РЕЗЮМЕ НА НАУЧНИТЕ ТРУДОВЕ

на

гл. ас. д-р Георги Руменов Цочев

**За участие в конкурс за заемане на академична длъжност „Доцент“,
В област на висше образование: 5. Технически науки, професионално направление: 5.3. Комуникационна и компютърна техника, научна специалност: „Компютърни системи, комплекси и мрежи “, обявен в ДВ брой 94/25-11-2022 г.**

Представените за конкурса материали включват: 37 научни публикации, 1 монографично изследване и 1 учебно пособие. Тематично са разделени в следните три направления:

I. Модели, методи и средства за изграждане, мониторинг и мрежова сигурност в компютърни системи

публикации Г7.4, Г7.5, Г7.6, Г7.10, Г8.1, Г8.2, Г8.3, Г8.5, Г8.7, Г8.11, Г8.12, Г8.13, Г8.15, Г8.16, Г8.17, Г8.19, Г8.20

II. Комплекси за сигурност при изграждане и мониторинг в SCADA индустриални системи

публикации Г7.3, Г7.8, Г7.11, Г7.13, Г7.15, Г8.4, Г8.8, Г8.10, Г8.21
монографично изследване В3.1

III. Изследване на модели, методи и средства за мониторинг на сигурност и достъпност на компютърни мрежи, както и на методи и средства за обучението им.

публикации Г7.1, Г7.2, Г7.7, Г7.9, Г7.12, Г7.14, Г7.16, Г8.6, Г8.9, Г8.14, Г8.18,
учебно пособие Е24.1

В следващите точки на този документ е представено подробно описание на дейностите по посочените три направления и по показатели.

I. Модели, методи и средства за изграждане, мониторинг и мрежова сигурност в компютърни системи

В представените публикации към тази секция са анализирани проблеми и тенденции на развитие на съвременните компютърни системи. Направен е системен анализ и класификация на заплахите за бизнес информационните системи. Изследвани са различни подходи за изграждане на класификационни алгоритми и техники за изграждане на защитни модели. Разгледани са въпроси отнасящи се до оперативната съвместимост на компютърните системи, чрез използване парадигмите на изкуствения интелект и възможностите за тяхното приложение. Разгледани са класификационни алгоритми и техники за анализ и извличане на знания от данни.

Публикации, в секция I

Г8.1 I. Stankov and **G. Tsochev**, Vulnerability and Protection of Business Management Systems: Threats and Challenges, Problems of Engineering Cybernetics and Robotics, 2020, Vol. 72, pp. 29-40, p-ISSN: 0204-9848; e-ISSN: ISSN: 1314-409X

Резюме: Внедряването на една информационна система е сложен процес. Още по-сложно е, когато става въпрос за бизнес информационни системи. Тези информационни системи вече са еволюирали в това, което е по-известно като бизнес информационни системи. Тогава трябва да се има предвид и заплахата от кибератаки. В тази статия е направен кратък преглед на основните бизнес информационни системи. Въз основа на прегледа на литературата са индетифицирани най-често срещаните уязвимости, свързани с тях, и са направени някои препоръки за спиране на различни видове заплахи срещу тях.

Г8.2 G. Tsochev, R. Trifonov, O. Nakov, S. Manolov and G. Pavlova, Mobile agents in Intrusion Detection Systems: Advantages and Disadvantages. WSEAS Transactions on Information Science and Applications, 2020, Vol. 17, pp. 61-68, p-ISSN: 1790-0832, e-ISSN: 2224-3402

Резюме: Дигитализацията на информацията във всички сфери на човешката дейност и използването на технологични иновации, като основен случай за появата на всички заплахи и атаки, които са недостатъчни на съвременните технологии и непрекъснатото разширяване на сложността на сигурността и хардуера. Защитата от тези атаки и заплахите могат да се разглеждат в различни посоки в информационните и комуникационни технологии. Компютърната сигурност се определя като защита на компютърните системи срещу заплахи за поверителността, целостта и достъпността. Проникването се определя като набор от действия за компрометиране на целостта, поверителността и наличността на ресурсите. За наблюдение на събитията, които се случват в компютърни системи или мрежи, се използват системи за откриване на проникване (Intrusion detection systems - IDS). Тази статия представя базираните на мобилни агенти технологии като инструмент в IDS системите и техните предимства и недостатъци.

Г8.3 O. Iliev, R. Yoshinov and **G. Tsochev**, Verification of user identity and datasecurity in the context of LMS and LCMS, Mathematics and Education in MATHEMATICS, Proceedings of the Forty-ninth Spring Conferenceof the Union of Bulgarian Mathematicians, 2020, pp. 144-151, p-ISSN: 1313-3330

Резюме: Съвременното образование предлага разнообразни методи и инструменти за онлайн обучение. В наши дни системите за управление на обучението са инструмент, който улеснява съвременното обучение. Ето защо сигурността на тези системи по отношение на удостоверяване и проверка на потребителите е важен елемент. Това повдига въпроса за осигуряване на сигурност на данните на изключително високо ниво и също така задължава системата да осигури начин за проверка на самоличността на потребителите. Статията представя възможности за постигане на тези изисквания чрез комбинация от криптографски алгоритми, използване на гъвкава софтуерна архитектура и модел за идентификация на потребителя.

