ФКСТ 44 - АД3 - 033
05.04.2018г.

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ ФКСТ СОФИЯ

Резюме
на научните трудове по конкурса

доц. д-р инж. Румен Трифонов

• Монографични трудове

▪ В **първият монографичен труд** е направено изследване за приложението на съществуващите интелигентни методи в мрежовата и информационна сигурност за повишаване на защитата при различни видове заплахи.

▪ **Вторият монографичен труд** е изследване на проблемите на интелигентните подходи в информационните системи при приложението им за електронното управление.

• Научни трудовете извън монографичните трудове

→ Статии в рецензирани научни списания

▪ **Научен труд [1]** – Направен е обзор и сравнителен анализ на различни методи на изкуствен интелект за борба с престъпността в киберпространството и тяхното приложение в системи за откриване и предотвратяване на проникване. Разгледано е използване на интелигентни автономни или полуавтономни агенти за откриване, оценка и реакция с подходящи действия на инциденти или киберзаплахи.

▪ **Научен труд [2]** - Разгледани са различни алгоритми за класификация с техните предимства и недостатъци (дървета на решенията, SVM и логистичната регресия) в извличането на данни (Data mining). Тези алгоритми са разделени в групи според интелигентните техники за машинно обучение като честотни таблици, ковариантни матрици и други аналитични статистически подходи. Акцентира върху случаите, в които се налага бинарна класификация.

▪ **Научен труд [3]** – Извършен е анализ различните интелигентни алгоритми или методи на базата на откриване на скрити модели в наборите от данни. Разгледани са няколко теста, базирани на статистиката, за да се провери дали разликите между методите не се дължат на случайни набори. Направен е общ преглед и анализ на техниките за измерване на ефективността (метод на изчакването, k-fold кросвалидация, bootstrap), използвайки предварително подготвени данни, за да се осигури адекватна производителност на алгоритмите за класификация на извличането на данни.

- **Научен труд [4]** - Изследвани са основните интелигентни методи за оценка на развитието на електронното правителство и неговата ефективност. Анализирано е приложението на COBRA и MUSA методологиите, които могат лесно да бъдат приложени за различни данни и че оценката на електронното правителство може да планира всеки път, когато се появят нови данни за критериите. В тази статия са предложени разработване на нови интелигентни методологии за определяне на напредъка в електронното правителство и намиране на по-подходящи и точни индекси за класиране.
- **Научен труд [5]** – Изследван е процеса на извличането на знания, който. включва подготовка на данни (за трансформиране на данните в правилния формат), изпълняване на алгоритъм за извличане на знания (който идентифицира полезната информация) и фазата на анализ (преглежда статистическата информация след завършване на алгоритъма). Предложени са критерии за избор на най-добрия алгоритъм за конкретна област на приложение чрез прилагане на различни алгоритми за класификация (дървета на решенията, генератор за правила за покриване, к-най-близък съсед, невронни мрежи) и интелигентни подходи за класификация към конкретни набори от данни в генерирания модел.
- **Научен труд [6]** – Направен е анализ на начините за интелигентен отговор на компютърните инциденти вследствие на нарастващата активност на киберпрестъпността в глобален мащаб през последните години. Разгледани са и електронните платформи за обмен на информация въз основа на жизненият цикъл за отработване на инцидента. Предложена е автоматизация на кооперирane между CERT-вете на различните страни и рамка за обмяна на информацията в киберсигурността въз основа на международно приети стандарти.
- **Научен труд [7]** – Представен е проект за разработване на интелигентен инструмент за електронно обучение по оперативна съвместимост на електронно правителство предназначен за публичната администрация. Описани са и поставените цели и определените задачи за изпълнение от проекта. Подготвеният е-курс интелигентно се разделя на модули според знанията, необходими за различните целеви групи.
- **Научен труд [8]** – Основната цел на изследването е да се проучи ефективността на разработените приложения по проекта „Електронно обучение в контекста на електронното правителство“. Описани са разработените инструменти за диагностика, които са използвани за изследването. Показани са резултатите от направения експеримент в тестова среда, като са представени данните, получени чрез анкетиране на респонденти и служители в държавната администрация и в частния сектор.
- **Научен труд [9]** – Направен е задълбочен аналитичен преглед на най-често използваните стандарти при разработването на интелигентни агенти и агент-базирани интелигентни системи. Подробно са показани резултатите от

сравнителен анализ на FIPA стандарти за изграждане на мултиагентни интелигентни системи.

