Р Е З Ю М Е

НА НАУЧНИТЕ ТРУДОВЕ
на полк. доц. д-р инж. НИКОЛАЙ ТОДОРОВ СТОЯНОВ

Научните трудове са представени в три категории:

I. Монографични трудове и университетски учебници
II. Научни статии и доклади
III. Научноизследователска и развойна дейност

I. МОНОГРАФИЧНИ ТРУДОВЕ И УНИВЕРСИТЕТСКИ УЧЕБНИЦИ

II.1.3. Г. Велев, М. Божилова, **Н. Стоянов**, **КОМПЮТЪРНИ МРЕЖИ И КОМУНИКАЦИИ**, Издателство "За буквите - О писменехь", ISBN - 978-619-185-148-5, София, 2014, обем: 208 стр., COBISS.BG-ID – 1269811940

Монографията е посветена на компютърните мрежи, на основните принципи на тяхното функциониране и изграждане. Разгледани са и са сравнени двата най-приложими мрежови модели, като основа на мрежовите комуникации. Представени са теоретичните и физическите основи на комуникационните среди. Изложението е структурирано на базата на OSI модела, като във фокуса на разглеждане и анализиране са протоколите, идентифицирани в TCP/IP протоколния стек.

II.1.4, **Н. Стоянов**, **ЗАЩИТА НА ИНФОРМАЦИЯТА**, Издателство "За буквите - О писменехь", ISBN - 978-619-185-130-0, София, 2014, обем: 156 стр., COBISS.BG-ID – 1269970404

В настоящата книга са разгледани въпроси, свързани със защитата на информацията. Представени са основните понятия, различните аспекти при защитата на информацията. Обърнато е внимание на основните формални модели, дадени са базови елементи от криптографията като наука, разгледани са различни протоколи за защита на трафика и са представени технологични решения за защита, като виртуални частни мрежи и архитектура с публичен ключ.

II.1.5. Alexander Kott, **Nikolai Stoianov**, Nazife Baykal, Alfred Moller, Reginald, Sawilla, Pram Jain, Mona Lange, and Cristian Vidu, **ASSESSING MISSION IMPACT OF CYBERATTACKS**: Report of the NATO IST-128

Workshop, студия, ARL-TR-7566, DEC 2015, US Army Research Laboratory, ATTN: RDRL-CIN, 2800 Powder Mill Road, Adelphi, MD 20783-1138, 38 стр.

Този доклад представя резултатите от семинар, проведен от Групата по информационни системи (IST) на Организацията за Наука и технологии на НАТО в Истанбул, Турция, през юни 2015 г., за изследване на технологиите за характеризиране на въздействието на кибератаките върху различни видове мисии. Успехът на военната мисия е силно зависим от комуникационните и информационни системи (CIS), които поддържат мисията и тяхното използване в кибер пространството. Неумолимо нарастващата зависимост от обработката на изчислителна информация за оръжия, разузнаване, комуникационни и логистични системи продължава да увеличава уязвимостта на мисиите към различни киберзаплахи. Атаки срещу КИС или други киберинциденти влошават или прекъсват използването на КИС. Очаква се честотата и сложността на тези инциденти да нараства.

II.1.6. В. Целков, О. Исмаилов, **Н. Стоянов**, **УПРАВЛЕНИЕ НА РИСКА, ТЕСТВАНЕ И ОЦЕНКА НА МРЕЖОВАТА И НФОРМАЦИОННА СИГУРНОСТ,** монография, "Издателство:„За буквите – О писменехь”, ISBN 978-619-185-159-1, София, 2016 г., обем: 334 стр.

Изследванията, стандартите и добрите практики, свързани с управление на риска, тестването и оценката на мрежовата и информационна сигурност, са обект на разглеждане в настоящата книга.

Претенциозното заглавие показва, че съдържанието покрива голяма област от предметното поле на защитата на информацията в компютърните системи и мрежи. В изложението ясно могат да се открояят следните направления:

- *Основи на сигурността на информационните технологии;*
- *Тестване на информационната сигурност;*
- *Оценка на мрежовата и информационна сигурност;*
- *Развитие на стандартите за „добри практики“ за защита на информацията в компютърните системи и мрежи.*

II.1.7. Д. Полимирова, В. Шаламанов, **Н. Стоянов**, Т. Тагарев, Я. Янакиев, Г. Шарков, Я. Папазов, В. Ризов, К. Иванова, **КИБЕРСИГУРНОСТ И ВЪЗМОЖНОСТИ ЗА ПРИЛОЖЕНИЕ НА ИНОВАТИВНИ ТЕХНОЛОГИИ В РАБОТАТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ В БЪЛГАРИЯ**, глава от монография, Институт по публична администрация, София, 2018, ISBN: 978-619-7262-14-8, 285 стр.

Целта на настоящото изследване е установяване на празноти в регулациите на дейностите по киберсигурност и устойчивост в Република България, идентифициране на добри практики в Европейския съюз и НАТО и дефиниране на предложения за усъвършенстване на регулаторната рамка, политики и стратегии за гарантиране на сигурно и устойчиво функциониране на държавата, икономиката и обществото в киберпространството.

