РЕЦЕНЗИЯ

от доц. д-р Веселина Господинова Жечева
Център по информатика и технически науки,
Бургаски свободен университет

за дисертационен труд
„МОДЕЛИРАНЕ НА МРЕЖОВИ АТАКИ И АЛГОРИТМИ ЗА ЗАЩИТА“

на докторантката ПЕТЯ ИВАНОВА ПЕТРОВА,
по конкурс за присъждане на образователната и научна степен "доктор"
по професионално направление 4.6. "Информатика и компютърни науки"

Тази рецензия е изготвена в изпълнение на Заповед на Ректора на Бургаския свободен университет за откриване на процедура за защита на дисертационния труд на Петя Иванова Петрова, докторант на самостоятелна подготовка в Центъра по информатика и технически науки на БСУ. За целта са ми предоставени съответните материали, в т. ч. дисертационният труд, автореферат, цитираната заповед, протоколи от докторантските изпити, публикации на докторантката и т.н. Всички те поотделно и в съвкупност отговарят напълно на законовите изисквания и текущата практика на българските университети.
Общо представяне: докторантката е завършила Бургаския свободен университет, специалност Информатика и компютърни науки. Работила е в реалния сектор, което й е помогнало да натрупа полезен практически опит.

Тематика на дисертационния труд. Представеният текст на дисертация е на тема, която е безспорно много актуална поради факта, че дигиталните технологии навлязоха във всички сфери на обществения живот. Особено при кризата, свързана със световната пандемия, онлайн бизнес услугите се превърнаха в основно направление за развитие на бизнеса. Това доведе до нарастване на рисковете по отношение на сигурността, като този проблем има нарастваща важност през последните десетилетия. Предлагането на нарастващия обем онлайн услуги води до очаквано високо ниво на информационна и мрежова сигурност. Обектът на изследване в тази дисертация – мрежова сигурност - отговаря на тези тенденции в ИТ бизнеса. Всичко това обуславя актуалността на темата на дисертацията. На тази основа оценявам темата като дисертабилна и много актуална за ИТ сектора.

Методика. Използван е инструментариум, включващ методи от изкуствения интелект, по-точно генетичните алгоритми и диференциалното смятане.

Съдържание. Дисертационният труд е с обем от 114 страници и се състои от увод, 3 глави, заключение, списък на публикациите по дисертационния труд, декларация за оригиналност, приложение и списък с използвана литература. Включени са и списък с използваните фигури и често използвани съкращения.

В ***Увода*** са формулирани целта и задачите на дисертационния труд. Направен е общ обзор на моделирането на компютърните системи в мрежова среда, както и моделиране на сигурността и нейното нарушаване. Описани са някои методи за оценка на въздействието на злонамерен софтуер върху мрежите, както и различни видове нерегламентирано въздействие върху системата. Описани са системите за откриване на нарушения като средство за гарантиране на сигурността на системата и са разгледани различни алгоритми с приложения в областта на сигурността. Обоснована е необходимостта от изследването върху подобряване методите за постигане на сигурност. **Целта** на дисертационния труд е математическо моделиране на процеси в компютърните мрежи при

въздействие със злонамерен софтуер и нерегламентираното поведение на потребител, изграждане и приложение на генетичните алгоритми за откриване на проникванията в компютърната мрежа и защита на данни. Във връзка с тази обосновка са поставени една теоретична и три научно-практически **задачи**, а именно:

- Моделиране на процеси при въздействие на компютърна мрежа със злонамерен софтуер.
- Изграждане и приложение на генетични алгоритми за откриване на проникванията в компютърната мрежа.
- Определяне на функцията на пригодност в генетичния алгоритъм за откриване на прониквате в компютърните мрежи.
- Реализация на мрежова сигурност чрез криптиране с генетичен алгоритъм.

