ФОНД НАУЧНИ ИЗСЛЕДВАНИЯ
Министерство на образованието и науката

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ
75 ГОДИНИ

## Научно-изследователски проект

## „ Изследване възможностите за повишаване киберсигурността на системите в Индустрия 4.0 посредством изкуствен интелект “

# СЕМИНАР

## за представяне на резултатите от изпълнението на Етап 1 на проекта

**Технически университет – София**

**(София, 30 май 2022 г.)**

# Основни сведения (1)

- Наименование на конкурса: **КОНКУРС ЗА ФИНАНСИРАНЕ НА ФУНДАМЕНТАЛНИ НАУЧНИ ИЗСЛЕДВАНИЯ – 2020 Г.**
- Основна научна област / тематично направление: **ТЕХНИЧЕСКИ НАУКИ / ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ**
- Допълнителни научни области: **ИЗКУСТВЕН ИНТЕЛЕКТ, МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ**
- Заглавие на проекта: **Изследване възможностите за повишаване киберсигурността на системите в Индустрия 4.0 посредством изкуствен интелект**
- Базова организация: **ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ**
- Партньорски организации: **НЯМА**
- Ръководител на научния колектив: **Проф. д-р инж. Румен Трифонов – ръководител на катедра ИТИ, ФКСТ**
- Сума за изпълнение на проекта: **120 000 + 50 000 (ДМА) лева**

# Основни сведения (2)

## Членове на научния колектив

- проф. д-р инж. Огнян Наков
- проф. д-р инж.  Румен Трифонов
- проф. д-р инж. Даниела Гоцева
- проф. д-р инж. Милена Лазарова-Мицева
- проф. д-р инж. Радослав Йошинов
- проф. д-р инж. Георги Попов
- доц.  д-р инж. Славчо Манолов
- доц. д-р инж. Сергей Недев
- гл. ас. д-р инж. Галя Павлова
- гл. ас. д-р инж. Георги Цочев
- гл. ас. д-р инж. Камелия Райнова
- докт. маг. инж. Евгени Събев
- докт. маг. инж. Пламен Наков
- докт. маг. инж. Александър Христов

# Въведение (1)

В съвременното общество информационните и комуникационни технологии са проникнали дълбоко и са се превърнали в основа на всички дейности в икономиката, администрацията, обществото и личния живот. Дигиталните инфраструктури се превръщат от поддържаща среда в основен и критичен фактор за управлението и нормалното функциониране на всички ресурси и системи с национално значение, на развитието на конкурентна и иновативна икономика, прозрачно управление и на модерно демократично гражданско общество.

В общия ход на развитието на цифровото общество в последните години са проявява т.н. цифрова трансформация на индустрията – резултат от все по-масовото навлизане на Интернет на нещата (IoT), роботиката, 3D-принтирането, облачните решения и когнитивните технологии, базирани на изкуствен интелект. Всички тези технологии формират т.н. „Индустрия 4.0“, обусловена не само в проектирането и производството, но и във връзките на последното с пазара и потребителите.

Индустриалната сигурност (или кибер-сигурност) е считана като една от най-приоритетните области в модерното цифрово общество.

Кибер-атаките са директна заплаха за сигурността на държавата (т.н „критични инфраструктури“), 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. Кибер атаките с най-голям потенциал за нанасяне на значителни щети са насочените срещу различни критични инфраструктури. Уязвимостите на комуникационните и информационните системи и системите за управление на критични инфраструктури са ключов аспект от националната сигурност. Рисковете и заплахите в кибер-пространството, вкл. и в индустриалната сигурност, 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.**