II.1.8. В. Целков, **Н. Стоянов**, **СРЕДСТВА ЗА ТЕСТВАНЕ И АНАЛИЗ НА СИГУРНОСТТА НА КОМУНИКАЦИОННО-ИНФОРМАЦИОННИТЕ СИСТЕМИ**, публикуван университетски учебник, "Издателство:„За буквите – О писменехъ", ISBN 978-619-185-466-0, София, 2021 г. обем: 157 стр., COBISS.BG-ID - 46606344

В учебника е представено учебното съдържание на едноименния курс от програмите „Информационна сигурност", „Национална сигурност" и „Комуникации и информиране" на Университета по библиотекознание и информационни технологии (УниБИТ). Представени са и част от резултатите, получени от проучванията и изследванията, извършени в Министерството на отбраната, Комисията за защита на личните данни и Университета по библиотекознание и информационни технологии. Съдържанието е базирано и на добрите практики и световните стандарти и най-вече на стандартите на Съединените Американски Щати (САЩ). Учебникът съдържа въведение, четири глави, пет приложения, заключение, литература и информация за авторите.

II. НАУЧНИ СТАТИИ И ДОКЛАДИ

II.2.11. **Н. Стоянов**, А. Геов, **Архитектура за киберсигурност – технологични аспекти**, научно-приложна статия, CIO брой 7, година IX, юли 2013, стр. 64-65, ISSN 13112-5605

В доклада се разглеждат основните елементи при дефиниране на архитектури за киберсигурност. Отчетени са различните особености при дефиниране на технически изисквания към системите и тяхното отрежение върху архитектурата (в двете посоки). Разгледани са съществуващи архитектури: на SANS; на Northrop Grumman Corporation (FAN); и на DNDAF.

II.2.12. **Н. Стоянов**, **Метрики за киберсигурност**, научно-приложна статия, CIO брой 7, година XI, юли 2015, стр. 59-60, ISSN 13112-5605

В доклада са дадени основните изисквания при дефиниране на метрики за киберсигурност. Разгледани са подходите SMART, PRAGMATIC и SMART-PRAGMATIC.

II.3.69. В. Целков, **Н. Стоянов, ЕДИН ВЪПРОСНИК ЗА ОДИТ НА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ**, научно-приложен

доклад, научна конференция с международно участие „Военни технологии и системи за осигуряване на отбраната 2011 (MT&S 2011), 8-9 декември 2011, София, 2012, Институт по отбрана, ISBN 978-619-90024-1-4, стр. 47-55

В тази статия авторите представят образец на въпросник за одит на сигурността в информационните системи. Въпросникът е базиран на BS 7799 и ISO 27000.

II.3.70. **Н. Стоянов**, **НАПРАВЛЕНИЯ ЗА РАЗВИТИЕ НА КРИПТОГРАФИЯТА СЛЕД КВАНТОВИЯ КОМПЮТЪР**, научно-приложен доклад, научна конференция с международно участие „Военни технологии и системи за осигуряване на отбраната 2011 (MT&S 2011), 8-9 декември 2011, София, 2012, Институт по отбрана, ISBN 978-619-90024-1-4, стр. 56-60

В тази статия са представени насоки за развитие на пост-квантовата криптография. Направено е кратко описание на проблема с квантовите изчисления, засягащи криптографията. Представено е обяснение на следните криптографски протоколи: Криптография, базирана на решетки, криптография, базирана на кодове и криптография, базирана на хеш функции. Дадени са основни дефиниции и трудни за решаване математически проблеми.

II.3.71. Д. Желязков, **Н. Стоянов**, **ПРОБЛЕМИ ПРИ ЗАЩИТА НА ИНФОРМАЦИЯТА В РЕШЕНИЯ ОТ ТИП „CLOUD COMPUTING”,** Научно-приложен доклад, Научна конференция с международно участие „Военни технологии и системи за осигуряване на отбраната 2011 (MT&S 2011), 8-9 декември 2011, София, 2012, Институт по отбрана, ISBN 978-619-90024-1-4, стр. 248-256

В тази статия авторите представят някои аспекти и проблеми на сигурността на информацията в облачни изчислителни среди. В изследването е направена класификация на облачните изчислителни услуги и информационните инфраструктури. Представен е анализ на проблемите на информационната сигурност. Статята представя възгледите на авторите въз основа на техния опит в прилагането на решения за сигурност, свързани с облачните изчисления в Институт по отбрана.