- **Научен труд [10]** – В статията са очертани проблемите със сигурността и някои ключови въпроси за изграждането на правителствена рамка за сигурност на облаците, включително оценка на риска, мерки за сигурност, споразумение за ниво на обслужване, сертифициране по сигурността и докладване на инциденти. Направено е изследване на проблемите, свързани с мрежата на Националния правителствения облак и информационната сигурност. Препоръчани са възможни интелигентни подходи и решения на тези проблеми въз основа на добрите европейски и международни практики.
- **Научен труд [11]** – Направен критичен анализ на международните стандарти в областта на електронната идентификация във връзка с приетия Регламент (ЕС) № 910/2014 относно електронната идентификация при доверителни услуги за електронни транзакции на интегралния пазар. Предложени са интелигентни подходи при решаване на редица въпроси, свързани с тяхното прилагане и съответните са действия, насочени към разбирането и спазването на международните стандарти в тази област.
- **Научен труд [12]** – Разглеждат се решаването на финансовите задачи, свързани с прогнозирането, класификацията и управлението чрез изкуствена невронна мрежа. Описани са технологията и методите за прогнозиране на финансовите данни, както и е предложена система за прогнозиране на финансовите пазари чрез невронни мрежи. както и архитектурата на невронна мрежа, използваща четири различни технически показателя. Предложената система с невронна мрежа е универсална и може да се прилага към различни финансови инструменти.
- **Научен труд [13]** – Представен е критичен преглед на установените интелигентни методи за оценка на качеството на отворените данни (Open Data), подробно са анализирани разликите между тези интелигентни подходи в различни измерения и са дефинирани инструментите, подходящи за всеки подход. Предложен е многостепенен интегриран интелигентен подход за оценка качеството на данните.
- **Научен труд [14]** – Направено е проучване на прилагането на интелигентни методи за повишаване сигурността на компютърните мрежи. Показани са характерните особености на дефинирането на кибер-заплахите (Cyber Threats Intelligence (CTI)) . Направен е сравнителен анализ на методите на изкуствения интелект за това кои е удачно да се прилагат на тактическото и кои на оперативно ниво на кибур-разузнаването.
- **Научен труд [15]** – Представен е разработен концептуален модел на система за предотвратяване и откриване на проникване. Посочени са методи на изкуствения интелект, които могат да бъдат използвани в работата на моделираната система. Те са разделени на две основни групи – за традиционна и адаптивна оптимизация. Предложеният модел се състои от три

слоя и основната му цел е откриването на аномалии в поведението на системата.

- **Научен труд [16]** – Показана е система за мониторинг на мрежовия трафик, използваща методи на изкуствения интелект. Изследваната система за оценка на поведението на предполагаемия противник се състои от две основни фази: 1) фаза офлайн обучение за калибриране на системата и 2) онлайн фаза, която използва системата за разпознаване на типа поведение и ги превежда в компютърните команди. Доказва се, че най-добрите възможни резултати се постигат когато се работи с по-малък брой параметри, които описват нормалната работа на мрежата.

