, Приложения – 28, Използвана литература – 8, Списък с публикациите по дисертацията – 1.

Основните елементи, върху които се гради дисертационния труд, са архитектурните образци и образците на сигурност.

Архитектурните образци са технологично фиксирани в дисертацията – това са проектно-технологични образци. Архитектурата като технологично решение е фиксирано от докторанта. Тези образци са добре известни както и техните технологични реализации. В дисертацията те са комбинирани в инженерно решение.

Образците на сигурност в дисертационния труд са взети от източници, в които автор или съавтор е докторантът. Посочени са източниците за всеки отделен образец на сигурност.

## 6. Основни научни и научно-приложните приноси в дисертационния труд

Приносите на дисертацията са посочени както следва (номерацията е от мен):

1. Извършено е изследване и анализ на архитектурите базирани на микросървиси с цел повишаване на сигурността.
2. Предложен е концептуален модел, прилагащ микросървисна архитектура, с помощта на който са Graphical.
3. Извършен е анализ на заплахите върху дефинираните уязвими области, като за всяка са предложени съответни модели за сигурност и обосновката на решенията.
4. Разработен е йерархичен модел и е представена йерархична таксономия от модели за сигурност с помощта на обектно ориентирано моделиране.
5. Разработен е графичен интерфейс, който онагледява връзките между уязвимите области в микросървисните архитектура и избраните модели за сигурност.
6. Представена е архитектура на платформа имплементираща предложените модели, чрез използване на съвременни технологии за управление на микросървиси.

По принос 1, авторът се е запознал с архитектурите на микроуслугите и с редица образци на сигурност.

По принос 2, авторът е дефинирал архитектура на базата на шест проектно-технологични образци. Смисълът, който влага в характеристиката „Graphical“ е неясен.

По принос 3 е направена класификация на образците на сигурност по STRIDE и по проектно-технологичните образци. Образците на сигурност са коментирани в контекста на технологиите на архитектурните (проектно-технологичните) образци.

По принос 4 е създадена CIM таксономия на образците на сигурност във вид на обекти за управление на конфигурация. Таксономията е йерархична в смисъла на предложената архитектура.

По принос 5 е визуализирана разработената таксономия във вид на таблици по проектно-технологичните образци.

По принос 6 е представено компонентно-детайлизирано решение на архитектурата от дисертацията с детайлизация до ниво код или конфигурация на образците на сигурност.

## 7. Оценка на авторското участие в получаване на приносите

За оригиналност на представената работа може да се съди по декларацията за оригиналност. Публикациите по дисертационния труд или са в съавторство с научния ръководител или самостоятелни. Няма декларации за приносите в тези публикации. В предвид на обстоятелствата и от изложеното в дисертационния труд може да се заключи, че приносите по дисертацията са дело на докторанта. Ролята на научните ръководители е била по-скоро методологична.

## 8. Преценка на публикациите по дисертационния труд

По дисертационния труд са представени 5 публикации:

1. Tihomir Tenev, Dimitar Birov, Security Patterns for Microservice Account and Identity, In proceedings of 15th International Conference on Informatics and Information Technologies, 2018, pages:124-128, ISBN:978-608-4699-08-8,
2. Tihomir Tenev, Dimitar Birov, Security Patterns for Microservice Communication, Доклади на Четиридесет и седма пролетна конференция на Съюза на математиците в България, 2018, ISSN (online):1313-3330

3. Tihomir Tenev, SECURITY PATTERNS FOR MICROSERVICE DATA MANAGEMENT, In proceedings of Doctoral Conference: Young Scientists, 2018, pages:575-581, ISBN:978-954-07-4611-1
4. Tihomir Tenev, Dimitar Birov, SECURITY PATTERNS FOR MICROSERVICES LOCATED ON DIFFERENT VENDORS, VII International Conference on Engineering, Technologies and Systems TECHSYS 2018, Technical University – Sofia, Plovdiv, 2018, pages:130-133, ISSN (online):2535-0048
5. Tihomir Tenev, Simeon Tsvetanov, Enhancing security in Microservice environments, 9th Balkan Conference in Informatics, ISec2019 Workshop, 2019

Публикация 1 е на международна конференция в Северна Македония и е цитирана като [27] в списъка с използвана литература.

Публикация 2 е цитирана като [42] в списъка с използвана литература.

Публикация 3 е цитирана като [54] в списъка с използвана литература.

Публикация 4 е цитирана като [65] в списъка с използвана литература.

Публикация 5 е публикувана в списание Computer and Communications Engineering, Vol. 13, No. 4, 2019 и е цитирана като [59] в списъка с използвана литература.

Посочените публикации са основата на глави 2-6. Основните резултати от тези глави са публикувани.

**9. Използване на получените в дисертационния труд резултати и препоръки за бъдещето им внедряване**

Получените резултати, такива каквито са, могат да бъдат използвани в изследвания на безопасността на архитектурата на микроуслугите. Натрупана е немалко фактология.

**10. Относно автореферата към дисертационния труд**

Авторефератът към дисертационния труд е от 40 страници. В него е изнесена основната част от съдържанието на дисертационния труд.

**11. Критични бележки**

Дисертацията не е добре оформена.

Номерацията на отделните части на дисертацията е еклектична и объркваща. Например, Увод е отделна част, но ЗАКЛЮЧЕНИЕ е с номер 9.

Реферираната литература е сведена до ненужно ниско ниво. Например [26] е Gmail.

По-голяма част от терминологията не е преведена от английски. Там където е направен превод от английски това е направено много лошо. Например, „A Pattern for WS-Trust“ просто не е преведено, а терминът „pattern” е преведен на много места като „модел“.

В текста дисертацията липсва обзор и анализ на изследваните области: архитектурата на микроуслугите и на заплахите към софтуерните системи.

**12. Други въпроси**

Не познавам лично докторанта.

Оформянето на дисертацията, поради кончината на научния ръководител доц. Димитър Биров, е поета в последния етап от доц. Симеон Цветанов.

От друга страна, атмосферата в катедрата не е способствала за прецизиране на дисертационния труд.

**13. Заключение**

Представеният от автора дисертационен труд, удовлетворява изискванията на ЗРАСРБ, ПЗРАСРБ, ПУРПНСЗАДСУ и ПУРПНСЗАДСУФМИ. Не ми е известно и не съм открил плагиатство в представения материал. Препоръчвам на уважаемото жури да допусне Тихомир Димитров Тенев до защита на образователната и научна степен „доктор“ в областта на висше образования „4.5 Природни науки, математика и информатика“, професионално направление „4.6 Информатика и компютърни науки“ и препоръчвам положителна оценка.

X
Владимир Димитров

**Дата**: 26 юни 2020 г. **Рецензент**:

.....

гр. София (проф., д-р Владимир Димитров)