Проект по Фонд „Научни изследвания“ № ФНИ Н 07/56

ФОНД НАУЧНИ ИЗСЛЕДВАНИЯ
МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА

Технически университет - София
Ние успяваме!

Научно-изследователски проект

„Повишаване нивото на мрежовата и информационна сигурност чрез използване на интелигентни методи“

СЕМИНАР

за представяне на резултатите от изпълнението на Етап 1 на проекта

Гранд хотел „Витоша“
(София, 02 март 2018 г.)

Основни сведения (1)

- Наименование на конкурса: **КОНКУРС ЗА ФИНАНСИРАНЕ НА ФУНДАМЕНТАЛНИ НАУЧНИ ИЗСЛЕДВАНИЯ – 2016 Г.**
- Основна научна област / тематично направление: **ТЕХНИЧЕСКИ НАУКИ / ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ**
- Допълнителни научни области: **ИЗКУСТВЕН ИНТЕЛЕКТ, МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ**
- Заглавие на проекта: **ПОВИШАВАНЕ НИВОТО НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ ЧРЕЗ ИЗПОЛЗВАНЕ НА ИНТЕЛИГЕНТНИ МЕТОДИ**
- Базова организация: **ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ**
- Партньорски организации: **НЯМА**
- Ръководител на научния колектив: **Доц. д-р Румен Трифонов**
- Сума за изпълнение на проекта: **120 000 лева**

Основни сведения (2)

Членове на научния колектив

- проф. д-р инж. Огнян Наков Наков
- проф. д-р инж. Даниела Асенова Гоцева
- проф. д-р инж. Милена Кирилова Лазарова-Мицева
- проф. д-р инж. Христо Ангелов Христов
- доц. д-р инж. Румен Иванов Трифонов
- доц. д-р инж. Пламен Иванов Вачков
- доц. д-р инж. Славчо Алекснадров Манолов
- доц. д-р инж. Радослав Даков Йошинов
- доц. д-р инж. Георги Илинчев Попов
- доц. д-р инж. Аделина Пламенова Алексиева-Петрова
- ас. инж. Галя Веселинова Павлова
- маг. инж. Георги Руменов Цочев
- инж. Момчил Мариянов Петков

Въведение (1)

Съвременната икономика и общество не само зависят, но и се развиват все по-перспективно в нови направления, свързани с интензивното използване на информационните и телекомуникационни технологии, софтуерни системи за управление, както и на ефективни процеси, базирани на дигиталните инфраструктури. Така към традиционните рискове се добавят нови, кибер-рискове с ключово значение, игнорирането на които може да доведе до катастрофални резултати.

Кибер-атаките са директна заплаха за сигурността на гражданите и функционирането на държавата, икономиката, обществото, науката и образованието. Те могат да бъдат извършени от разстояние, с прости и ефективни механизми, минимални икономически ресурси и да причинят значителни поражения с нанасяне на материални и дори човешки загуби.

Въведение (2)

Кибер-атаките нямат национални, културни или юридически граници. Рисковете и заплахите в кибер-пространството са трудни за дефиниране поради сложността за определяне на източника на въздействие, целите и мотивите, бързото ескалиране на заплахата и трудно предвидимите перспективи за развитие, сложността и интензивността на съвременните комуникационни и информационни процеси, динамиката на логическите и физическите връзки и неопределеността на процесите.

Сред най-сериозните деструктивни въздействия са тези от хибриден характер - комбинация от кибер-атака и физическа атака, кибер-атака целяща критичен кинетичен процес, кибер-атака по време на природно бедствие или неизправност в критични системи.

Кибер-престъпност (1)

За съжаление, но напълно закономерно, паралелно с позитивните явления на информационното общество се появи и бурно се разпространи в световен мащаб и техния негативен антипод – **световната кибер-престъпност.**

На световната икономика ѝ бяха необходими няколко века от утвърждаването на пазарните отношения до постигане на глобализация. За сенчестата икономика на кибер-престъпността за този преход бяха достатъчни **едно-две десетилетия.** По оценки на сериозни анализатори годишният оборот на „Интернет-базираната сенчеста икономика" вече се приближава **до търговията с наркотици.** Налице е сложен „он-лайн" черен пазар с десетки хиляди участници и без национални граници.

Кибер-престъпност (2)

Кибер-престъпност (3)

Кибер-заплахите са асиметрични, нелегални и силно наподобяват похватите на класическия тероризъм. Т.е. отделно лице или малка група някъде по света могат без особени разходи да се опитат да проникнат в системи, съдържащи жизнено важна информация или да предприемат разрушаващи атаки срещу критична инфраструктура. Инструментите и ресурсите за такива атаки са лесно достъпни чрез Интернет и уязвимостите на атакуваните системи са лесно откриваеми и използваеми.

