

СТАНОВИЩЕ

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

Тема на дисертационния труд: **АНАЛИЗ НА ИЗТЕКЛИ КРИТИЧНИ ДАННИ С ЦЕЛ РАЗПОЗНАВАНЕ НА ПОТЕНЦИАЛНИ ЗАПЛАХИ ЗА ИНФОРМАЦИОННАТА СИГУРНОСТ**

Професионално направление **5.13. “Общо инженерство”**

Докторска програма „**Компютърни технологии в инженерната дейност**“

Автор на дисертационния труд: **маг. инж. Иван Любомиров Дрънков**

Председател на научното жури: **доц. д-р инж. Йорданка Анастасова**

Представеният дисертационен труд е в обем 131 страници. Съдържанието е структурирано в Увод, Четири глави, Заключение, Приноси на дисертационния труд, Публикации, Литературни източници. Информацията е илюстрирана с 80 фигури и 9 таблици.

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

Проблемът с изтичането на критични данни е от особена значимост за сигурността при информационните системи поради факта че те съдържат чувствителна, конфиденциална или структурно определяща информация и могат да се ползват за последващи пробиви, компрометиране или неототоризиран достъп.

Целта на дисертационния труд е разработване и прилагане на методологичен подход за автоматизирана обработка, унифициране и анализ на големи обеми хетерогенни данни от изтекли или компрометирани източници с цел профилиране, категоризация и извличане на потенциални заплахи. За реализация на целта са дефинирани и изпълнени пет основни задачи, при чието решаване са използвани съвременни подходи и технологии.

Направеното изследване, представено в дисертационния труд, цели да се разкрият закономерности и зависимости, които да подпомогнат ранното откриване на рискове и изграждането на механизми за превенция на киберзаплахи.

2. Степен на познаване на състоянието на проблема и творческа интерпретация на литературния материал

В дисертационния труд авторът показва много добро познаване на тематиката и адекватна интерпретация на литературния материал. Това личи ясно от направения в първа глава на дисертацията обзор на съществуващите и използвани системи за анализ на изтекли критични данни. Докторантът предлага и дефиниция за система за анализ на критични данни, както и методи за класификация на видовете изтекли данни.

Класифицирани са 3 основни вида системи за анализ на критични данни, а именно пасивна, система за известяване и активна.

В резултат от направените проучвания ясно е дефинирана целта и конкретизирани задачите в дисертационния труд.

Дисертационният труд е в обем от 131 страници и включва 80 фигури и 9 таблици. Използвани са 56 библиографски източника, от които само 1 на български и 55 на английски, които коректно са посочени за достъп онлайн и са коректно цитирани в дисертационния труд. Преобладаваща част от източниците са публикувани в последните години, което показва задълбочено познаване на съвременните тенденции в областта на анализа на критични данни.

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

Докторантът е избрал методология за създаване на система АСАИД, която включва 5 основни подсистеми, а именно Бази от данни, Система за управление на бази данни, Анализатор на данните, Система за известяване и Система за складиране. За реализация на АСАИД е използвана модулна трислойна архитектура тип клиент-сървър, включваща клиентски, сървърен слой и слой за данни (база данни без споделяне), както и помощни модули за изчисление.

Важен елемент при анализа на изтекли критични данни е събирането им в суров вид и обработката, което в реализираната АСАИД Pyformat включва модули за валидиране, верифициране, форматиране, филтриране, компресиране и архивиране на данните. Докторантът е избрал формат CVS поради факта, че има малък обем и работи с ZFS файлова система, която поддържа няколко вида компресиране.

Анализите на изтекли критични данни включват анализ на пароли, вида и декриптирането им, на brutforce атаки, на установяване на локация, триангулация и последно местоположение, документи, изображения и метаданни. Целта на извършвания анализ е откриване на потенциални заплахи и атаки.

Разработената АСАИД се базира на технологичен стек – съвкупност от всички необходими технологии, програмни езици, рамки (frameworks) и инструменти. Предложеният модел за модулна трислойна архитектура клиент-сървър включва клиентски слой, клъстерен сървър, база данни без споделяне и допълнителни модули за изчисление. Клиентският слой е разработен непълно в прототипа, като включва контроли за работа с АСАИД и служи за визуализация на данните. Показан е псевдокод, който демонстрира принципите на свързване между клиентския и сървърния слой чрез API. За реализация на слоя данни в АСАИД се използва технологията MongoDB Sharded Cluster. Реализиран е модул за известяване, който е основен компонент в АСАИД и работи във фонов режим, като в представената реална система ползва Python.

Оптималното решение е АСАИД да бъде реализирана като облачна система, но цената за това е твърде висока за нуждите на дисертацията. В предложената АСАИД първо се намират и верифицират данните, което се реализира с различни технологии. Обработката на данните се извършва с модула Pyformat, който е създаден с Python и файл на XML.