II.3.72. **N. Stoianov**, M. Bozhilova, **A STUDY OF LATTICE-BASED CRYPTOGRAPHY**, Научно-приложен доклад, 5th international scientific conference on defensive technologies, ОТЕН, 2012, Pages 465-469

Криптографията е една от най-важните части на информационната сигурност. Повечето от асиметричните криптографски алгоритми се основават на трудно решени математически проблеми. С нарастването на скоростта на работа на компютъра и наличието на огромно количество компютърна памет някои от тези проблеми изглежда ще бъдат решени в близко време. Освен това изследването на физиката и по-специално разработването

на квантов компютър драматично ще промени света на криптографията. Така наречените квантови алгоритми на Шор и Гроувър са факти. Тези алгоритми ще нарушат широко използвания асиметричен алгоритъм – RSA. Освен това са разработени някои групи нови алгоритми и те изглеждат по-трудни за решаване с квантови алгоритми. Тази статия представя изследване на една група алгоритми, базирани на така наречените „решетъчни проблеми“. Дадена е основна математическа дефиниция, показани са обяснения на проблемите с решетката (проблем с най-късия вектор и проблем с най-близкия вектор) и свързаните криптографски проблеми. Обясняват се най-популярните криптографски схеми и е даден малък числов пример за NTRU с публични параметри (13, 2, 31, 2).

II.3.74. **N. Stoianov**, E. Altimirski, **A STUDY OF OPEN SOURCE PKI SYSTEMS APPLICABLE INTO INDECT PROJECT**, Научно-приложен доклад, XLVIII International Scientific Conference on Information, Communication and Energy Systems and Technologies, ICEST 2013, 26-29 June 2013, Ohrid, Macedonia, Vol. 1, ISBN: 978-9989-786-90-7, pp. 191-194, http://www.icestconf.org/wp-content/uploads/2016/proceedings/icest_2013_01.pdf

Тази статия предоставя проучване на PKI системи с отворен код, приложими в европейския проект INDECT (FP7). Изискванията за вида на сертификатите, дължината на ключа и йерархичната структура са дефинирани в доклада. Обяснена е архитектурата на INDECT PKI с две нива на CA. Въз основа на предложената архитектура бяха проучени две PKI системи с отворен код: OpenCA и EJBCA. С цел създаване на тестова платформа са извършени редица тестове, които са представени в доклада. Предложена е схема на основата на EJBCA, която предлага PKI архитектура и покрива всички изисквания (системни и криптографски) за създаване на крайната INDECT PKI система.

II.3.75. Manuel Urueña, Petr Machník, Marcin Niemiec, **Nikolai Stoianov**, **INDECT SECURITY ARCHITECTURE**,Научно-приложен доклад, Communications in Computer and Information Science, Volume 368 CCIS, Pages 273 - 2872013 6th International Conference on Multimedia Communications, Services and Security, MCSS 2013, 6 June 2013, through 7 June 2013

За да изпълнява задълженията си да служи и защитава, полицията трябва да внедри нови инструменти и приложения, за да поддържа темпото на технологичното развитие. Проектът INDECT разработва такива нови инструменти за разследване, с цел подпомагане на европейските полицейски сили. Полицейските ИКТ системи обаче имат строги изисквания за сигурност, които могат да забавят внедряването на тези нови приложения. Този доклад представя интегрирана архитектура за сигурност, която е в състояние да предос-

тави общи услуги за сигурност както на нови, така и на наследени ИКТ приложения, като същевременно изпълнява високите изисквания за сигурност на полицейските сили. Чрез повторно използване на услугите за сигурност, предоставени от тази архитектура, новите системи не трябва сами да прилагат персонализирани механизми за сигурност и могат лесно да бъдат интегрирани в съществуващата полицейска ИКТ инфраструктура. Предложената архитектура за сигурност на INDECT включва най-съвременни технологии, като криптирани комуникации на мрежови и приложни нива или многофакторно удостоверяване, базирано на сертификати, съхранени в смарт карти.

II.3.76. А. Геов, **Н. Стоянов**, **ОСНОВНИ КОМПОНЕНТИ НА АРХИТЕКТУРА ЗА КИБЕРСИГУРНОСТ В ЗАЩИТЕНИ КОМПЮТЪРНИ СИСТЕМИ,** Научно-приложен доклад, Научна сесия 2013, Национален военен университет, факултет "Артилерия, ПВО и КИС", Шумен 2013 г., ISSN 1313-7433

В доклада, озаглавен „Основни компоненти на архитектурата за киберсигурност в защитени компютърни системи", е дадена основна структура на система за киберсигурност за комуникационни и информационни системи. Предложената структура е разделена на две основни области: технологични компоненти и функционални компоненти. Предложените компоненти са обяснени и е дадена връзката между тях и домейните. Предложеният подход е резултат от работата на авторите в областта на киберсигурността и киберотбраната.

II.3.77. З. Здравков, **Н. Стоянов**, И. Радулов, **ТЕХНОЛОГИЧНИ ВЪЗМОЖНОСТИ ЗА ПРОВЕЖДАНЕ НА КИБЕРОПЕРАЦИИ**, Научно-приложен доклад, Научна сесия 2013, Национален военен университет, факултет "Артилерия, ПВО и КИС", Шумен 2013 г., ISSN 1313-7433

Този документ представя обобщен изглед за Cyber Operation Technologies. Технологии които са класифицирани като кибероръжия и средства за киберотбрана.