Освен това, за разлика от класическия тероризъм, кибер-престъпниците използват за своите цели множество нищо не подозиращи потребители на компютри и Интернет. Заразените компютри на тези потребители формират т.н. „бот-мрежи”, чрез които се организират атаки към важни източници на информация или се изпращат „спам-писма” и вредни програми към многобройни адресанти, а също така се разпространява забранено съдържание.

Кибер-престъпност (4)

Първото поколение на престъпните действия в кибер-пространството се характеризира с бързото размножаване на зловреден код, който експлоатира разпространени уязвимости.

Отличителната черта на кибер-престъпленията от второ поколение е мотивът за печалба.

Две отличителни черти отбелязва третото поколение: организация и дискретност. Кибер-престъпниците стават по-зрели, като осъзнават предимствата на съвместната работа за незаконни доходи.

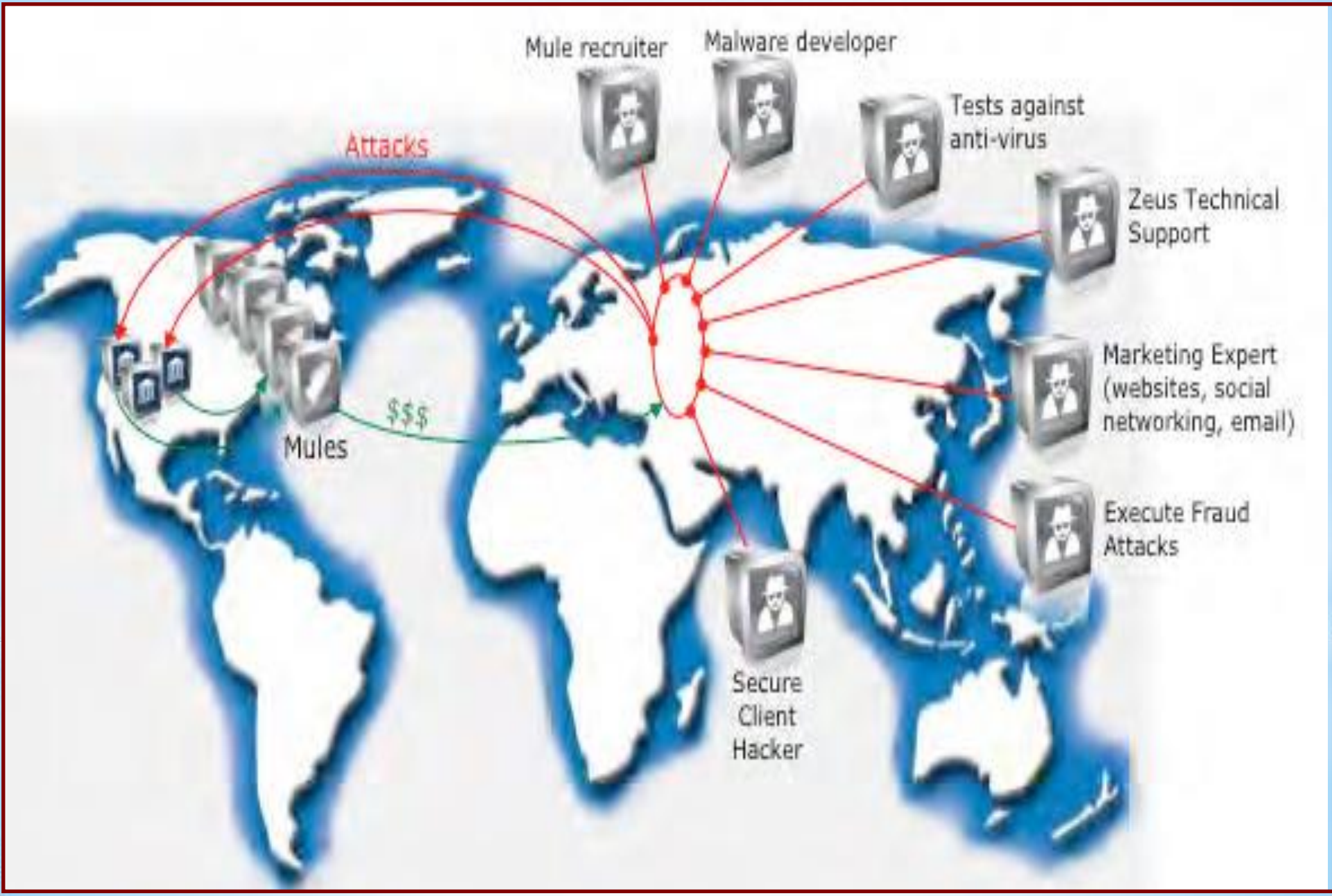
Възникването на дейност „C2C (Criminal-to-Criminal)" дава началото на четвъртото поколение на кибер-престъпността. Появява се силна и ефективна сива икономика, която предоставя възможности за киберпрестъпниците да купуват и продават стоки и услуги един на друг.