Г7.4 G. Tsochev, R. Trifonov, S. Manolov and G. Pavlova, Investigation Of Secure Mobile Agents As A Tool In Intrusion Detection Systems, 2020 International Conference on Mathematics and Computers in Science and Engineering (MACISE), 2020, pp. 114-118, ISBN: 978-1-7281-6696-4, doi: 10.1109/MACISE49704.2020.00026 **(Scopus)**

Резюме: Целта на тази статия е да представи използването на мобилни агенти като инструмент за нови видове решения за информационна сигурност. Идеята е да се предложат гъвкави и ефективни решения на проблем, който е труден за справяне с конвенционалните подходи. Мобилните агенти могат да се използват за откриване на проникване за разработване на нови проекти, които са по-ефективни, мащабируеми и стабилни. Въпреки че не е идеално решение, технологията за мобилен агент се движи към идеалното поведение, желано от IDS. Не само аспектите на установяване на полезността на задачите, но и, може би по-важно, отговорът на задачите е значително подобрен. Тъй като IDS в момента не включва технология за мобилни агенти, ние не очакваме масов преход към тази парадигма. Технологията обаче се поддава на постепенно приемане и използване. Поради отбелязаните предимства, особено по отношение на реакцията на проникване, технологията на мобилния агент има потенциала да придобие първоначална опора и да разшири своя обхват с течение на времето.

Г7.5 G. Tsochev and I. Stankov, A Study On Information Security Management, 2020 XXIX International Scientific Conference Electronics (ET), 2020, pp. 1-4, ISBN: 978-1-7281-7427-3 doi: 10.1109/ET50336.2020.9238331 **(Scopus)**

Резюме: Киберсигурността е единствената защита в една от най-дългите войни, които светът някога е познавал. Ежедневно се водят битки срещу национални държави, организирана престъпност, крадци, терористи и отегчени, но умни деца. Тази война ескалира всеки ден, докато бойното поле расте. Основният фокус на ИТ екипа е да осигури ефективна и бърза обработка на информацията, докато основната цел на екипа по информационна сигурност е да гарантира поверителността, целостта и достъпността на информацията. Статията представя преглед на управлението на информационната сигурност и основните принципи в тази област от гледна точка на компютърните системи.

Г8.5 G. Tsochev, Developing Monte Carlo Simulator of Reinforcement Learning Type, Problems of Engineering Cybernetics and Robotics, 2020, Vol. 73, pp. 39-46, p-ISSN: 0204-9848, e-ISSN: 1314-409X, https://doi.org/10.7546/PECR.7

Резюме: Методите на Монте Карло са начин за решаване на проблема с подсилване на обучението въз основа на средни резултати от теста. За да се гарантира, че са налични добре дефинирани резултати, методите на Монте Карло се използват само за епизодични задачи. Терминът Монте Карло често се използва по-широко във всеки метод за оценка, чиято работа включва значително участие на случаен принцип. Тук се използва специално за методи, базирани на средната стойност на пълните резултати (за разлика от методите, които се научават от непълни резултати). Документът описва симулатор за оценка на дъждовните капки в определена област с помощта на пакета matlib.

Г7.6 R. Trifonov, O. Nakov, G. Pavlova, S. Manolov, **G. Tsochev** and P. Nakov, Analysis of the Principles and Criteria for Secure Software Development, 2020 28th National Conference with International Participation TELECOM, 2020, pp. 125-128, ISBN: 978-1-7281-8718-1, doi: 10.1109/TELECOM50385.2020.9299567 **(Scopus)**

Резюме: Софтуерните приложения обикновено се разработват с помощта на езици за програмиране на високо ниво, които сами по себе си могат да имат уязвимости в сигурността и също така работят в мрежова среда. Формулирани са набор от критерии за разработване на защитени софтуерни приложения, за да се гарантира наличността, поверителността и целостта на информационните системи. Познаването на международните стандарти за разработка на защитен софтуер и най-добрите практики в тази област, както и спазването на изискванията за сигурност може да доведе до пълноценно противодействие на многобройните заплахи за софтуерната сигурност в организациите.

Г8.7 G. Tsochev, R. Trifonov, O. Nakov, S. Manolov and G. Pavlova, Some recommendations for the implementation of GDPR at the University, 9th International Scientific Conference COMPUTER SCIENCE'2020, Velingrad, Bulgaria, 2020, ISBN: 978-619-167-433-6

Резюме: След май 2018 г. много неща се променят с влизането в сила на регламента за защита на данните (GDPR). GDPR заменя предишната инициатива за данни, която ЕС имаше, Директива за защита на данните 95/46/ЕС. GDPR беше приет главно с цел хармонизиране на законите за поверителност на данните в Европа и гарантиране на поверителността на данните за всички европейски граждани. Тази статия предоставя някои препоръки за прилагане на GDPR в университетите.

Г7.10 R. Trifonov, O. Nakov, S. Manolov, **G. Tsochev** and G. Pavlova, New Approaches to the Investigations and Classification of Cyber Threats Challenged by the Application of Artificial Intelligence Methods, Proceedings of the Information Systems and Grid Technologies – ISGT 2020, Sofia, Bulgaria, 2020, pp. 148-158, ISSN: 1613-0073, http://ceur-ws.org/Vol-2656/paper8.pdf **(Scopus) (SJR = 0.228)**

Резюме: Разследванията на киберзаплахите в глобален мащаб през последните години придобиха ново измерение, свързано с безпрецедентния растеж на киберпрестъпленията, кибертероризма и кибервойните, както и въвеждането на методи на изкуствения интелект в областта на киберзащитата. Изследванията и практиката на това внедряване показват, че няма достатъчно универсален метод, който да е достатъчно ефективен за защита срещу различни видове кибератаки. Оказва се, че изборът на методи за изкуствен интелект, които са най-подходящи за противодействие на определени класове заплахи, зависи от систематизацията, унификацията и класификацията на заплахите за киберсигурността и източниците на тези заплахи. Тази статия разглежда новите подходи за идентифициране и анализ на киберзаплахите, както и инструментите, използвани от различните така наречени „агенти за заплахи“. Тези анализи и класификационни схеми могат да служат за създаване на критерии за избор на подходящи методи за изкуствен интелект за противодействие на конкретни класове кибернетични заплахи.