II.3.79. И. Ненов, **Н. Стоянов**, В. Целков, **ПОДХОДИ ЗА ОЦЕНКА НА УЯЗВИМОСТИТЕ В КОМПЮТЪРНИ МРЕЖИ И СИСТЕМИ,** Научно-приложен доклад, Съвременни стратегии и иновации в управление на знанието, Сборник доклади, Първата научна конференция „Съвременни стратегии и иновации в управление на знанието": УниБИТ, 3-4 декември 2014 г, Издателство „За буквите – О писменехъ", София, 2014, ISBN 978-619-185-140-9, стр. 256-268

Разгледаният в доклада подход се основава на автоматизирана оценка на уязвимостта на скенери Nessus на Tenable Network Security и The Open Vulnerability Assessment System (OpenVAS). Направен е сравнителен анализ на предимствата и недостатъците на двата продукта.

II.3.80. **N. Stoianov**, M. Urueña, M. Niemiec, P. Machník, G. Maestro, **INTEGRATED SECURITY INFRASTRUCTURES FOR LAW ENFORCEMENT AGENCIES**, Научно-приложен доклад, Multimedia Tools and Applications, Open AccessVolume 74, Issue 12, Pages 4453 - 4468, 13 June 2015

Този доклад предоставя общ преглед на архитектурата за сигурност на правоприлагащите агенции (LEA), разработена в проекта INDECT и по-специално на инфраструктурите за сигурност, които са внедрени досега. Тези инфраструктури за сигурност могат да бъдат организирани в следните основни области: инфраструктура на публичния ключ (PKI) и управление на потребителите, сигурност на комуникациите и нови криптографски алгоритми. Представени са новите идеи, архитектури и разгърнати тестови платформи за тези области. По-специално, обяснена е вътрешната структура на INDECT PKI, използван за управление на федерална идентичност, различните технологии, използвани в тестовия VPN, INDECT Block Cipher (IBC) – нов криптографски алгоритъм, който е интегриран в библиотеката OpenSSL и как IBC -активирани TLS/SSL сесии и X.509 сертификати се използват за защита на INDECT приложения. Всички предложени механизми са проектирани да работят по интегриран начин като основа за сигурност на всички системи, разработени от проекта INDECT за LEA.

II.3.82. Manuel Urueña, Petr Machník, Marcin Niemiec, **Nikolai Stoianov**, **SECURITY ARCHITECTURE FOR LAW ENFORCEMENT AGENCIES,** Научно-приложен доклад, Multimedia Tools and Applications, Open AccessVolume 75, Issue 17, Pages 10709 - 107321 September 2016

За да изпълнят задължението си да служат и защитават, правоприлагащите агенции (LEA) трябва да внедрят нови инструменти и приложения, за да бъдат в крак с темпото на развиващите се технологии. Системите за полицейска информационна и комуникационна технология (ИКТ) обаче имат строги изисквания за сигурност, които могат да забавят внедряването на тези нови приложения, тъй като първо трябва да бъдат приложени необходимите мерки за сигурност. Този документ представя интегрирана архитектура за сигурност за LEA, която е в състояние да предостави общи услуги за сигурност на нови и наследени ИКТ приложения, като същевременно изпълнява високите изисквания за сигурност на полицейските сили. Чрез повторно използване на услугите за сигурност, предоставени от тази архитектура, новите системи не трябва сами да прилагат персонализирани механизми за сигурност и могат лесно да бъдат интегрирани в съществуващите полицейски ИКТ инфраструктури. Предложената архитектура за сигурност на LEA включва най-съвременни тех-

нологии, като криптирани комуникации на мрежови и приложни нива или многофакторно удостоверяване на базата на сертификати, съхранени в смарт карти.

II.3.83. Д. Махлянов, **Н. Стоянов**, **СИГУРНОСТТА В ИНТЕРНЕТ НА НЕЩАТА (INTERNET OF THINGS - IOT),** Научно-приложен доклад, Eighth International Scientific Conference „HEMUS-2016“, p.III-217 - III-225 (2016)

IoT съществува в наши дни с всичките му предимства и рискове. Настоящата статия описва накратко същността на IoT и основните проблеми, свързани със сигурността в IoT. Посочени са различни видове атаки срещу IoT, както и някои проблеми, свързани с внедряването на IoT системи. Представена е основна концепция за създаване на защитена среда с IoT.

II.3.84. М. Куцакис, **Н. Стоянов**, **ЕЗИК ЗА МОДЕЛИРАНЕ НА КИБЕР-СИГУРНОСТ – CYSEMOL**, Научно-приложен доклад, Осма международна научна конференция, Научните изследвания – ключов фактор за придобиване на нови отбранителни способности, ХЕМУС-2016, 26 май 2016 г., София, 2016 ISSN 1312–291

С течение на времето ИТ системите се разрастнаха. Това доведе до увеличаване както на сложността, така и на трудността за поддържане на пълно знание за системата. Освен това възможностите за атака и броят на уязвимостите в системата нарастват. Това представлява проблем за администраторите и служителите по сигурността, които често работят при ограничен бюджет и трябва да дадат приоритет къде да проучат или подобрят системата. Предложени са различни инструменти за подпомагане на вземащите решения при този вид проблеми. Един такъв инструмент е CySeMoL (Cyber Security Modeling Language), който използва байесови мрежи за изчисляване на рисковете за сигурността в модел на системата. Чрез използването на CySeMoL за моделиране на известни предишни атаки е възможно както да се валидира моделът, така и да се намерят области, които могат да бъдат подобрени.