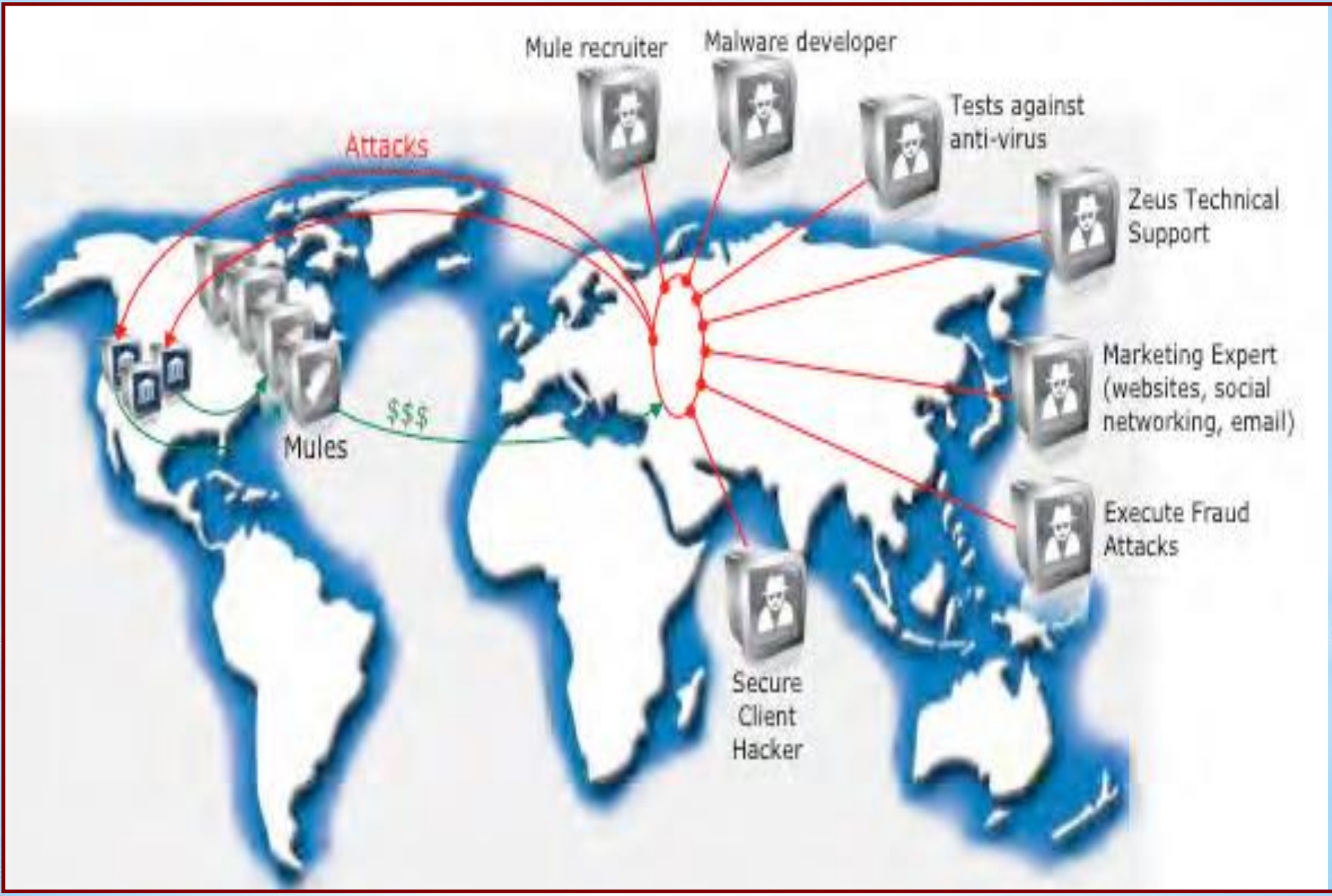
**Възникването на дейност „C2C (Criminal-to-Criminal)" дава началото на четвъртото поколение на кибер-престъпността. Появява се силна и ефективна сива икономика, която предоставя възможности за киберпрестъпниците да купуват и продават стоки и услуги един на друг.**

# 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 киберсигурността на индустриални системи, преди всичко на техните кибер-физични компоненти.

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 индустриална система.

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

В системите за управление на високоотговорни технологични процеси, в системите за защита на индустриалните 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 в индустриални системи.

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 кибер-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 индустриалните мрежи, 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 киберсигурността.** 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 възможностите за ефективно приложение на методите на изкуствения интелект в кибер-сигурността на индустриалните системи.**

- Дейност 1.1. Анализ на заплахите, насочени към индустриалните системи, в частност, към техните кибер-физични компоненти.
- Дейност 1.2. Анализ на съществуващите и използваните вече за целите на кибер-сигурността методи на изкуствения интелект от гледна точка на използването им за кибер-защита на индустриалните системи.
- 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 «базов» метод на изкуствения интелект.**

- 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 киберсигурността на индустриалните системи.**

- 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/или в издания с импакт фактор (IF)
- Дейност 4.4 Изготвяне на доклад за препоръчително използване на интелигентни методи за повишаване нивото на киберсигурността на индустриалните системи.