Г8.11 R. Trifonov, S. Manolov, **G. Tsochev** and G. Pavlova, Examination of the cyber threats focused on choise of adequate cyber intelligence methods, Journal Communication & Cognition, 2019, Vol. 52, Issue 1-2, pp. 45-58, ISSN: 0378-0880

Резюме: За да се отговори адекватно на новите предизвикателства на кибер заплахите, експертната общност съветва да се използват методи на изкуствения интелект за противодействие на кибератаките. Изборът на методи за изкуствен интелект, които са най-подходящи за противодействие на определени класове заплахи, зависи от систематизацията, унификацията и класификацията на заплахите за киберсигурността и източниците на тези заплахи. Мотивацията на изследването се основава на убеждението, че новите подходи за идентифициране и анализ на заплахите ще бъдат полезни при избора на подходящ метод на приложение за противодействие. Изследванията на този етап са завършени и резултатите от тях са послужили като основа за избор на методи за изкуствен интелект за различни случаи на киберзащита.

Г8.12 R. Trifonov, S. Manolov, R. Yoshinov, **G. Tsochev**, G. Popov and G. Pavlova, New Approaches in the Examination of Cyber Threats, Proceedings of the International Conference on Information Technologies (InfoTech-2018), 20-21 September, Bulgaria, 2018, pp. 49-56, p-ISSN: 1314-1023

Резюме: Настоящата статия описва някои от резултатите, свързани с прилагането на интелигентни методи за повишаване на сигурността в компютърните системи. За да се изгради рационален и последователен подход при избора на методи за изкуствен интелект, най-подходящи за противодействие на определени класове заплахи, е необходимо да се постигне систематизиране, унифициране и класификация на заплахите за киберсигурността и източниците на тези заплахи. Това може да се реализира с помощта на новите концепции и класификации в областта на изследването на кибер заплахите.

Г8.13 R. Trifonov, S. Manolov, **G. Tsochev** and G. Pavlova, Artificial intelligence methods suitable for operational cyber-threat intelligence, Journal Communication & Cognition, 2018, Vol. 51, Issue 3-4, pp. 57-72, p-ISSN: 0378-0880

Резюме: Според мнението на водещи експерти в областта на киберсигурността през последните няколко години се наблюдава преход от етапа на киберпрестъпността към етапа на кибервойната. За да отговори адекватно на новите предизвикателства, експертната общност има два основни подхода: възприемане на философията и методите на военното разузнаване и използване на методите на изкуствения интелект за противодействие на кибератаките. Настоящата статия описва някои от резултатите при внедряването на интелигентни методи за повишаване на сигурността в компютърните системи.

Г8.15 R. Trifonov, O. Nakov, P. Vachkov, S. Manolov, R. Yoshinov, G. Popov, **G. Tsochev** and G. Pavlova, Intelligent Methods and Cybersecurity, TELECOM, 2017, Vol. 1, pp. 113-120, p-ISSN: 1314-2690

Резюме: В условията на пето поколение киберпрестъпност, характеризиращо се с автоматизация на разработването и разпространението на инструментите за атака, както и интеграция в рамките на няколко комплекта инструменти, преобладаващият брой експерти считат, че традиционните методи за защита са вече слабо продуктивни и е

необходим качествен преход към нови инструменти за реализация на мрежовата и информационна сигурност. Едно от посочваните с приоритет направления на този преход е широкото приложение на интелигентни методи за анализ на обменяната на информация, на потоците в мрежите, на източниците на заплахи, както и планиране на ефективни мерки за въздействие, в т.ч. проактивни. Настоящият доклад е посветен на приложението и експериментирането на един конкретен метод на изкуствения интелект за защита на компютърните системи.

Г8.16 R. Trifonov, **G. Tsochev**, S. Manolov, R. Yoshinov and G. Pavlova, Increasing the level of network and information security using artificial intelligence, Fifth Intl. Conf. Advances in Computing, Communication and Information Technology-CCIT 2017, 2017, pp. 83-88, e-ISBN: 978-1-63248-131-3, DOI:10.15224/978-1-63248-131-3-25

Резюме: В статията са отчетени различни адаптивни техники за оптимизация за интелигентна сигурност при компютърните системи. В резултат на направени анализи се предлага съвместяване между различни подходи в системите за откриване на нарушители. Разгледан е пример на комбинацията от мрежово и хост базирани мулти-агентни системи за откриване на нарушители IDPS (NIDPS, HIDPS) в разпределена хетерогенна среда. Демонстрирано е влиянието на тази система върху повишаването на ефективността за откриване на пробиви и нарушители и намаляването на процента на фалшиви аларми.

Г8.17 R. Trifonov, **G. Tsochev**, S. Manolov, R. Yoshinov and G. Pavlova, A Survey of Artificial Intelligence for Enhancing the Information Security, International Journal of Development Research, 2017, Vol. 07, Issue 11, pp. 16866-16872, ISSN:2230-9926, ISI IF: 4.753

Резюме: Анализът на най-новите тенденции в заплахите за различни видове атаки адекватно отразява радикалните промени през последните три-четири години в ландшафта на защитата от киберзаплахи. Конвенционалните инструменти за мрежова защита, като откриване на проникване и антивирус, фокусиран върху компонента за уязвимост на риска и традиционната методология за реакция при инциденти, са станали неадекватни за определени играчи поради еволюцията на целите и сложността на навлизането на компютърните мрежи. Следователно борбата срещу тях може да се осъществи с интелигентни полуавтономни или напълно автономни агенти, които могат да откриват, оценяват и реагират с подходящо защитно действие. Тези интелигентни методи ще трябва да могат да управляват целия процес в отговор на атака. Тя се основава на изкуствения интелект и използването на неговите методи за защита от киберпрестъпления. Целта на това изследване е да представи и сравни различни методи на изкуствен интелект за борба с престъпността в киберпространството или по-скоро приложението им в системи за откриване и предотвратяване на проникванията.