II.3.85. **Н. Стоянов**, Л. Петров**, ОБЗОР НА КРИТИЧНАТА ИНФРАСТРУКТУРА - ОБЩИ ПОЛОЖЕНИЯ, ДЕФИНИЦИЯ, ТИПОВЕ**, Научно-приложен доклад, Осма международна научна конференция, Научните изследвания – ключов фактор за придобиване на нови отбранителни способности, ХЕМУС-2016, 26 май 2016 г., София, 2016 ISSN 1312–291

В доклада са представени основи понятия, дефиниции и типове критични инфраструктури. На основата на представена класификация са идентифицирани основни заплахи за сигурността в тези инфраструктури. На основата на анализа е предложен модел за защита на критична инфраструктура.

II.3.86. Д. Атанасова, **Н. Стоянов**, **КИБЕРСИГУРНОСТ В БЪЛГАРИЯ И ОБЩОЕВРОПЕЙСКИ СТРУКТУРИ**, Научно-приложен доклад, Осма международна научна конференция, Научните изследвания – ключов фактор за придобиване на нови отбранителни способности, ХЕМУС-2016, 26 май 2016 г., София, 2016 ISSN 1312–291

В доклада са разгледани основните „играчи“ в ЕС в областта на киберсигурността. Представени са техните области на действие и потенциални способности. На основата на анализа е предложен модел за координация в областта на защитата на информацията и киберсигурността. Интерпретирани са и получените резултати за ЕС с цел изграждане на капацитет в Република България.

II.3.87. Я. Колегова-Делчева, **Н. Стоянов**, **АНАЛИЗ НА КИБЕРСИГУРНОСТТА ВЪВ ВЪОРЪЖЕНИТЕ СИЛИ**, Научно-приложен доклад, Осма международна научна конференция, Научните изследвания – ключов фактор за придобиване на нови отбранителни способности, ХЕМУС-2016, 26 май 2016 г., София, 2016 ISSN 1312–291

Бързото развитие на информационните системи, глобализацията и технологичният процес са предпоставка за развитие на престъпленията в киберпространството. Бързорастящият брой киберпрестъпления, използването на интернет от терористи налагат необходимостта от провеждане на ефективна и ефикасна политика за киберсигурност. Политиката за киберсигурност присъства във всички държавни и частни структури, но водещите структури в поддържането на мира и гарантирането на сигурността са въоръжените сили. Следователно те са натоварени със сложната задача да създадат, възприемат и внедрят механизмите за противодействие на кибератаките.

II.3.88. И. Иванов, **Н. Стоянов**, **АНАЛИЗ НА АРХИТЕКТУРИТЕ ЗА ОБЛАЧНИ УСЛУГИ**, Научно-приложен доклад, Научна конференция с международно участие "Облачните технологии и защитата на информацията", 12-13 май 2016 г, Шумен

В доклада е направен анализ на различните видове облачни архитектури – SaaS, PaaS, IaaS и различните типове и начини за изграждане на облачни системи – публичен, частен и смесен. На основата на анализа са предложени подходи за изграждане на „специализирани архитектури за облачни услуги“.

II.3.89. L. Petrov, **N. Stoianov**, T. Tagarev, **CRITICAL INFORMATION INFRASTRUCTURE PROTECTION MODEL AND METHODOLOGY, BASED ON NATIONAL AND NATO STUDY**, Научно-приложен доклад, In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds) Advances in Dependability Engineering of Complex Systems. DepCoS-RELCOMEX

2017. Advances in Intelligent Systems and Computing, vol 582. Springer, Cham. https://doi.org/10.1007/978-3-319-59415-6_34

Националната и международната сигурност, нашият финансов, индустриален и икономически просперитет, здравната система и националното благосъстояние като цяло зависят от критичните инфраструктури, които могат да бъдат описани като силно взаимозависими. Налични са много примери, като националната електрическа мрежа, системите за нефт и природен газ, телекомуникационни и информационни мрежи, транспортни мрежи, водни системи, банкови и финансови системи. Поддържането им в надеждно и сигурно състояние и изучаването на техните зависимости е от първостепенно значение за всяко правителство или организация. Съществува спешна необходимост от тяхната класификация. Създаването и разработването на модел и методология, които биха могли да опишат тяхното поведение, ще направи този свят по-безопасен. Представеният тук модел и базираното на него проучване и първоначалните резултати са стъпки към надеждна и сигурна критична информационна инфраструктура.