Глава 1, озаглавена „Моделиране на процеси при въздействие на компютърна мрежа със злонамерен софтуер“, съдържа изследване и разработване на математически модел на поведението на компютърната мрежа и динамиката на нейните компоненти, които са податливи, експонирани, инфектирани и възстановени след атака със злонамерен софтуер. За реализиране на математическия модел е използван инструментариум от областта на системите диференциални уравнения, които описват състоянието на мрежата. Приложен е моделът SEIR, използван за описание разпространението на биологичните вируси, за моделиране поведението на компютърен червей в мрежата. Описани са различните състояния на възлите, както и преходите между състоянията чрез функциите на възстановяване и динамиката на типовете възли. Представено е решение на системата от диференциални уравнения и са определени екстремалните стойности на характеристиките на компютърната мрежа при атака със злонамерен софтуер при равновесно и неравновесно състояние на системата. Представени са резултати от числени експерименти при избрани стойности на разгледаните параметри и са изследвани зависимостите на някои характеристики на системата (уязвимост, възстановимост, изложение и т.н.) от времето при равновесие и неравновесие на системата. Направен е изводът, че при ендемично равновесие, т.е. отсъствие на защитен софтуер, показателите, характеризиращи поведението на компютърната мрежа нарастват с изменение на времето, докато при неравновесие, т.е. наличие на защитен софтуер, параметрите имат сложна зависимост от времето.

В ***Глава 2 Изграждане на генетичен алгоритъм за откриване на проникванията в компютърната мрежа*** е описан метод за откриване на нарушения на базата на генетичен алгоритъм. Направен е обзор на класическите системи за откриване и предотвратяване на нарушения, като са разгледани и някои основни видове атаки. Описани са базовите понятия на генетичните алгоритми и тяхното приложение в мрежовите атаки. За описание на правилата е използвана предикатна логика, като състоянията са представени чрез мрежови характеристики (IP адреси на източник и местоназначение и номера на портове, използвани мрежови протоколи, продължителност на комуникацията и др.). Представени са използваните атрибути на правилата с техните типове, диапазони на стойностите и описание, както и хромозомите и форматът на кодовете им. Описани са примерни правила и тяхното предназначение. Представени са основните операции върху хромозомите от дадено поколение – селекция, кръстосване и мутация и оценка на еволюцията на текуща генерация от хромозоми чрез дефинирани функции на пригодност. Включен е и псевдокод на генетичния алгоритъм.

Глава 3 Реализация на мрежова сигурност с помощта на криптиращ генетичен алгоритъм е посветена на алгоритъм за сигурността на данните по време на предаване по мрежата. Представено е подобрение на класическия алгоритъм RSA чрез избора на първоначалните параметри. Описано е приложението на генетичния алгоритъм Алгоритъмът е подробно описан и е представена негова реализация на C# и съответна блок-схема.

Приноси. Авторът на настоящата рецензия приема дефинираните от докторантката научно-приложни приноси, а именно:

1. НАУЧНИ РЕЗУЛТАТИ

1.1. Предложен е модел на процесите на податливост, експозиция, инфекция и възстановяване на компютърна мрежа в случай на въздействие на злонамерен софтуер, описани със система от диференциални уравнения за моментна и прогнозна оценка на състоянието на компютърната мрежа – система от уравнения.

1.2. Предложено е оригинално решение на системата от диференциални уравнения в два случая - на равновесие при константни променливи – аналитичен израз (37) - глава I и отсъствие на равновесие при време зависими променливи - аналитичен израз (65) - глава I, дефиниращи класовете състояния на машините в компютърната мрежа.

1.3. От решението на системата от нехомогенни диференциални уравнения са изведени аналитични изрази за изчисляване на мрежовите характеристики в случай на податливост, експозиция, инфекция и възстановяване (реконструкция) на машините в компютърната мрежа по време на атака със злонамерен софтуер.

2. НАУЧНО-ПРИЛОЖНИ РЕЗУЛТАТИ

2.1. Разработен е софтуерен инструмент за защита на компютърна мрежа чрез криптиране на предаваната информация с приложение на операторите на генетичен алгоритъм, реализиран с програмния език C# (глава III).

2.2. Разработени са софтуерни продукти, реализирани в среда Matlab за илюстрация на решенията на системата диференциални уравнения за моментна и прогнозна оценка.

3. ПРИЛОЖНИ РЕЗУЛТАТИ

3.1. Разширен е списъкът с атрибути, генната структура и кодовете на мрежовите характеристики на хромозомата (правилото) в генетичния алгоритъм, разширяваща обхвата на неговото действие по откриване на мрежови прониквания.

3.2. Оценена е структурата на функцията на пригодност на Firas Alabsi и са илюстрирани основните операции върху хромозомите от дадено поколение с данни, получени от числен експеримент..

3.3. Направена е експериментална оценки на параметрите A, AB на функцията на пригодност на Firas Alabsi с данни, получени от симулиране на мрежови комуникации от типа Normal, DoS, R2L, U2R, Probe, реализирани със случайно генерирани мрежови характеристики на пет хромозомни структури за всяка категория.