Г8.19 T. Petrova, I. Naydenova, L. Pironkov, A. Filipov, **G. Tsochev** and I. Ganev, Integrating of A National E-Learning Platform Clp4net, Proceedings of the Technical University of Sofia, 2016, Vol. 66, Issue 3, pp. 241-248, ISSN: 1311-0829

Резюме: Настоящата работа представя извършените етапи в процеса на изграждане на първия в страната национален портал за електронно обучение в областта на ядрената енергетика чрез внедряването на платформата CLP4NET. Тя е Moodle-базирана и е разработена и поддържана от Международната агенция за атомна енергия.

Представена е основната и функционалност по отношение на управлението и изпълнението на процесите на обучение в даденото направление.

Г8.20 I. Naydenova, L. Pironkov, A. Filipov, T. Petrova, **G. Tsochev** and I. Ganev, Implementation of CLP4NET in Bulgaria, Third International Conference Nuclear Knowledge Management - Challenges and approaches, IAEA, 7-11 November, Vienna, Austria, 2016, pp. 103, ISBN: 978–92–0–108818–5, ISSN: 0074–1884

Резюме: Мрежовите решения (мрежи за върхови постижения, общности на практики, портали за знания и др.) са признати за ефективни инструменти за ядрено обучение и образователни услуги, трансфер на добри практики, знания и програми и управление на знания. В допълнение, електронното обучение се препоръчва като най-съвременен и икономически ефективен подход за допълване на традиционните програми за обучение и обучение лице в лице. Така в системата за обучение на АЕЦ "Козлодуй" (АЕЦ "Козлодуй") беше внедрена Cyber Learning Platform for Nuclear Education and Training (CLP4NET). Въз основа на опита на АЕЦ "Козлодуй", CLP4NET беше внедрена и в Колежа по енергетика и електроника (КЕЕ), Технически университет в София (ТУ-София), предоставяйки подходящ инструмент за по-нататъшно създаване на Национална мрежа за ядрена компетентност. Настоящото изследване е фокусирано основно върху специфични проблеми и уроци, извлечени по време на инсталирането на CLP4NET в КЕЕ, ТУ-София.

Г8.21 Г. Цочев, Състезания на сигнали като метод за атака и подходи за избягването им, списание Computer & Communications Engineering, 2016, Vol. 10, Issue 1, pp. 67-73, ISSN: 1314-229

Резюме: Състезанията на сигнали може да се определят като аномално поведение, причинено от неочакваната зависимост от относителното време на събитията. С други думи един програмист или администратор неправилно приема, че дадено събитие винаги ще се случи преди друго. Статията разглежда състезанията на сигнали като методи за атака. Разгледани са процесите в апаратната част и Unix базирани системи. Представени са примери за получаване на състезания. Описани са някой основни техники за избягването им.

II. Комплекси за сигурност при изграждане и мониторинг на SCADA индустриални системи

В представените публикации към тази секция са анализирани проблеми и тенденции на развитие на индустриалните системи и тяхната сигурност. Направен е системен анализ и класификация на заплахите за индустриалните системи. Изследването е специфицирано за системи от тип за цялостен контрол и управление на автоматизираните процеси (Supervisory Control And Data Acquisition - SCADA). Изследвана е съвместимостта между традиционните информационни системи и тези за управление на промишлени процеси, чрез прилагане на различни методи на изкуствения интелект. Разгледани са възможностите за тяхното приложение в конкретни области на сигурността. Предложени са алгоритми и техники за анализ и извличане на знания от данни, за повишаване на нивото на сигурността.

Публикации, в секция II

Г7.3 G. Tsochev and M. Sharabov, Artificial intelligence methods used in industry 4.0 in particular industrial control systems, AIP Conference Proceedings, 2021, Vol. 2333, pp.07001-07007, ISBN: 978-0-7354-4077-7, https://doi.org/10.1063/5.0041610, **(Scopus) (SJR = 0.262)**

Резюме: Изкуственият интелект (AI) е много обещаващо поле за развитие в много посоки. Той е широко разпространен в компютърните технологии (биотехнологии, нанотехнологии, интернет на нещата и др.), както и в роботиката, 3D принтирането, квантовите изчисления и много други. Използването му за предсказване и защита от кибератаки е друго от многото му приложения. В изпълнение на проект за изследване на сигурността на киберфизическите връзки в контекста на компютърни мрежи от следващо поколение е направен преглед на методите на ИИ и тяхното приложение в Индустрия 4.0. Обърнато е повече внимание на приложението на AI като средство за защита на технологии като SCADA, индустриален интернет на нещата и като цяло кибер-физически връзки. Целта на това изследване е да представи и сравни различни методи на AI за борба с кибератаки, или по-скоро приложението им в системи за откриване и предотвратяване на проникванията в областта на споменатата технология.