# График за изпълнението проекта

| РП/ месец | 01-03 | 04-06 | 07-12 | 09-12 | 13-15 | 16-21 | 21-24 | 25-27 | 28-33 | 33-36 |
|---|---|---|---|---|---|---|---|---|---|---|
| РП 1 | | | | | | | | | | |
| РП 2 | | | | | | | | | | |
| РП 3 | | | | | | | | | | |
| РП 4 | | | | | | | | | | |

# Конкретни резултати (1)

**Понастоящем, научния екип изпълни Етап 1 на проекта „Изследване възможностите за повишаване киберсигурността на системите в Индустрия 4.0 посредством изкуствен интелект“, финансиран от фонд „Научни изследвания“ на Министерството на науката и образованието.**

**Приключена бе работата по РП1 «Анализ за възможностите за ефективно приложение на методите на изкуствения интелект в киберсигурността на индустриалните системи», в който беше направен:**

- **„ИНДУСТРИЯ 4.0. ИНДУСТРИАЛНИ КОМПЮТЪРНИ СИСТЕМИ. МЕТОДИ НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ**
- **СПЕЦИФИЧНИ ОСОБЕНОСТИ НА ЗАПЛАХИТЕ СРЕЩУ ИНДУСТРИАЛНИТЕ КОМПЮТЪРНИ СИСТЕМИ В СВЕТЛИНАТА НА ПОСЛЕДНИТЕ ИЗСЛЕДВАНИЯ И КЛАСИФИКАЦИИ НА ЗАПЛАХИТЕ В КИБЕР-ПРОСТРАНСТВОТО**
- **„АНАЛИЗ НА МЕТОДИТЕ ОТ ИЗКУСТВЕНИЯ ИНТЕЛЕКТ, ИЗПОЛЗВАНИ В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА”.**
- **СЪЩЕСТВЕНИ РАЗЛИЧИЯ И ТЕНДЕНЦИИ НА СБЛИЖАВАНЕ В НОРМАТИВНАТА И СТАНДАРТИЗАЦИОННА ОСНОВА НА КИБЕРСИГУРНОСТТА ПРИ ИНФОРМАЦИОННИТЕ И ИНДУСТРИАЛНИТЕ КОМПЮТЪРНИ СИСТЕМИ**
- **ЕФЕКТИВНИ СТРУКТУРИ ЗА КИБЕРСИГУРНОСТ ПРИ ИНФОРМАЦИОННИТЕ И ИНДУСТРИАЛНИТЕ КОМПЮТЪРНИ СИСТЕМИ**

# Конкретни резултати (2)

През първия етап на проекта започна, а през втория етап на проекта ще се завърши работата по РП2 «Моделиране и експериментално изследване на «базов» метод на изкуствения интелект».

Извършено бе създаване на теоретичен модел за експериментално изследване на избран след изчерпателен анализ определен интелигентен метод, надграждащ функционалността на системи за активно противодействие на опити за проникване при защита на индустриални системи.

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

# Конкретни резултати (3)

При изпълнението на проекта бе извършен анализ-сравнение по литературни източници на различни методи на изкуствения интелект от гледна точка на определени 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 IDS са високата точност, самообучението и устойчивостта.