→ Доклади на научни конференции

- **Научен труд [17]** – Представена е разработена стратегия за прилагане на методи и инструменти на изкуствения интелект при концепциите за планиране движението и действието на мобилни роботи, като се отчита моментното им състояние, специфичната околна среда и планиране на траекторията на движение при пълна или частична загуба на мобилност. Анализирани са проблемите при валидиране на средата, проблемите при валидиране на моментното състояние на робота и подходите за изграждане на стратегии. Показана е примерна сцена на действие в 2D пространството.
- **Научен труд [18]** – Предложен е интелигентен подход за динамично йерархично управление на мобилен робот, при който отчита текущото състояние на подсистемите му и спецификата на среда, в която се движи. Направена е типизация на състоянията и поведението на шесткрак робот в зависимост от тях и е определен управляващия вектор.
- **Научен труд [19]** – Направен подробен сравнителен анализ на различни методи на изкуствения интелект с техните предимства и недостатъци, използвани при защита от киберзаплахи. Разгледани са различни типове системи за откриване и предотвратяване на проникванията IDPS и прилагането на интелигентни методи в тях.
- **Научен труд [20]** – Направен е анализ на различните интелигентни адаптивни техники за оптимизация в мрежова сигурност. В резултат от анализа се предлага взаимодействие между различни интелигентни подходи. Акцентира се на предимството на хибридния подход: алгоритмите за обучение с утвърждаване (Reinforcement Learning) и размитата, което е особено важно за сложни системи като компютърните мрежи. Предложена е мащабируема, напълно разпределена структура на система за откриване и предотвратяване на проникванията и са изследвани рисковете от откриване при ниска точност и трудностите при синхронизирането на информацията между автономните агенти.
- **Научен труд [21]** – Представени са експерименталните резултати от

разработен модел на невронна мрежа за прогнозиране на посоката на движение на финансови данни с една стъпка напред. Архитектурата на невронната мрежа използва четири различни технически показателя, които се основават на суровите данни и текущия ден от седмицата. Методът на обучение е алгоритъм с обратно разпространение на грешката. Посочени са факторите, които оказват значително влияние върху ефективността на невронната мрежа: избор на входни променливи, предварителна обработка на данните и архитектура на невронната мрежа.

- **Научен труд [22]** – Направен е обзор на интелигентите роботизирани системи - архитектура и техните основни характеристики. Направен е сравнителен анализ на методите на изкуствения интелект според задачите, които могат да се решават чрез тях. Разгледани са критериите за избор на подходящ метод за решаване на определена задача: точността на апроксимация, необходимото време за обучение, линейност на алгоритъма, брой на използваните параметри и броят на характеристиките.
- **Научен труд [23]** – Представени са методи и инструменти за краткосрочно прогнозиране на финансови операции, използващи изкуствени невронни мрежи. Направен е анализ на чувствителността на система с невронна мрежа, която се използва за краткосрочно прогнозиране на движението на цените на акциите. Разработената система е със самоопределяне на оптималната топология на невронната мрежа, поради което тя става по-гъвкава и по-точна.
- **Научен труд [24]** – Направена е типизация на интелигентно поведение на робот с шест крака за адаптиране към наклонени терени и качване/слизане по стълби. Представена е архитектура на управлението, която по информация от сензорите за оценка на външната среда и вътрешното състояние на робота избира типа на походката и целесъобразни премествания на краката.
- **Научен труд [25]** – Направен е сравнителен анализ на изграждането на VPN връзка с протоколите IPSec и SSL. Показани са резултатите от изследване за прилики и разлики на IPSec и SSL, направено по 12 ключови критерия. Представени са интелигентни подходи към основната архитектура на двата метода в контекста на мрежовата и информационна сигурност.
- **Научен труд [26]** – Представена е архитектура на шесткрак робот и теоретичен модел за провеждане на експерименти за използване на методи на изкуствения интелект при движение при частична загуба на мобилност. Разработен е интелигентен алгоритъм за избиране на подходяща походка с цел осигуряване на стабилно движение.
- **Научен труд [27]** – Представени са резултатите от изследване на симулация на система за отчитане на движение, с използване на интелигентен метод на базата на размита логика, при два вида технологии в системите за сигурност – пасивни инфрачервени детектори (PIR) и ултразвукови детектори за движение (US). Симулациите са реализирани със софтуер Mat Lab.