Кибер-престъпност (5)

Заплахите в настоящото **пето поколение** са **все по-автоматизирани**, което позволява на киберпрестъпниците да бъдат по-продуктивни. Те започват да се ползват от предимството на инструменти и техники за писане на скриптове за автоматизиране на различни етапи на техните схеми. По-малко опитни хакери могат да закупят инструменти за лесно идентифициране на уязвими цели, за компрометиране на системи и за кражба на данни. По-напредналите киберпрестъпници могат да купуват инструменти или да поръчват разработването на специални инструменти и скриптове като допълнение към техните продукти.

Една от особеностите на петото поколение са т.н. "**Модерни настойчиви заплахи** (**APT - Advanced Persistent Threats**)„ - целенасочени атаки срещу конкретни организации от определени, **добре координирани кибер-престъпници**. В общността на експертите, APT най-често се отнася до сложни атаки, насочени **към правителства и корпорации**, с цел да се събира разузнавателна информация или постигане на конкретни финансови цели. APT често се използва от държавни органи или техни агенти, понякога са свързани с терористични и сепаратистки политически групи.

Кибер-престъпност (6)



Цел на научно-изследователския проект (1)

Целта на проекта е да се систематизират, анализират и оценят различните видове приложения на „изкуствения интелект“ в компютърната сигурност.

Необходимо е да се отбележи, че съгласно литературните източници приложенията на изкуствения интелект се употребяват в три основни действия, свързани с компютърната сигурност:

- откриване (detection) – идентифициране на атака;
- отстраняване на последствията (repair);
- отбрана (defense) – пасивна и активна

Цел на научно-изследователския проект (2)

В настоящия проект се предвижда да се обърне основно внимание на първото действие: откриване (detection) – идентифициране на атака.

Предварителните анализи на методите на „изкуствения интелект“, използвани в системите за мрежова и информационна сигурност, показват, че повечето от тях притежават както достойнства, така и недостатъци.

Една от основните цели на проектното предложение е, след като се проведе задълбочен анализ, съпроводен от експериментално изследване на най-перспективните методи, да се направи опит за подобряване на положителните страни и избягване на недостатъците.

Проблема за идентифициране на атаките (1)

Идентифицирането на атаките е процес на откриване на проникващи събития, възникващи в процеса на експлоатация на дадена информационна система.

Наличието на системи за идентифициране на атаки е задължителен **елемент от политиките за сигурност.**

Аналогично на системите за управление на високоотговорни технологични процеси, в системите за защита на информационните системи възниква изискването за разпознаването на проникващите действия **в момента на тяхното възникване**, а не след тяхното реализиране.

Едновременно с откриването на опит за проникване е необходимо да започне функционирането на механизъм за **превантивни действия**, които са свързани с ограничаване или изолиране на действието на източник на атака и предприемане на активно противодействие с цел неговото блокиране, изолиране и привеждане в неработоспособно състояние.

Проблема за идентифициране на атаките (2)

Въпреки значимостта на посочените защитни средства и антивирусни програми, тяхната комбинация в съвременните условия на комбинирани атаки често **не е достатъчна**, за да се предотвратят атаките на съвременните версии на зловреден софтуер и опити за неправомерно проникване.

Дори и следващото поколение защитни стени не са достатъчно ефикасни, тъй като те са оптимизирани за прилагане на политики, свързани с традиционните технологии, а не за откриване и блокиране на **бързо променящи се заплахи.**

В тези условия преобладаващото количество експерти се обединяват около тезата, че традиционните методи за защита са вече слабо продуктивни и е необходим **качествен преход** към нови инструменти за реализация на мрежовата и информационна сигурност.

Методи на изкуствения интелект (1)

Едно от посочваните с приоритет направления на този преход е широкото приложение на **интелигентни методи** за анализ на обменяната информация, на потоците в мрежите, на източниците на заплахи, както и планиране на ефективни мерки за въздействие, в т.ч. проактивни (т.е. атакуващи основните източници на заплаха, такива като управляващи центрове на „бот-нет“-и пр.).