II.3.90. **Nikolai T. Stoianov**, Maya G. Bozhilova, Grigor R. Velev, **TOWARDS SECURITY REQUIREMENTS OF THE SPIDER PROJECT,** Научно-приложен доклад, Международна научна конференция „Киберсигурността в информационното общество“, сборник научни трудове, НВУ “В. Левски” – Факултет “Артилерия, ПВО и КИС”, Шумен 2017, ISBN 978-954-9681-82-6, стр.25-стр.31

Необходимостта от използване на сензорни системи и мрежи за вътресградна ситуационна осведоменост при градски военни операции изисква строги изисквания за тяхната сигурност и надеждност. Докладът дефинира понятия, свързани със сигурността в съответствие с предназначението и функциите на сензорната система.

II.3.91. Д. Махлянов, **Н. Стоянов**, **АНАЛИЗ НА КИБЕРСИГУРНОСТТА В МОДЕЛИТЕ ЗА INTERNET OF MILITARY THINGS**, Научно-приложен доклад, Международна научна конференция „Киберсигурността в информационното общество“, сборник научни трудове, НВУ “В. Левски” – Факултет “Артилерия, ПВО и КИС”, Шумен 2017, ISBN 978-954-9681-82-6, стр.32-стр.39

IoT се разширява в различни области на живота ни. IoMT е почти чисто нов клон на IoT. Настоящата статия описва накратко основните модели за реализация на IoMT, базирани на обработката на информация. В доклада е извършен анализ, фокусиран върху киберсигурността за различни модели.

II.3.92. Л. Петров, **Н. Стоянов**, **МНОГОСЛОЕН МОДЕЛ ЗА КИБЕРСИГУРНОСТ НА КРИТИЧНА ИНФОРМАЦИОННА ИНФРАСТРУКТУРА**, Научно-приложен доклад, Международна научна конференция „Киберсигурността в информационното общество“, сборник научни трудове, НВУ “В. Левски” – Факултет “Артилерия, ПВО и КИС”, Шумен 2017, ISBN 978-954-9681-82-6, стр.124-стр.129

Националната и международната сигурност, нашето национално благополучие зависят от критични информационни инфраструктури, които могат да бъдат описани като силно взаимозависими. Поддържането им в надеждно и сигурно състояние и изучаването на техните зависимости е от първостепенно значение за всяко правителство или организация. Създаването и развитието на многослоен модел на критична информационна инфраструктура за киберсигурност ще направи този свят по-безопасен. Описаният тук модел е стъпка към надеждна и сигурна критична информационна инфраструктура.

II.3.93. М. Куцакис, **Н. Стоянов**, **ТЕХНОЛОГИЧЕН МОДЕЛ ЗА КИБЕРСИГУРНОСТ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ**, Научно-приложен доклад, Международна научна конференция „Киберсигурността в информационното общество“, сборник научни трудове, НВУ “В. Левски” – Факултет “Артилерия, ПВО и КИС”, Шумен 2017, ISBN 978-954-9681-82-6, стр.140-146

Държавната администрация е част от механизма на обществен контрол. Държавната администрация предоставя на гражданите редица услуги. Тези услуги работят благодарение на доброто планиране и надеждна инфраструктура. Услугите, предоставяни от публичните администрации, са защитени и изградени чрез конкретни планове и стъпки от: „Национална стратегия за киберсигурност“. Прехвърлянето на тези услуги в цифровия свят с неправилна компютърна и мрежова структура може да доведе до много уязвимости. Осигуряването на връзка и всякакви технически средства е наложително за правилното и безопасно функциониране на услугите.

II.3.94. Enev E., Velev G., **Stoianov N.**, Bozhilova M., **REQUIREMENTS TO THE SENSOR PLATFORM AND NETWORK FOR INDOOR DEPLOYMENT AND EXTERIOR BASED RADIOFREQUENCY AWARENESS,** Научно-приложен доклад , International Research Conference “105 Years Research and Knowledge for the Security and Defence, Bulgarian Military Academy “G. S. Rakovski”, 6-7 April, Sofia, 2017

Основната информация в този доклад е относно резултатите от проучването на проблемите, необходими при използване на сензорна платформа и мрежа за вътрешно разгръщане и външно базирано радиочестотно осведомя-

ване в градски операции. Избрани са основни тактически изисквания и пространствено-времеви параметри, в които трябва да работят техническите средства за придобиване на информация и данни. Докладът представлява и допълнителна информация за бъдещите тенденции на експерименти в този проект.

II.3.95. T. Tagarev, G. Sharkov, **N. Stoianov**, Cyber Security and Resilience of Modern Societies: A Research Management Architecture, Научно-приложен доклад 16 Information & Security: An International Journal, Volume 38, p.93-108 (2017), http://dx.doi.org/10.11610/isij.3807

Усъвършенстваните информационни и комуникационни технологии (ИКТ) улесняват повишаването на ефективността и ефикасността на организациите за отбрана и сигурност, правителствените услуги, икономиката и качеството на живот, като в същото време предоставят възможности на злонамерените участници да причинят значителни щети. Политиките за сигурност и устойчивост на съвременните общества към заплахи и рискове от киберпространството отчитат предвидените киберзаплахи, тяхното непосредствено въздействие върху ИКТ инфраструктурата, последващите ефекти върху критичните услуги, както и каскадните ефекти в системите и инфраструктурите. Този доклад представя архитектурата, използвана за планиране и, следователно, управление на изследванията в областта на киберсигурността в България. Той обхваща пет области на приложение (системи за управление на информацията; системи за индустриален контрол; безпилотни и дистанционно пилотирани превозни средства; биоинтегрирани системи, и когнитивни процеси и вземане на решения), изследване на системи от системи и подкрепа за формулирането и прилагане на политиката за киберсигурност.