Г7.8 G. Tsochev, R. Yoshinov and N. Zhukova, Some Security Issues with the Industrial Internet of Things and Comparison to SCADA Systems, SPIIRAS Proceedings, 2020, Vol. 19, Issue 2, pp. 358-382, ISSN: 2078-9181, e-ISSN: 2078-9599 https://doi.org/10.15622/sp.2020.19.2.5 **(Scopus) (Q3, SJR = 0.242)**

Резюме: Разглежда се въпрос за сигурността на Интернет на нещата, който не принадлежи към традиционния проблем на киберсигурността, тъй като е локален или разпределен мониторинг и/или мониторинг на състоянието на физически системи, свързани чрез Интернет. Архитектурата на системата за надзорен контрол и събиране на данни (SCADA) беше разгледана в предишни проучвания на авторите. Поради внедряването на SCADA системите бяха анализирани уязвимостите и различните варианти на кибератаки към тях. Като пример беше разгледан казус, базиран на дървета, като получените резултати бяха обобщени и визуализирани. Целта на статията е да се сравни новата индустриална технология на Интернет на нещата (Industrial Internet of Things) с предишните проучени традиционни SCADA системи. Индустриалният интернет на нещата е мрежа от устройства, които са свързани чрез комуникационни технологии. Някои от най-често срещаните проблеми със сигурността за индустриалния интернет на нещата са представени в този документ. Представен е кратък преглед на структурата на индустриалния интернет на нещата, описани са основните принципи на сигурността и основните проблеми, които могат да възникнат с устройствата на интернет на нещата. Въз основа на изследване и анализ на риска от заплахи в областта на индустриалния интернет на нещата, като основен подход се разглежда конкретен случай на разрушително въздействие, базиран на дървовиден анализ. Предоставено е описание на създаването на стойност на листовия възел на дърво за атака и анализ на резултатите. Извършва се анализ на сценария за промяна на електронния запис за увеличаване на скоростта на инфузия на преливна помпа с помощта на индекс на сложност. Анализират се последствията в сравнение с предишно проучване на SCADA системи и се прави съответното заключение.

Г8.4 G. Tsochev and R. Trifonov, Some Key Strategies and Best Practice in Cloud Computing Security, Journal Computer and communications engineering, 2020, Vol. 14, Issue 2, pp. 3-8, p-ISSN: 1314-2291

Резюме: Cloud Security се стреми да предотвратява, открива и реагира на уязвимости и заплахи. Проверките за сигурност осигуряват превенция, но не можем да разчитаме само на нея. Използват се различни методи за повишаване на сигурността, което е свързано с идентифициране на заплахи и а възможни решения за осигуряване на информационна сигурност на данните и приложенията на потребителите в облачната среда, насочване на усилията за преодоляването им в конкретни области. Въвеждането на ефективен мониторинг на сигурността е ключова стратегия за сигурността в облака. В тази статия ще обсъдим някои ключови стратегии и добри практики в облачната сигурност.

Г8.6 R. Trifonov, O. Nakov, S. Manolov, **G. Tsochev** and G. Pavlova, A new approach to cyber security policy development using artificial intelligence methods, 9th International Scientific Conference COMPUTER SCIENCE'2020, Velingrad, Bulgaria, 2020, ISBN: 978-619-167-433-6

Резюме: Създаването на политики за киберсигурност е стохастичен процес, който не може недвусмислено да гарантира обективността на получените резултати. Това е съществено обстоятелство, предвид икономическата съставка на разработваните политики. Мерките за повишаване нивото на сигурност са свързани със сериозни разходи и обикновено ръководството на организацията е изправено пред труден избор. Следователно, обикновено създаването на политика е итеративен процес, включващ последователни цикли от следните стъпки: оценка на риска, предвиждане на мерки за намаляването му, оценка на тези мерки, оценка на ръководството за осъществимостта и уместността на бъдещите разходи.

Г7.11 G. Tsochev, Strengthen the Security of SCADA Systems Through Polling, 2020 28th National Conference with International Participation TELECOM, 2020, pp. 133-136, ISBN: 978-1-7281-8718-1, doi:10.1109/TELECOM50385.2020.9299571. **(Scopus)**

Резюме: Критичната информационна инфраструктура е система от съоръжения, услуги, правила и начини за обработка на информация, чието спиране или нарушаване на функционалността може да доведе до сериозно негативно въздействие. В допълнение към тази концепция се появява нова област във военното и икономическото пространство – Домейна на киберпространството. Сигурността на SCADA системите е от особено значение в стратегически важни за икономиката промишлени и инфраструктурни обекти. Статията представя теоретичен модел за защита на устройства, работещи в SCADA системи, които могат директно да комуникират и взаимодействат с различни полеви устройства като сензори, клапани, помпи, двигатели, задвижвания и др., чрез интерфейс човек-машина.

Г8.8 M. Sharabov and **G. Tsochev**, The use of artificial intelligence in Industry 4.0, Problems of Engineering Cybernetics and Robotics, 2020, Vol. 72, pp. 17–29, p-ISSN: 0204-9848, e-ISSN: 1314-409X, https://doi.org/10.7546/PECR.73.20.02

Резюме: Тази статия представя кратък преглед на ефекта от новите технологии, как те променят производствения процес и как машините започват да стават много по-

умни благодарение на изкуствения интелект. Фокусът е върху изследването на Индустрия 4.0 и как тя революционизира целия производствен сегмент и какво обещание за по-добро, по-ефективно бъдеще носи. Този анализ се фокусира основно върху това как е интегриран изкуственият интелект, какви ползи носи и колко голямо е подобрението спрямо основното програмиране. Част от изследването се основава на 771 публикации, проследени през последните три до пет години. Публикациите са в някои от добре познатите бази данни Scopus, Web of Science и IEEE. Ще разгледаме основните сценарии за използване, при които AI е изключително необходим и как едно ново поколение на индустриална фабрика може да изглежда и да се чувства като живо човешко същество.

Г8.10 Г. Павлова, Р. Трифонов и **Г. Цочев**, Проблеми на колоборативната работа на хора и роботи, списание Автоматика и информатика, 2019, бр. 3, стр. 17-23, p-ISSN: 0861-7562, e-ISSN: 2683-1279

Резюме: Роботите са огромна част от всички човешки дейности. В индустрията е доказано, че съвместната работа на хора и роботи е по-ефективна от производствените технологии без хора. Това от своя страна създаде нов набор от проблеми, както по отношение на производителността, така и в безопасното сътрудничество, особено за хората. Настоящата работа има за цел да реши най-съществените проблеми за осигуряване на безконфликтна работа при гарантиране на висока производителност и качество на изпълняваните функционални задачи.