Световната практика отбелязва вече значителен брой от разнообразни **приложения на „изкуствен интелект“ в компютърната сигурност.** Без да се прави опит за изчерпателна класификация, бихме могли да разделим тези приложения в две основни направления:

Методи на изкуствения интелект (2)

- **А. Условно наречени „разпределени“ или „мрежови“ методи:**
  - **А1. Мулти-агентни системи от интелигентни агенти;**
  - **А2. Невронни мрежи;**
  - **А3. Изкуствени имунни системи и генетични алгоритми и т.н;**

- **Б. Условно наречени „компактни“ методи:**
  - **Б1. Системи за машинно самообучение (Machine Learning), в т.ч.: асоциативни методи, индуктивно логическо програмиране, Бейсова класификация и пр.**
  - **Б2. Алгоритми за разпознаване на образи;**
  - **Б3. Експертни системи;**
  - **Б4. Размита логика и пр.**

Работна програма на проекта (1)

РП1: Анализ за приложението на интелигентните методи в мрежовата и информационна сигурност.

- Дейност 1.1. Анализ на съществуващите интелигентни методи в областта на мрежовата и информационна сигурност.
- Дейност 1.2. Анализ на последните тенденции при различните видове кибер-атаки.
- Дейност 1.3. Подготовка на научни статии и участия в национални и международни научни конференции

Работна програма на проекта (2)

РП2: Моделиране и експериментално изследване на определени интелигентни методи.

- Дейност 2.1. Теоретичен модел.
- Дейност 2.2. Създаване на експериментална и изследователска постановка на теоретичния модел.
- Дейност 2.3. Изследване на работата на експерименталния модел.
- Дейност 2.4. Подготовка на научни статии и участия в национални и международни научни конференции

Работна програма на проекта (3)

РП3: Разработване и изследване на модифициран метод за повишаване нивото на мрежовата и информационна сигурност.

- Дейност 3.1. Разработване и изследване на модифициран метод.
- Дейност 3.2. Експериментално изследване на модифицирания метод.
- Дейност 3.3. Подготовка на научни статии и участия в национални и международни научни конференции

Работна програма на проекта (4)

РП4: Разпространение на резултатите.

- Дейност 4.1. Създаване на интернет страница на проекта и представяне на проекта.
- Дейност 4.2. Организиране на семинари с цел разпространяване на научните резултати от проекта.
- Дейност 4.3. Научни статии в реферирани и индексирани в световни вторични литературни източници (Web of Science и/или SCOPUS) и в издания с импакт фактор (IF)
- Дейност 4.4 Изготвяне на доклад за препоръчително използване на интелигентни методи за повишаване нивото на мрежовата и информационна сигурност.

График за изпълнението проекта

РП/ месец	01-03	04-06	07-09	09-12	13-15	16-18	19-21	22-24	25-27	27-30
РП 1										
РП 2										
РП 3										
РП 4										

Конкретни резултати (1)

Понастоящем, научния екип изпълни Етап 1 на проекта „Повишаване нивото на мрежовата и информационна сигурност чрез използване на интелигентни методи“, финансиран от фонд „Научни изследвания“ на Министерството на науката и образованието.

Приключена бе работата по РП1 «Анализ за приложението на интелигентните методи в мрежовата и информационна сигурност», в който беше направен:

- „Анализ на последните тенденции при различните видове кибер-атаки”, както и
- „Анализ на съществуващите интелигентни методи в областта на мрежовата и информационна сигурност”.

По-подробно резултатите ще бъдат представени в следващи презентации.

Конкретни резултати (2)

В първата част на проекта също се завърши и работата по РП2 «Моделиране и експериментално изследване на определени интелигентни методи».

Извърши се моделиране и експериментално изследване на избран след изчерпателен анализ определен интелигентен метод, надграждащ функционалността на системи за активно противодействие на опити за проникване при защита на мрежови сървър и хостове в мрежата.

В качество на такава система за активно противодействие бе избрана една от най-популярните в последно време – система за откриване и противодействие на проникване (IDPS – Intrusion Detection and Prevention System).

Резултатите по този пакет ще бъдат докладвани също в една от следващите презентации.

Конкретни резултати (3)

При изпълнението на проекта бе извършен анализ-сравнение по литературни източници на различни методи на изкуствения интелект от гледна точка на горепосочените критерии.

Установено бе, че методологията на аномално настроените мулти-агентни системи превъзхожда болшинството традиционни системи, базирани на изкуствения интелект при откриването на атаки, особено с неизвестен характер.