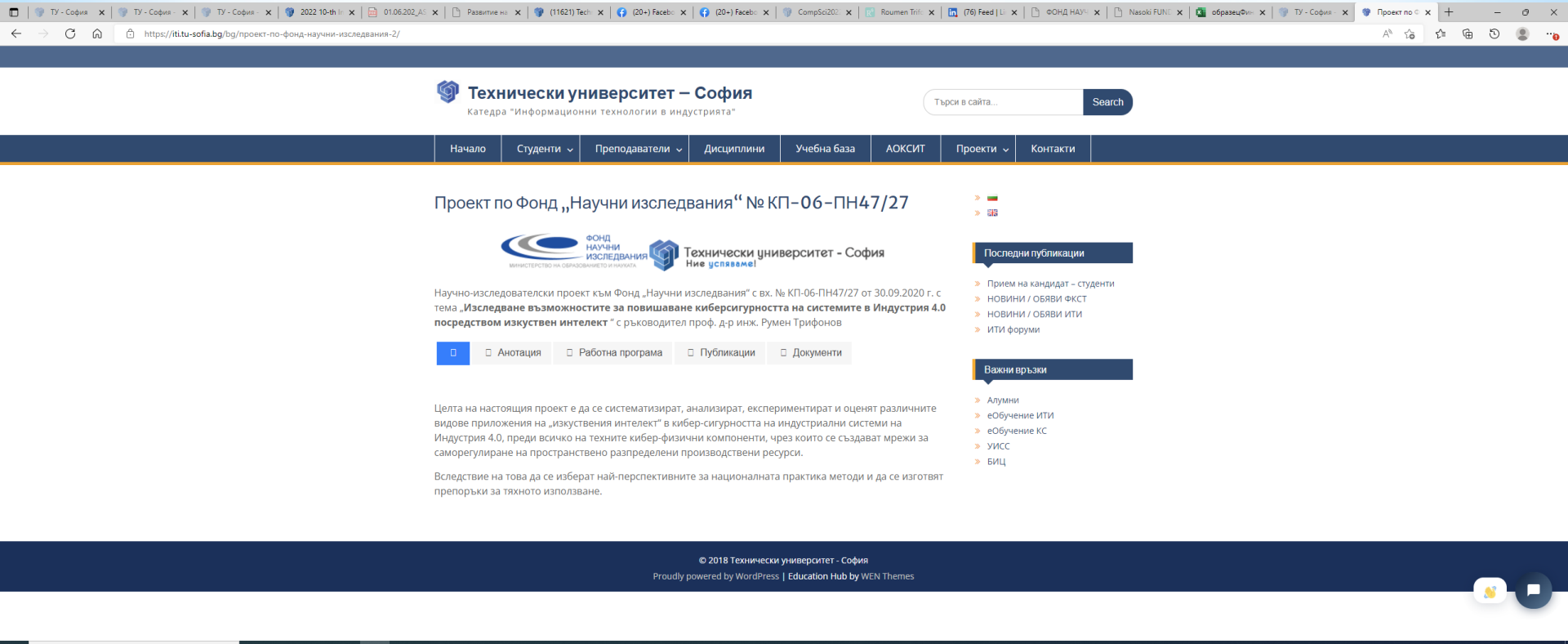
Без съмнение, мулти-агентно-базираните подходи могат потенциално да достигнат повишена гъвкавост, което ще ги направи още по-популярни в близко бъдеще.

Поради това, експерименталният модел, създаден на първия етап от проекта по РП2, е класическа система за откриване на проникване (IDS) базирана на мулти-агентна система.

# Конкретни резултати (5)

През първия етап на проекта се осъществи работата по РП4 «Разпространение на резултатите».

- Създадена бе Интернет страница за представяне на проекта и неговите реузлтати: https://iti.tu-sofia.bg



# Конкретни резултати (6)

- Организиран и проведен бе семинар с цел разпространяване на научните резултати от проекта

  - семинар за представяне на резултатите от изпълнението на Етап 1 на проекта - 30 май 2022г., Технически университет - София
  - вътрешен семинар на екипа на проекта за обсъждане на научните задачи, напредъка на тяхното изпълнение и насоки за бъдещата работа

# Конкретни резултати (7)

- **Подготовка и публикуване на научни статии в реферирани и индексирани в световни вторични литературни източници и/или в издания с импакт фактор, IF (Web of Science) и/или импакт ранг SJR (SCOPUS)**

- **Доклади на международни научни конференции в страната и чужбина – 8 броя (от които 7 бр. в IEEE/SCOPUS и 1 бр. в Open Access)**
- **Статии в международни и национални рецензирани научни списания – 1 брой**

**По-подробно публикуваните научни статии ще бъдат представени в една от следващите презентации.**

# Заключение (1)

Резултатите от изпълнението на Етап 1 на проекта показват, че предложения теоретичен модел ще осигури откриване на атаките насочени към защитаваната индустриална система, с определена степен на точност и в реално време.

Резултатите от анализа доказват перспективите на използването на методите на „изкуствения интелект“ в киберсигурността на индустриалните системите.

# Благодаря за вниманието!

Въпроси?