Г7.13 G. Tsochev, Some Security Problems and Aspects of the Industrial Internet of Things, 2020 International Conference on Information Technologies (InfoTech), 2020, pp. 1-5, e-ISBN: 978-1-7281-6914-9, doi: 10.1109/InfoTech49733.2020.9211078 **(Scopus)**

Резюме: Светът навлиза в новата ера на индустриалните системи. Безкрайното развитие на технологиите несъмнено е подобрило ефективността на промишлените процеси. Интернет на нещата е от съществено значение за нас в наши дни. Реалният и виртуалният свят вече започват да се сливат в производството, поставяйки началото на Индустрия 4.0 или четвъртата индустриална революция. В тази статия ще обсъдим начините, по които индустриалните компании трябва да подходят към предизвикателствата пред сигурността, присъщи на пазара на индустриалния интернет на нещата, както и някои препоръки към тях.

Г7.15 G. Tsochev, R. Yoshinov and O. Iliev, Key Problems of the Critical Information Infrastructure through Scada Systems Research, SPIIRAS Proceedings, 2019, Vol. 18, Issue 6, pp. 1333-1356, ISSN: 2078-9181, e-ISSN: 2078-9599, https://doi.org/10.15622/sp.2019.18.6.1333-1356 **(Scopus) (Q3, SJR = 0.226)**

Резюме: В днешния век киберсигурността е основен елемент на всяка информационна система. Ключов аспект е в критичната информационна инфраструктура, където информационната сигурност се превърна в основен приоритет за експертите по информационна и мрежова сигурност. Оперативната съвместимост на ИКТ инфраструктура с други нейни компоненти е важен аспект от нейния жизнен цикъл. Тъй като системите за надзорен контрол и събиране на данни (SCADA) са част от критичната инфраструктура, тяхната киберзащита е особено важна в стратегически важни промишлени и инфраструктурни обекти – електроцентрали, рафинерии, нефтопроводи, пречиствателни станции, производствени съоръжения, комуникационни и транспортни инфраструктури. Заедно с напредъка на технологиите, нарастващия брой

Scada устройства, достъпни онлайн, уязвимостта на контролираните от тях сектори също се увеличи. В света на интернет на нещата (всичко), крайните устройства предизвикват нова вълна от възможни уязвимости в SCADA. Те се превръщат в нови места за атаки и пробиви, чрез които системата може да бъде достъпна или дори компрометирана. В Общността има редица критични инфраструктури, чието прекъсване или разрушаване би имало значителни трансгранични последици за повече от един сектор в резултат на взаимозависимостта на взаимосвързаните инфраструктури. Такива европейски критични инфраструктури са създадени и стартирани съгласно обща процедура, разработена от Европейската комисия, като изискванията за сигурност се оценяват съгласно общ минимален подход. Настоящата статия разкрива и разглежда критичните инфраструктури на Европейския съюз и България. Чрез представяне на структурата на Scada система бяха анализирани уязвимостите и различните възможности за атака. Като пример е разгледан конкретен случай, базиран на дървета, като получените резултати са обобщени и визуализирани. Последствията са анализирани и е направено съответното заключение.

Монографични изследвания в секция II

В3.1 **Г. Цочев** и Р. Йошинов, Изследване сигурността на киберфизичните системи, Издателство „Образование и познание“, 2020, 258 с., ISBN: 978-619-7515-21-3, e-ISBN: 978-619-7515-22-0

Резюме: Информацията винаги е била и остава най-търсената и скъпа стока, което особено засяга съвременното информационно общество. С динамичното развитие на информационните технологии, въпросите за компютърната и информационната сигурност стават все по-сериозни и многобройни атаките върху киберфизичните компютърни системи и се отличават с все по-нови и развити техники. Използването на информационни и комуникационни технологии в човешката дейност, чрез разнообразни по вид компютърни устройства, създава предпоставки за осъществяване на събития и действия, които представляват заплахи за информационната сигурност – чрез манипулиране на данни е информация, изкривяване на тяхната достоверност, нарушаване на тяхната конфиденциалност, ограничаване на достъпността им или отнемане на други значими техни качества. Типичен пример за заплаха за информационната сигурност са компютърните вируси, които са в състояние да унищожат информация, събирана с години в една киберфизична компютърна система. На национално, европейско и световно ниво продължават да се провеждат редица форуми, имащи за цел да анализират световните тенденции в кибератаките, както и да бъдат направени редица стъпки за подобряване на информационната сигурност в киберфизичните системи.

Основната цел на настоящото изследване е да се представи същността на информационната сигурност, основните видове заплахи, както и общата концептуална рамка и подходи за осигуряване на надеждна защита на киберфизичните системи (КФС), от гледна точка на тяхното приложение в индустриалните системи за управление.

III. Изследване на модели, методи и средства за мониторинг на сигурност и достъпност на компютърни мрежи, както и на методи и средства за обучението им

В представените публикации към тази секция са анализирани проблеми и тенденции от гледна точка на сигурността при развитието на компютърните мрежи. Направен е системен анализ и класификация на заплахите за мрежова и информационна сигурност. Изследвани са различни подходи в областта на осигуряване на мрежовата

сигурност чрез използване на парадигмите на изкуствения интелект. Изследвани са възможностите за тяхното приложение в определени проблемни области на тази секция. Резултатите от изследванията подпомагат развитието на методиката на обучение по компютърни мрежи в присъствена и дистанционна форма. Предложени са средства за осъществяване на обучение в дистанционна форма.