Ефективността на откриване на опасности при мулти-агентните системи също превъзхожда традиционните системи.

Конкретни резултати (4)

Най-съществените аспекти на мулти-агентно-базираните системи за IDPS са високата точност, самообучението и устойчивостта.

Без съмнение, мулти-агентно-базираните подходи могат потенциално да достигнат повишена гъвкавост, което ще ги направи още по-популярни в близко бъдеще.

Поради това, експерименталният модел, създаден на първия етап от проекта, е комбинация от мулти-агентна система и система за откриване и предотвратяване на проникване (IDPS).

Публикации по проекта (1)

❑ Статии в международни рецензирани научни списания с импакт фактор (IF)

1. Roumen Trifonov et all, A SURVEY OF ARTIFICIAL INTELLIGENCE FOR ENHANCING THE INFORMATION SECURITY, International Journal of Development Research, Vol. 07, Issue, 11, November, 2017, ISSN: 2230-9926, pp.16866-16872 (IF 4.753)

❑ Статии в рецензирани научни списания с импакт ранг (SJR)

2. Roumen Trifonov et all, AN ADEQUATE RESPONSE TO NEW CYBER SECURITY CHALLENGES THROUGH ARTIFICIAL INTELLIGENCE METHODS. Applications in Business and Economics., WSEAS TRANSACTIONS on BUSINESS and ECONOMICS, Volume 14, 2017, E-ISSN: 2224-2899 (SJR = 0.150)

❑ Статии в рецензирани научни списания

3. *Roumen Trifonov, GOVERNMENTAL CLOUD SECURITY PROBLEMS, WSEAS Transactions on Computer Research, Volume 4, 2016, E-ISSN: 2415-1521

4. *Roumen Trifonov, TRUST SERVICES FOR ELECTRONIC TRANSACTIONS, WSEAS Transactions on Computer Research, Volume 5, 2017, E-ISSN: 2415-1521

Публикации по проекта (2)

❑ Статии в рецензирани научни списания

5. Roumen Trifonov et all, CONCEPTUAL MODEL FOR CYBER INTELLIGENCE NETWORK SECURITY SYSTEM, International Journal of Computers, Volume 11, 2017, ISSN: 1998-4308

❑ Доклади на научни конференции

6. Roumen Trifonov et all, ARTIFICIAL INTELLIGENCE METHODS FOR CYBER THREATS INTELLIGENCE, 17th International Conference on APPLIED COMPUTER SCIENCE (ACS '17), Dubrovnik, Croatia September 27-29, 2017, докладът от конференцията е публикуван в списание: International Journal of Computers, Volume 2, 2017, ISSN: 2367-8895

7. R. Trifonov et all, INCREASING THE LEVEL OF NETWORK AND INFORMATION SECURITY USING ARTIFICIAL INTELLIGENCE, Fifth Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2017, 2-3 September, 2017, Zurich, Swiss, ISBN: 978-1-63248-131-3

8. R. Trifonov et all, ADAPTIVE OPTIMIZATION TECHNIQUES FOR INTELIGENT NETWORK SECURITY, 4th International Conference on Mathematics and Computers in Sciences and Industry MCSI 2017, August 24-26, 2017, Corfu Island, Greece, Conference Publishing Services of IEEE (2017), ISBN-13: 978-1-5090-0973-2

9. Р. Трифонов и др., ИНТЕЛИГЕНТНИ МЕТОДИ И КИБЕРСИГУРНОСТ, XXV conference Telecom 2017, 26-27 October, NCST, Sofia, Bulgaria, ISSN: 1314-2690

Заключение (1)

Резултатите от изпълнението на първата част - Етап 1 на проекта показват, че предложената система работи достатъчно успешно при откриване на атаките и зловредния код, които са насочени към защитаваната система, с висока степен на точност и в реално време.

Резултатите от експерименталния модел за пореден път показва перспективите на използването на методите на „изкуствения интелект“ в системите за мрежова и информационна сигурност. Потвърждават се предварителните анализи на тези методи, които показват, че повечето от тях притежават както достойнства, така и недостатъци.

Заключение (2)

Една от основните цели на изпълнявания научно-изследователски проект в следващата част – Етап 2 на проекта са:

- след като се проведе задълбочен анализ на експерименталното изследване на най-перспективните методи,
- да се направи опит за подобряване на положителните страни и избягване на недостатъците:
  - или чрез модифициране на избрания метод,
  - или чрез хибридизация на няколко избрани метода.

Благодаря за вниманието!

Въпроси?