Проведени са експерименти с реални данни, като е използвана информация с големина приблизително 2 TB, която е преобразувана във формат CSV. Анализирани са шаблони за пароли, като са използвани около 4 милиона реални потребителски пароли и обект на анализа са дължината на паролите и най използваните символи и клавиши.

Представени са и модули за анализ на локация, триангулация и намиране на последни следи при реален случай, анализ по домейн, който представлява методика за проследяване и оценка на изтекли данни за конкретна организация. Показани са и модули за анализ на изображения и метаданни.

Системата АСАИД автоматично анализира наличната база данни с изтекли или компрометирани такива, класифицира ги по категории и свързва всяка категория с потенциални заплахи, като може да разиграе сценарии за атаки с цел оценка на риска и предприемане на защитни мерки.

Крайният резултат е автоматично генериран аналитичен доклад, съставен от модула на системата АСАИД въз основа на резултатите от извършените анализи.

Сравнителният анализ между създадената АСАИД и съществуващите системи за анализ на изтекли критични данни показва, че тя включва множество аналитични модули, които позволяват обработка на различни типове данни, автоматизирано откриване на зависимости и извеждане на информация за възможни атаки и уязвимости.

Дисертационният труд разглежда сложната задача за проект на цялостно решение за изследване и анализиране на изтекли данни, което е особено важно за увеличаване на информационната сигурност, която се явява основно предизвикателство в съвременния дигитален свят.

Считам, че избраната методика на изследване и реализация напълно съответстват на поставената в дисертацията цел и формулираните задачи, като предлагат цялостен проект и демонстрират частична реализация на АСАИД.

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

Авторефератът отговаря на изискванията на ЗРАСРБ и ПП ЗРАСРБ. Неговите структура и съдържание съответстват на изложеното в дисертационния труд.

Резултатите от изследванията на инж. Иван Дрънков са публикувани в три статии, като 2 са отпечатани, а третата е приета за публикуване. Всички статии са представени на международната конференция на МГУ, която се провежда ежегодно. Публикациите са направени в периода 2022-2026 година и покриват тематиката на представената дисертационна работа, като отразяват постигнатите резултати и приноси.

Една от статиите е самостоятелна, две са в съавторство, като инж. Дрънков е първи автор. Статиите са публикувани в периодичния Annual of the University of Mining and Geology "St. Ivan Rilski" и са индексирани в Google Scholar, CrossRef и Reseachgate. Към настоящия момент не са открити цитирания на представените статии. Публикационната дейност на дисертанта отговаря на изискванията за придобиване на ОНС „Доктор“ и считам, че публикациите са придобили достатъчно публичност в научната общност.

Отчитайки броя и качеството на публикациите считам, че получените резултати са изключително дело на автора, като не съм установила недостоверност на данните или плагиатство, което е отразено и в доклада, генериран от StrikePlagiarism.

5. Оценка на научните резултати и приносите и степента на лично участие на докторанта в разработената тематика

В дисертационния труд авторът е формулирал следните приноси, които приемам и в резюме са както следва:

Научно-приложни:

1. Реализиран е софтуерен продукт Pyformat за обработка на големи масиви изтекли критични данни.
2. Съпоставени са различните видове анализи и принципа им на работа, които се прилагат при изтекли критични данни.
3. Формулирани и анализирани са основните етапи при обработката на големи масиви изтекли критични данни.

Приложни:

1. Създаден е концептуален модел на активна система за анализ и известяване за изтекли данни (АСАИД).
2. Създаден е проект на активна система за анализиране на изтекли данни и известяване (АСАИД), който е частично реализиран.

6. Мнения, критични бележки и препоръки

Дисертационният труд е изготвен в стройна логическа последователност. Коректно са цитирани използваните източници. Описани са подробно използваните съкращения в дисертационния труд. Фигурите и таблиците са цитирани акуратно и допълват много уместно текстовото изложение.

Препоръчвам на докторанта за в бъдеще да публикува получените резултати от работата си и последващите му изследвания в издания, които се индексират в Scopus и WoS.

7. Заключение

Оценявам **положително** дисертационния труд „Анализ на изтекли критични данни с цел разпознаване на потенциални заплахи за информационната сигурност“ с автор маг. инж. Иван Любомиров Дрънков. Считам, че е изготвен прецизно, акуратно и на високо професионално ниво, като авторът е постигнал поставените цели и задачи в дисертационния труд. Резултатите и приносите на дисертационния труд са отразени в научни публикации, които са представени на научната общност на международни конференции, публикувани и индексирани. Научно-приложните и приложни приноси са

значими и съответстват на изискванията за придобиване на научно-образователната степен „Доктор“ съгласно Закона за развитие на академичния състав в Република България, 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.

Предлагам на уважаемото Научно жури да присъди образователна и научна степен „Доктор“ на маг. инж. Иван Любомиров Дрънков в професионално направление 5.13. Общо инженерство, докторска програма „Компютърни технологии в инженерната дейност“.

03.08.2026 г.

Председател на научното жури:

(доц. д-р инж. Йорданка Анастасова)