II.3.96. Lytvynov, V., **Stoianov, N.**, Skiter, I., Trunova, H., & Hrebennyk, A, **ЗАХИСТ КОРПОРАТИВНИХ МЕРЕЖ ВІД АТАК З ВИКОРИСТАННЯМ КОНТЕНТ-АНАЛІЗУ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ**, Научно-приложен доклад, Технічні науки та технології, (1(11), 115–130. вилучено із http://tst.stu.cn.ua/article/view/135504

Целта на статията е организирането на колективна защита на корпоративните мрежи чрез въвеждане на системи за наблюдение на заплахи, активни разузнавателни дейности в глобалното информационно пространство с цел търсене, събиране и анализ на данни за атаки, необичайно поведение и съдържание на интернет ресурсите.

II.3.98. В. Литвинов, **Н. Стоянов**, І. Скітер, О. Трунова, А. Гребенник, **АНАЛІЗ СИСТЕМ ТА МЕТОДІВ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ**

ВТОРГНЕНЬ У КОМП'ЮТЕРНІ МЕРЕЖІ, Научно-приложен доклад, Інформаційні і телекомунікаційні технології, УДК 004.056.5, ISSN 1028-9763. Математичні машини і системи, 2018, № 1

В доклада е представен математически подход за формиране на подход на нормално функциониране на системи и дефиниране на обобщена оценка на състоянието на системата, която трябва да бъде защитена. Описани са основните недостатъци и насоките за по-нататъшно развитие на системите за откриване на проникване.

II.3.99. Tagarev, Todor & **Stoianov, Nikolai** & Sharkov, George, **INTEGRATIVE APPROACH TO UNDERSTAND VULNERABILITIES AND ENHANCE THE SECURITY OF CYBER-BIO-COGNITIVE-PHYSICAL SYSTEMS,** Научно-приложен доклад, (2019) Conference: 18th European Conference on Cyber Warfare and Security ECCWS 2019At: University of Coimbra, Portugal, 2019 pp. 492-500

Тази статия очертава проблема с уязвимостта на всеки от петте домейна към влияния от киберпространството. Представя някои постижения в междудомейн разбирането на уязвимостите, подкрепени от примери за проучвания на киберсигурността и предоставя очертанията на съответна интердисциплинарна изследователска програма, изградена около концепцията за системи от системи. Авторите заключават, като прогнозират, че областта на киберсигурността ще бъде обект на значителен растеж през следващите години, изисквайки мулти- и интердисциплинарни компетенции и научна подкрепа.

II.3.100 A. Ivanov, **N. Stoianov**, **NEW APPROACH OF SOLVING CONGRUENCE EQUATION SYSTEM,** Научно-приложен доклад, Communications in Computer and Information Science,Volume 1284 CCIS, Pages 16 - 24, 2020 10th International Conference on Multimedia Communications, Services and Security, MCSS 2020, Kraków, 8 October 2020through 9 October 2020

Днес в криптографията с публичен ключ се използват някои специални основни алгоритми. Разширеният Евклидов алгоритъм и Китайската теорема за остатъка са най-разпространените основни алгоритми. През последните години математиците направиха много, за да подобрят скоростта на изпълнение на тези алгоритъми. В статията е представен нов подход за решаване на система от конгруентни уравнения.

II.3.101 M. Pappalardo, M. Niemiec, M Bozhilova, **N. Stoianov**, A. Dziech, B. Stiller, **MULTI-SECTOR ASSESSMENT FRAMEWORK – A NEW APPROACH TO ANALYSE CYBERSECURITY CHALLENGES AND OPPORTUNITIES**, Научно-приложен доклад, Communications in Computer and Information Science, Volume 1284 CCIS, Pages 1 – 15, 2020 10th International

Conference on Multimedia Communications, Services and Security, MCSS 2020, Kraków8 October 2020, through 9 October 2020

В този доклад е представен нов подход за анализ на предизвикателствата и възможностите за киберсигурност, фокусиран върху разработването на нова рамка за оценка и управление на риска. Такава многосекторна рамка за оценка следва да може да оценява и приоритизира рисковете за киберсигурността в междуведомствен и междусекторен контекст. Това води до правилно разпределение на ресурсите и действия за смекчаване след атака.

