

СТАНОВИЩЕ

Относно: Дисертационен труд на Иван Любомиров Дрънков, на тема: „Анализ на изтекли данни с цел разпознаване на потенциални заплахи за информационната сигурност”, представен за придобиване на образователна и научна степен „Доктор“ по професионално направление: 5.13. „Общо инженерство”, докторска програма „Компютърни технологии в инженерната дейност”. от доцент д-р Станислав Димитров, ИИКТ-БАН, член на научното жури,

Информация за процедурата

Съгласно заповед № РД – 13-33 / 24.06.2026 г. на Ректора на МГУ „Св. Иван Рилски” съм избран за член на научно жури, а на първото заседание на научното жури, състояло се на 30.06.2026 г. бях определен да подготвя становище по процедурата, за която получих всички документи.

1. Актуалност на разработения в дисертационния труд проблем в научно и научно-приложно отношение

Дигиталната трансформация представлява процес на организационна промяна, обусловен от все по-широкото използване на информационни и комуникационни технологии в публичния и частния сектор. В резултат на тази трансформация се генерират, обработват и съхраняват огромни обеми от данни, съдържащи чувствителна, поверителна и критична информация.

Успоредно с това развитието на интернет услугите, облачните платформи, социалните мрежи и електронната търговия създава условия за натрупване на значителни масиви от данни. Те представляват ценен стратегически ресурс за организациите, защото подпомагат анализирането на процеси, вземане на решения и създаване на нови услуги. Същевременно тези данни се превръщат в основна цел на различни видове кибератаки.

Злонамерените действия на хакери, уязвимостите в информационните системи, недостатъците на съвременните технологии и ниската дигитална култура на потребителите създават предпоставки за изтичане на големи масиви от данни. Тези масиви се характеризират с голям обем, бързо и интензивно натрупване, разнообразие от формати и различна степен на достоверност.

Посочените характеристики налагат разработването и прилагането на нови методологични и технологични подходи за автоматизирана обработка, анализ и интерпретация на данните, които ще позволят ефективно откриване на аномалии, идентифициране на потенциални киберзаплахи и своевременно подобряване на процесите по управление на информационната сигурност.

Познаване на изследвания проблем

Докторантът показва задълбочени познания от областта в която работи и е изключително добре запознат с естеството на изследвания проблем. Доказателство за това са направеният литературен обзор, който съдържа общо 56 литературни източника основно на английски език и публикуваните резултати.

2. Аналитична характеристика

Дисертационният труд е в общ обем от 131 страници, 82 фигури, 9 таблици, и 56 литературни източника. Структуриран е от списък на съкращения и термини, увод, 4 глави, заключение, приноси на дисертационния труд, източници.

В глава 1 хронологично е проследено влиянието на информацията за обществото и използването на технологиите за нейното разпространение както и необходимостта от защита на данните. Описан е детайлно негативния феномен свързан с дигиталната информация изтичане на данни. Представени са методи за класифициране на видовете изтекла информация и законовите изисквания за работа с тях. Изготвен е обширен обзор на характеристиките и особеностите на съществуващите системите за обработване и анализ на изтекли данни.

В глава 2 е представена методология за създаване на Активна Система и Анализатор на Изтекли Данни АСАИД като са представени етапите на нейното разработване, моделът за изграждане и възможностите за изграждане и разширяване и поддържане на висока ефективност.

В глава 3 е представено изследването на проблеми с форматирането, валидиране и верифицирането на данни, филтрирането и откриването на данните според определени критерии. Изготвен е анализ разпределението на данните и класифицирането на данните в различни категории. Приложен е междинен формат за преобразуване на стандартизирани и не стандартизирани данни. Използват се функции за съхранение на необработени данни и различни техники за компенсиране на данните. Описани са различните видове анализи, които се реализират в разработената система и разгледан сценарии относно ефективността от прилагането на АСАИД.

В глава 4 са описани технологичните средства, хардуерните ресурси и създадените модули за реализация на АСАИД. Проучено реализирането на системата като облачна технология и нейните недостатъци. Представен е процеса по събиране на данните и първоначална обработка със създадения от докторанта модул ruformat, които е сравнен с MS Excel по отношение времето за обработка на данните. Детайлно са представени всички анализи, които могат да се реализират и генериране на отчет от тях. Представен е сравнителен, който показва предимствата на разработената система над съществуващите.

В заключението са обобщени получените резултати в от сложна задача за проектиране на цялостно решение за изследване и анализиране на изтекли данни. Резултатите от тези изследвания са средство за увеличаване на информационната сигурност.