Тези приноси надграждат съществуващи анализи и отварят нови насоки за изследване в актуалната и бързо променяща се област на информационната сигурност.

Публикации и участия в научни форуми. Представени са шест публикации, от които 1 е доклад на конференция в България и 5 са статии в научни списания (две в индексирани в SCOPUS издания и две в списъка на НАЦИД). Три от публикациите са на английски и три на български език. Три от публикациите са индексирани в SCOPUS, като на една единствен автор е научният ръководител (https://www.scilit.net/article/3a8dde1b1d44362e92cf2d2581715a50). В приложената справка се вижда, че кандидатката покрива минималните изисквания за публикации.

Списъкът с използвана литература включва 114 източника, от които 98 статии и книги и 16 – интернет ресурси. Библиографията е пълна и актуална, повечето източници са на английски език, като няколко са на български. Ще отбележим, че представените публикации по дисертацията също са включени в списъка с използвана литература. Следва също да се отбележи, че по-малко от половината стати и книги (41 източници) са от последните 10 години, което не е много в бързо променяща се област като информационната сигурност.

Дисертацията е оформена прилежно, всички таблици и фигури са номерирани. Авторефератът е в обем от 36 страници, като правилно отразява съдържанието на дисертацията.

Като цяло този дисертационен труд отговаря на стандартните изисквания за докторска работа, показва висока академична ерудиция и практически умения на докторантката и заслужава положителна оценка. Структурата на дисертационния труд е добре разработена, в логична

последователност на отделните раздели с относително слаба връзка между тях. Отделните глави са посветени на изследвания на различни аспекти на сигурността по отношение на различни заплахи. Като силни страни на дисертацията определям както следва:

- **Актуалността й** - В условията на бързо променящите се условия във виртуалното пространство това изследване и има съществена практическа/приложна стойност.
- **Методическият подход и използвания математически апарат** – В дисертацията са използвани методи от областта на изкуствения интелект (генетични алгоритми) и диференциалното смятане, което показва добра теоретична подготовка.

Във връзка с дисертационния труд могат да се отправят следните **забележки, въпроси и коментари**:

1. Обзорът е по-скоро място за общо въведение в темата, обосновка и формулиране целта и задачите на дисертацията, а не за навлизане в детайли в представянето на различни подходи и алгоритми.
2. Липсва систематичен терминологичен обзор на злонамерените средства / видовете атаки на съвременните системи, както и сравнение на различните въздействия и честотата им в съвременния свят. Оттам можеше да следва по-задълбочена обосновка на избраните модели и изследвания.
3. В глава 1 не е изяснено влиянието на кой защитен софтуер се изследва, както и не са описани мерните единици и интервалите на изменение на величините.
4. В точка 2.9 е казано „Като бъдеща активност на автора … се предвижда изграждане на база от данни (правила, знания) за нови неизследвани структури от мрежови характеристики на компютърни атаки, както и методи за тяхното противодействие и превенция“. По принцип база данни със сигнатури на известни злонамерени средства се използва от години. Може ли докторантката да обясни повече за идеята да се състави база за нови неизвестни средства за атака? База данни, база с правила и знания са различни понятия, кое от всичките се предвижда?
5. В заключението на глава 3 е казано, че „разработеният генетичен алгоритъм е с надеждно и устойчиво криптиране с висока степен на защита на предаваното съобщение и може да бъде приложен при обмен на данни, изискващи високо ниво на сигурност“. Не са приложени данни обаче от експеримент, който доказва това твърдение и не е направено сравнение със стандартния RSA.

Заключение

Направените по-горе забележки и коментари нямат за цел да омаловажат работата, която представлява сериозно изследване в областта на информационната сигурност чрез методите на диференциалните уравнения и генетичните алгоритми. Представеният дисертационен труд отговаря на изискванията на Правилника за развитие на академичния състав в Бургаския свободен университет. Въз основа на изложеното по-горе считам, че кандидатката Петя Иванова Петрова изпълнява всички критерии и изисквания по Закона за развитие на академичния състав в Република България, Правилника за неговото прилагане и Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности в Бургаския свободен университет и предлагам да й бъде присъдена образователната и научна степен "доктор", професионално направление 4.6. "Информатика и компютърни науки".

Подпис:

/доц. д-р В.Жечева/

Бургас
20.05.2022 г.