Публикации, в секция III

Г7.1 G. Tsochev, Research on Web Applications for Remote Laboratory Exercises on Computer Networks, 2021 International Conference on Information Technologies (InfoTech), 2021, pp. 1-4, ISBN: 978-1-6654-3134-7, e-ISBN:978-1-6654-0324-5, doi:10.1109/InfoTech52438.2021.9548329 **(Scopus)**

Резюме: Методологията на симулацията става все по-популярна сред изследователите на компютърни мрежи по света по време на пандемия от COVID. За да изберете подходящ мрежов симулатор за конкретно приложение, е важно да имате познания за наличните инструменти за симулатор, заедно с техните предимства и недостатъци. Разясняват се основните начини за монтажа им. Направено е предложение за добра практика в онлайн симулатори за провеждане на лабораторни упражнения по компютърни мрежи.

Г7.2 G. Tsochev, Some problems in Engineering Education with Computer Science Profile During COVID-19, Mathematics and Informatics, 2021, Vol. 64, Issue 3, pp. 255-263, ISSN: 1310–2230, e-ISSN: 1314–8532 **(WoS) (JCI = 014)**

Резюме: Пандемията от COVID-19 въведе много ограничения и промени в живота ни и по-специално в образованието. Тази статия представя проблемите на дистанционното обучение в областта на компютърните мрежи и информационната сигурност в периода март – юни 2020 г. при обучението на инженери с профил компютърни науки.

Г7.7 M. Tianxing, N. Zhukova and **G. Tsochev**, A Multilevel Intelligent Assistant for Multilevel Social Network Analysis, 2020 IEEE 10th International Conference on Intelligent Systems (IS), 2020, pp. 404-408, ISBN: 978-1-7281-5457-2, doi:10.1109/IS48319.2020.9199840. **(Scopus)**

Резюме: През последните години анализът на данни от социалните мрежи е новопоявяваща се област. Многостепенният анализ на социалните мрежи може да помогне на изследователите да разберат всеобхватни фактори на влияние. Но необработените данни, извлечени от живота, са сложни и неработещи, така че целият процес на анализ е многоетапен и променлив. Характеристиките на наборите от данни в социалните мрежи на различни нива са разнообразни. Няма общи алгоритми за анализ на данни за всяко ниво. Характеристиките на данните и изискванията на задачата са важна основа за избор на подходящи методи за анализ. Но това е трудно за изследователите, които не са експерти. Този документ предлага интелигентен многостепенен асистент за многостепенен анализ на социални мрежи и го прилага въз основа на онтологична технология. Алгоритмите на различни нива обработват съответните форми на данни, докато се генерира подходящият изходен модел. Използването на онтологична технология прави тази рамка разширима и разбираема. Такава рамка е важна за неекспертите.

Г7.9 R. Trifonov, O. Nakov, S. Manolov, **G. Tsochev** and G. Pavlova, Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods, 2020 International Conference Automatics and Informatics (ICAI), 2020, pp. 1-4, ISBN: 978-1-7281-9309-0, doi: 10.1109/ICAI50593.2020.9311333. **(Scopus)**

Резюме: Факултетът по компютърни системи и технологии на Техническия университет в София избра стратегия за развитие на обучението по киберсигурност, базирана на: международни стандартизационни документи; концептуален модел, разработен от Съвместната работна група за обучение по киберсигурност; добри практики на модулната структура и динамичните принципи на изграждане, позволяващи бързи промени в съдържанието. Въз основа на принципите на „области на знания“ и „области на приложение“, всяка дисциплина е предназначена да бъде разработена като работен процес за конкретна област на приложение, съставена от модули, представляващи подходящите области на знанието. Решително подобряване на образованието чрез въвеждане на динамични принципи и персонализиране в учебната програма може да се реализира чрез така наречените адаптивни системи за обучение. В допълнение, управлението на адаптацията може да се реализира чрез методи на изкуствения интелект, в използването на които авторите имат опит в приложението им в областта на киберсигурността.

Г7.12 G. Tsochev, R. Trifonov, O. Nakov, S. Manolov and G. Pavlova, Cyber security: Threats and Challenges, 2020 International Conference Automatics and Informatics (ICAI), 2020, pp. 1-6, ISBN: 978-1-7281-9309-0, doi:10.1109/ICAI50593.2020.9311369. **(Scopus)**

Резюме: В днешно време поддръжката на компютърни и мрежови системи е също толкова важна, колкото и тяхната защита. Вирусите представляват един от най-успешните начини за атака на тези системи и тяхното използване неизбежно е част от компютърния бизнес в световен мащаб. Използването на идентификация и/или проверка трябва да бъде защитено от препоръчителния антивирусен софтуер, защитни стени и т.н., както и от множество други технологии, създадени за защита на триединството на информационната сигурност: поверителност, цялост и наличност. Няма специфична стандартизирана процедура за проектиране на защитена мрежа. Сигурността на мрежата трябва да бъде съобразена с текущите нужди на организацията и да постигне необходимата подходяща защита. В тази статия разглеждаме и обобщаваме най-популярните и успешни средства за защита, използвани от организации, както и от физически лица.

Г8.9 R. Trifonov, O. Nakov, S. Manolov, G. Popov, **G. Tsochev** and G. Pavlova, Framework for the Development of Cybersecurity Training Programs for Students of Engineering Specialties, Related to Computer Systems and Information Technologies, Journal Computer and Communications Engineering, 2019, Vol. 13, Issue 2, pp. 68-72, p-ISSN: 1314-2291

Резюме: Имайки предвид безпрецедентната международна съгласуваност, унификация и стандартизация на всички елементи на киберзащитата, включително нейния ключов елемент – обучението по киберсигурност, екипът от Факултета по компютърни системи и технологии на Техническия университет в София избра стратегия за развитие, базирана на: международни стандартизационни документи и преди всичко препоръките на NIST SP 800-16 и ENISA; концептуалния модел, разработен от Съвместната работна група за обучение по киберсигурност; добри практики на

модулната структура и динамичните принципи на изграждане, позволяващи бързи промени в съдържанието. Въз основа на принципите на „области на знания“ и „области на приложение“, всяка дисциплина е предназначена да бъде разработена като работен процес за конкретна област на приложение, съставена от модули, представляващи подходящите области на знанието.