- **Научен труд [28]** – Представен е обобщен мрежов модел (ОММ) за изследване поведение на сътрудничество между интелигентни виртуални агенти (ИВА). ОММ е съставен от три подмрежи: за извличане на правилата на сценария и когнитивен анализ; за планиране и анализ; и за изпълнение на задачите според направения план. Експериментите от изследването показват, че когато ИВА се съобразяват с плановете си, успяват да ги реализират и предотвратяват възникването на конфликтни ситуации.
- **Научен труд [29]** – Изследвани са проблеми в роботиката като са формулирани задачите за структурна и функционална интеграция на механичните и компютърни (управляващи) системи на роботите. Представена е структурна схема за обучение, самообучение и натрупване на знания с използване на изкуствен интелект.
- **Научен труд [30]** – Представено е изследване на различните стандарти, които трябва да се спазват при изграждането на агенти базирани интелигентни системи в областта на информационната сигурност. Направен е сравнителен анализ на двата основни езика за комуникация между интелигентни агенти в мултиагентните системи - Knowledge Query and Manipulation Language (KQML) и Фондацията за интелигентни физически агенти (FIPA-ACL).
- **Научен труд [31]** – Изследвано е поведението на сътрудничеството между интелигентните виртуални агенти. За целите на експеримента е предложена програмна система със сценарий, според която интелигентните виртуални агенти с PRE-ThINK архитектура подреждат задачите на работното си място. Показана е и динамиката на вземане на решения: в проблематични ситуации. Експерименти с интелигентните агенти са обсъдени както за случая на съвместно поведение, така и за липса на комуникация.
- **Научен труд [32]** – Обобщени са резултатите от изследване за приложението на интелигентните методи от направлявано машинно обучение към проблема за класифициране на емоционалните състояния на човешките субекти въз основа на електроенцефалограма от мозъка на човека. Направен е сравнителен анализ на шест алгоритъма от машинното обучение , за да се разграничат свързаните със събитията потенциали, като се обработват различни емоционални валенции, събрани докато субектите гледат силно възбуждащи изображения с положително или отрицателно емоционално съдържание. Реализирани са експерименти с 98% постигната прецизност на класификацията, което надминава предишните публикувани резултати.
- **Научен труд [33]** – Разработена е интелигентна система за интерфейс човек-машина (MMI) с 3 оператора. Системата събира данните от операторите и произвежда изходно решение, използвайки функцията за кворум 2v3, при което се наблюдава значително намаляване на човешката грешка. Направеният динамичният анализ показва, че за определен интензитет на входното събитие, системата практически не дава грешни резултати. Тази интелигентна схема може да се прилага при системи за контрол на висок риск.

- **Научен труд [34]** – Предложено е интелигентно решение на вградена система, работеща в реално време със съответните технически и технологични параметри. Представена е разработена интелигентна система за отглеждане в реално време на култури от изключително питателни водорасли Spirulina Maxima, подходящи за директна консумация или обработени с други продукти. Описаният прототип може да се мултиплицира в мини ферма с известни допълнителни технически и програмни усилия.
- **Научен труд [35]** – Предложена е интелигентна концепция за интегрирана среда за електронен обмен на документи. Представената среда се състои от четирите слоя на класическия референтен модел на приложна архитектура. Тя е управляема среда за стандартизиран обмен на структурирани документи и е разработена в пълно съответствие със Закона за електронното управление и шестте негови регламента и е резултат на направения критичен анализ на свършената работа до момента в областта на електронното правителство.
- **Научен труд [36]** – Анализирани са специфичните проблеми на информационната сигурност в облачните компютърни приложения за електронно управление. Направен е извода, че големите концентрации на наличните ресурси и данни са по-привлекателна цел за нападателите, но защитата на информационната сигурност, базирана на облаците, може да бъде по-стабилна, мащабируема и рентабилна.
- **Научен труд [37]** – Изследвани са въпросите на информационната сигурност на приложенията за електронно управление. Предложен е нов подход за информационна сигурност в информационните системи за електронно управление. Обобщени са препоръки за действие на базата на европейския и световен опит.

05.04.2018г.
гр. София

Съставил:
доц. д-р инж. Р. Трифонов