РЕЦЕНЗИЯ

на дисертационен труд за присъждане на образователна и научна степен „Доктор" по научно направление **4.6 "Информатика и компютърни науки"** и специалност по шифър **01.01.12 "Информатика"**,

на тема:

МОДЕЛИ НА ПРОЦЕСИ В МРЕЖОВА СИГУРНОСТ ЧРЕЗ ОБОБЩЕНИ МРЕЖИ
с автор:
гл.ас. Ивелина Миткова Вардева

Научни ръководители:

проф. дтн дмн Красимир Атанасов, Институт по биофизика и биомедицинско инженерство - БАН
доц. д-р Сотир Сотиров, Университет „Проф. Асен Златаров", Бургас

Рецензент: доц. д-р Стоян Атанасов Порязов, Институт по математика и информатика на БАН, секция „Информационно моделиране"

Дисертационният труд на гл. ас. Вардева е в обем от 119 страници, и е съставен от: използвани съкращения, списък на фигурите, увод, пет глави, заключение, библиография със 107 заглавия и списък на публикациите по дисертационния труд с 9 заглавия.

Разработван проблем: Разработване на модели на процесите в глобален план за видовете атаки в компютърната мрежа, при предаване на медицинска информация; Построяване на симулационен модел, оценяващ степента на атакуване на съобщения в обществената мрежа.

Актуалност: Разработения проблем е изключително актуален, в светлината на Европейската харта за правата на човека и приетите решения относно създаването на интегрирана система за електронен обмен на данни в здравеопазването, въз основа на Националната стратегия за внедряване на електронно здравеопазване в България.

Познаване на изследванията по проблема: Използвани са, с вещина, 107 съвременни публикации по темата, които обхващат всички съществени страни на проблема, разработвани в дисертацията.

Използвана методика: Използвани са методите на системния анализ, обобщените мрежи, интуиционистките размити множества и компютърната симулация. Обобщените мрежи (ОМ) са основният използван метод, който е предложен и развит от един от научните ръководители на докторанта (проф. Красимир Атанасов). Използвани са правилно необходимите, за целта, специфични средства на ОМ, с необходимата дълбочина на разбиране на техните моделиращи възможности. Методите на интуиционистките размити множества, също са разработени от проф. Красимир Атанасов, включително като едно от развитията на ОМ. За симулацията на конкретни модели е използван компютърен симулатор на ОМ, разработен от Валери Гочев, бивш докторант на проф. Атанасов. Методиката е съвременна, подходяща за задачата и е използвана е коректно.

Приноси в дисертационния труд:

В **Глава 1**. са анализирани различни процеси на движението на информация и изграждане на защита между две крайни точки, които могат да бъдат както здравни структури така и пациенти, изискващи лична здравна информация. Обоснована е необходимостта да се осигури защита на личните данни и здравната информация, защита на потребителите, на интелектуалната и индустриална собственост. Обосновано е, че в този аспект ОМ са изключително подходящо средство за моделиране и симулация на процесите в здравеопазването. Описани са, необходимите за изследването, специфични свойства на ОМ и на операторите в тях.

В **Глава 2.** са разгледани основни проблеми в мрежовата сигурност и са предложени ОМ модели на мрежови атаки свързани с подслушване, прекъсване и промяна на предаваните съобщения. Разгледани са системи с асиметричен ключ за криптиране и декриптиране информацията, както и „скала за оценяване на мрежовата сигурност". Тази „скала", в същност, е ОМ модел, който, в изходната си информация, дава интуиционистки-размита оценка за степента на подлагане на различни видове атаки на моделираните съобщения.

В **Глава 3.** са разработени пет ОМ модела: 1) на класическа структура на криптографска система чрез използване на симетричен ключ; 2) Моделиране на SSL (Secure Socket Layer) чрез апарата на обобщени мрежи; 3) ОМ модел на SSL с интуиционистки размити оценки; 4) ОМ модел за създаване наVPN (Virtual Private Network) чрез използване на PPP (Point-to-Point Potocol) върху Scure Shell. 5) ОМ модел на създаване наVPN чрез използване на PPP върху Scure Shell2 за изграждане на безпаролна VPN връзка.

В **Глава 4.** е разработен ОМ модел за защита на данни на пациенти предавани между информационни болнични системи в обществената мрежа.

В **Глава 5.** е проведено тестване на модел, чрез обобщени мрежи и иинтуиционистки размити вярностни стойности, за получаване на оценки за атакуване на съобщения. Тестването се извършва посредством сравняване на стойностите получени от компютърна симулация на ОМ модела и теоретични изчисления. Прави добро впечатление, че: относителната разлика между стойностите от симулация и теоретични изчисления е под 1%, за ядрата минаващи през две позиции; моделът е практически в стационарно състояние почти в целия наблюдаван интервал на броя на постъпилите заявки: от около 384 до 16384.

Приносите в дисертацията могат да се класифицират като научни и научно-приложни, защото представляват създаване и верификация на нови модели на процеси в мрежова сигурност чрез ОМ, които имат пряка приложимост.

Получените резултати могат да подпомагат създаването и внедряването на специфични за здравеопазването софтуерни и хардуерни продукти, които да бъдат съобразени с международните стандарти за обмен и защита на медицинските данни (например оразмеряване при проектиране и управление на системите). Те позволяват да се осигури възможност за статистически анализ относно сигурността, при предаване на конфиденциална информация. Моделите могат да се използват за обучение на специалисти по мрежова сигурност, както и по разработване и експлоатация на комплексни и интегрирани помежду си, информационни системи в здравеопазването.

Резултатите са публикувани в 9 статии, както следва: 2 в списание Issue on Intuitionistic Fuzzy Sets and Generalized nets (Полша), 1 в „Доклади на БАН”, 2 в тематични издания на Полската академия на науките, 2 в списания в България и 2 в сборници на научни конференции.

В 6 труда докторантката е самостоятелен автор, а останалите три имат още по 1 съавтор, което показва значителна степен на самостоятелност на получените в дисертационния труд приноси.

Постиженията в дисертацията са отразени достатъчно пълно и точно в публикуваните статии.

Представени са данни за 8 цитирания на 4 статии.

Авторефератът достатъчно пълно отразява направените в дисертацията приноси и е изготвен в съответствие с изискванията.

Мнения и препоръки: Работата е структурирана добре, но може да се подобри по отношение на стила и прецизността на терминологията и изложението. Заслужава да се отбележи Фиг. 2.6. „Обобщено мрежови модел на скала за оценяване степента на атакуваните съобщения предавани по обществената мрежа" – ОМ модел на атаките е показан, но няма достатъчно пояснения за скалата, както на фигурата, така и в пояснителния текст. Добре би било да се акцентира повече върху сравнение на получените от автора резултати със съществуващите, ако има такива.

Заключение: Въз основа на: описаните в дисертационния труд и публикациите към него, безспорни научни и научно-приложни приноси; достатъчното им разгласяване сред научната общественост и практическата им полезност, считам, че дисертацията напълно покрива изискванията на закона за придобиване на образователната и научна степен "доктор". Затова я оценявам положително и препоръчвам на уважаемите членове на Научното жури да да гласуват за присъждането на **гл. ас. Ивелина Миткова Вардева** на образователната и научна степен "**Доктор**" по научното направление **4.6 "Информатика и компютърни науки"** и съответната специалност **01.01.12 "Информатика".**

Рецензент:

/доц. д-р Стоян Порязов/

28.03.2012 г.