Г8.14 G. Tsochev, R. Trifonov, O. Nakov and D. Gotseva, A Case Study Research on Intrusion Detection System, Journal Computer and Communications Engineering, 2018, Vol. 12, Issue 1, pp. 13-17, p-ISSN: 1314-2291

Резюме: Мрежовата и информационна сигурност в днешно време е много актуален въпрос. Прилагането на размити правила към IDS за компютърна мрежа в рамките на меко базирани методологии за информационна сигурност подобрява способността на IDS за вземане на решения и, от своя страна, мрежата. В тази статия логиката на разума се разглежда като начин за откриване на атаки в изследванията на трафика. Беше проведено експериментално проучване с помощта на софтуера MatLab и Fuzzy Logic Toolbox. Движението е предварително зададено и преминава към входа на експерименталното обучение.

Г8.18 G G. Tsochev, R. Trifonov and R. Yoshinov, VPN Comparison: IPSEC and SSL, Proceedings of the International Conference on Information Technologies (InfoTech-2016), 20-21 September, Bulgaria, 2016, pp. 226-233, ISSN: 1314-1023

Резюме: В тази статия е направен сравнителен анализ между IPsec и SSL. Всеки от протоколите има уникални свойства. Изборът на IPsec или SSL зависи от изискванията за сигурност. IPsec може да се използва за защита на всеки IP трафик, а SSL е фокусиран върху трафика на ниво приложение. IPsec е много подходящ за дълготрайни връзки, където са необходими широки и постоянни връзки на мрежовия слой. SSL, от друга страна, е много подходящ за приложения, където системата трябва да свърже индивиди с приложения и ресурси. И двете технологии са еднакво сигурни. Изборът на стратегия за отдалечен достъп често не се основава на превъзходството на една технология над друга, а по-скоро на решение кое решение отговаря най-добре на нуждите на организацията.

Г7.14 G. Tsochev and R. Yoshinov, The Research on Intelligent DNS Security, 2020 IEEE 10th International Conference on Intelligent Systems (IS), 2020, pp. 409-414, ISSN: 1541-1672, doi:10.1109/IS48319.2020.9200151. **(Scopus)**

Резюме: Дигитализацията на информацията във всички сфери на човешката дейност и използването на технологични иновации, като основен случай за появата на всички заплахи и атаки, които могат да бъдат недостатъчни на съвременните технологии и непрекъснатото разширяване на сложността на сигурността и хардуера. Защитата срещу тези атаки може да се разглежда в различни посоки в информационните и комуникационни технологии. DNS сървърите се разглеждат като предмет на изследването. Основната идея зад това е да се симулират различни видове DNS атаки и да се предложи метод за търсене на прихващания и аларми, използвайки система за откриване и предотвратяване на проникване в DNS сървър. Заедно с това има възможност резултатите, което трябва да се визуализират, да бъдат статистически обработени във графики и диаграми.

Г7.16 R. Trifonov, R. Yoshinov, G. Pavlova, and **G. Tsochev**, Artificial neural network intelligent method for prediction, AIP Conference Proceedings, 2017, Vol. 1872, pp. 020021-020026, ISBN: 978-0-7354-1552-2, https://doi.org/10.1063/1.4996678 **(Scopus) (SJR = 0.165)**

Резюме: Проблемите със счетоводната и финансовата класификация и прогнозиране са голямо предизвикателство и изследователите използват различни методи за решаването им. Разглеждат се методи и инструменти за краткосрочно прогнозиране на финансови операции с помощта на изкуствена невронна мрежа. В статията са описани методите, използвани за прогнозиране на финансови данни, както и разработената система за прогнозиране с невронна мрежа. Архитектурата на една невронна мрежа използва четири различни технически индикатора, които се основават на необработените данни и се представя текущият ден от седмицата. Разработената мрежа се използва за прогнозиране на движението на цените на акциите един ден напред и се състои от входящ слой, един скрит слой и изходящ слой. Методът на обучение е алгоритъм с обратно разпространение на грешката. Основното предимство на разработената система е самоопределянето на оптималната топология на невронната мрежа, поради което тя става гъвкава и по-прецизна. Предложената система с невронна мрежа е универсална и може да се прилага към различни финансови инструменти, като се използват само основни технически индикатори като входни данни.

Учебни пособия в секция III

Е24.1 Г. Цочев и Р. Трифонов, Ръководство за лабораторни упражнения по мрежова и информационна сигурност, Издателство Авангард Прима, 2021, 178 с., ISBN: 978-619-239-621-3, e-ISBN: 978-619-239-622-0

Резюме: Ръководството е предназначено за студенти, изучаващи дисциплината „Мрежова и информационна сигурност”, както и за всеки, който иска да разшири практическите си познания в областта. Състои се от десет теми, съпроводени с теоретични бележки, опитната постановка, необходимо оборудване, задачи и стъпките за тяхното изпълнение и литература за допълнителна подготовка. Всяка от тях е организирана като едно упражнение. Темите могат да бъдат симулирани с помощта на Cisco Packet Tracer и/или Huawei eNSP Network Simulator. За подготовката им са използвани литературни източници от световно известни автори, публикувани стандарти, ръководството на Cisco CCNA Security, ръководството на HCNA-Security и основно опита на авторите в областта на компютърните мрежи и информационната сигурност.