3. Обект и Съответствие на избраната методика на изследване с поставената цел и задачи на дисертационния труд и с постигнатите приноси

Обект на изследването е процесът на автоматизирана обработка, унифициране и анализ на големи обеми хетерогенни данни от изтекли или компрометирани източници.

Предмет на изследването е профилирането, категоризацията и извличането на потенциални заплахи от изтекли и компрометирани данни.

Целите на изследването са насочени към разкриване на закономерности и зависимости в обработваните данни, които да подпомогнат ранното откриване на рискове и изграждането на механизми за превенция на киберзаплахи.

Избраната методология в изследването се основава на представянето на АСАИД като информационна система, изградена от множество функционално взаимосвързани подсистеми. Основните подсистеми включват база от данни, система за управление на базата от данни, анализатор на данните, система за известяване и система за съхранение.

Архитектурата на информационната система е модулна трислойна клиент-сървър структура, с клъстерен сървър, база от данни без споделяне (shared-nothing database) и допълнителни изчислителни модули. Трислойната архитектура обособява слоевете за представяне, приложна логика и управление на данните, което позволява разделяне на функционалностите и независимо развитие на отделните компоненти.

Използването на клъстерна архитектура и база от данни без споделяне осигурява възможност за разпределяне на обработката и съхранението на данните между отделни изчислителни ресурси. Допълнителните изчислителни модули подпомагат автоматизираната обработка и анализа на големи обеми хетерогенни данни.

По този начин разработената архитектура на АСАИД създава единна среда за приемане, унифициране, съхранение, обработка и анализ на данни от изтекли или компрометирани източници. Чрез реализираните функционални подсистеми се създават предпоставки за автоматизирано профилиране и категоризиране на данните, откриване на закономерности и зависимости и идентифициране на потенциални рискове и киберзаплахи.

4. Оценка на автореферата и публикациите на автора, свързани с дисертационния труд

Представените автореферати на български и английски език, отразяват достоверно съдържанието на дисертационния труд и съответстват на изискванията на ЗРАСРБ и ППЗРАСРБ. От представената декларация за оригиналност и описанието на резултатите, може да се определи, че са лично дело на докторанта.

Докторантът има 2 публикувани статии и една приета за печат. Едната статия е самостоятелна, а другите две са в съавторство, като Иван Дрънков е първи автор. Не са докладвани цитирания на публикации към настоящия момент.

Така представените публикации по темата на дисертацията напълно удовлетворяват специфичните изисквания на МГУ „Св. Иван Рилски“ за придобиване на образователна и научна степен „Доктор“, т. к. от изискуемите 30 точки, докторантът има 40 т.

Резултатът от проверката за плагиатство от сайта StrikePlagiarism.com, показва следните резултати: Коефициент за сходство 1: 1,63 % и коефициент за сходство 2: 0,65 %

5. Приноси на докторанта

Напълно приемам така формулираните приноси на докторанта.

6. Мнения, критични бележки и препоръки

Нямам критични забележки към работата на докторанта, а само редакционни. След направените препоръки от мен по време на разширения катедрен съвет на катедра „Математика и информатика“ при МГУ „Св. Иван Рилски“ на 10.06.2026 г., относно вътрешна защита на дисертационния труд на Иван Дрънков, потвърждавам, че той ги е отработил и отразил в окончателния си вариант на своето дисертационно изследване.

7. Заключителна комплексна оценка

Получените резултати по темата на дисертационния труд показват убедително, че Иван Любомиров Дрънков притежава необходимите теоретични знания и практически умения в сферата на информатиката и компютърни науки. Представеният дисертационен труд напълно отговаря на изискванията на Закона за развитие на академичния състав в Република България, Правилника за неговото прилагане, както и на Правилника за приложението му и Правила и процедури за приемане и обучение на докторанти и придобиване на ОНС „Доктор“ и НС „Доктор на науките“ на Минно-геоложки университет „Св. Иван Рилски“, София. **Получените резултати в дисертационния труд ми дават основание да дам категорично положителна оценка на представения труд и предлагам на уважаемото Научно жури да присъди на маг. инж. Иван Любомиров Дрънков образователната и научна степен „Доктор“ по докторска програма „Компютърни технологии в инженерната дейност“, професионално направление 5.13. „Общо инженерство“.**

11.08.2026

Член на журито:

/доц. д-р инж. Станислав Димитров/