II.3.102 I. Burmaka, **N. Stoianov**, V. Lytvynov, M. Dorosh, S. Lytvyn, **PROOF OF STAKE FOR BLOCKCHAIN BASED DISTRIBUTED INTRUSION DETECTING SYSTEM**, Научно-приложен доклад, Advances in Intelligent Systems and Computing, Volume 1265 AISC, Pages 237 – 247, 2021 15th International Scientific-Practical Conference on Mathematical Modeling and Simulation of Systems, MODS 2020, Chernihiv29 June 2020through 1 July 2020

Един от най-важните компоненти на всяка корпоративна мрежа е системата за откриване на проникване. В същото време, обаче, е трудно да се намери механизъм за установяване на доверие между възлите в голяма разпределена система. Блокчейн може да се използва като такъв механизъм, но повечето работещи блокчейни използват случаи, свързани с криптовалути. В този доклад авторите предлагат няколко модификации на протокола за консенсус за доказване на дял, за да се приеме за използване с IDS, базиран на блокчейн. Също така е създаден модел, базиран на агент, за да симулира процес на залагане за нашия модифициран консенсусен протокол. Резултатът от моделирането ще помогне да се оцени ефективността на IDS, базиран на блокчейн, в нормално състояние и в някои критични ситуации и да се намерят най-подходящите параметри на консенсусния протокол в зависимост от размера на мрежата.

II.3.103 Bozhilova, M., Yanakiev Y., **Stoianov N.**, & Stoyanov D., **AN APPROACH FOR PRIORITISATION**, Научно-приложен доклад, Journal of Defence & Security Technologies 3, no. 1 (2020): 55-83

Тази статия има за цел да предложи методология за приоритизиране на националните интереси. Започва с изследване и дефиниране на ключовия термин – национален интерес. Фокусът на определението е върху дългосрочните и сравнително стабилни цели, които нациите се стремят да постигнат. След това статията представя преглед на съществуващите методи за оценка на националните интереси. Основната част на статията е фокусирана върху предложения подход за приоритизиране на националните интереси на страните-членки на ЕС, базиран на методи за експертна оценка и по-точно оценката се

извършва чрез прилагане на Аналитичен йерархичен процес. Накрая е описан илюстративен пример за проверка и валидиране на предложената методология.

II.3.104 Y. Yanakiev, **N. Stoianov**, D. Kirkov, G. Velev, **DEFENCE STRATEGY AND NEW DISRUPTIVE TECHNOLOGIES NEXUS: IMPLICATIONS FOR THE MILITARY ORGANISATIONS**, Научно-приложен доклад, Journal of Defence & Security Technologies, Volume 3, Issue 1, Number 2, p.7-41 (2020)

Тази статия има за цел да проучи ролята на стратегията в областта на отбраната, със специален фокус върху това как технологичните иновации могат да повлияят на развитието на стратегията. Ключовият въпрос е как и по какви начини технологичният напредък може да повлияе на развитието на отбранителната стратегия. Започва с еволюция на концепцията за отбранителна стратегия през последните години, както и нейната възможна бъдеща трансформация, успоредно с тенденциите на новите и нововъзникващи отбранителни технологии. След това се анализират различни концептуални модели на отбранителна стратегия въз основа на казуси от стратегически документи в областта на отбраната на нациите, представени в консорциума на проекта EU Predictive methodologY for Technology Intelligence Analysis (PYTHIA), както и документи на ЕС и НАТО. Накрая, статията обобщава някои изводи относно динамичния характер на взаимовръзката между развитието на отбранителните стратегии и технологичните иновации. Освен това са представени някои идеи относно това как научните изследвания в областта на отбраната могат да отговорят на оперативните нужди, като подкрепят с нови знания производството и доставката на най-необходимите оръжейни системи.

II.3.105 **Nikolai Stoianov**, Andrey Ivanov, **PUBLIC KEY GENERATION PRINCIPLES IMPACT CYBERSECURITY**, Научно-приложен доклад, Information & Security: An International Journal, Volume 47, Issue 2, p.249-260 (2020)

Криптографските алгоритми с публичен ключ се основават на законите и принципите на теорията на числата. За всяка криптографска система един от най-важните въпроси е ключът на потребителя, който той/тя използва за криптиране на съобщенията. Това е причината процесът на генериране на ключ винаги да е основен за защитата на данните и тъй като криптографията заема повече място в ежедневието ни, принципите за генериране на публичен ключ са толкова важни. В тази статия авторите обсъждат теста за основност на Милър-Рабин във връзката му с процеса на генериране на ключ.

II.3.106 **Nikolai Stoianov**, Maya Bozhilova, **A MODEL OF A CYBER DEFENCE AWARENESS SYSTEM OF CAMPAIGNS WITH MALICIOUS**

INFORMATION, Научно-приложен доклад, Information & Security: An International Journal, Volume 46, Issue 2, p.182-197 (2020)

Много организации са подложени на кибератаки с цел разпространение на злонамерена информация. Ситуационната осведоменост е инструмент за противодействие на кампаниите от злонамерена информация и намаляване на нейното разпространение. Тази статия предлага концептуален модел за система за осведоменост за киберотбраната, която има за цел да подпомогне човешките оператори да избегнат този тип заплаха. Системата ще идентифицира (класифицира) три вида кампании за злонамерени информационни операции – злонамерено инжектиране на информация в уеб съдържание, инжектиране на злонамерена информация във фалшиви акаунти в социални мрежи и разпространение на злонамерена информация чрез имейл съобщения. Предложен е модел за идентифициране на типа кампания от злонамерени информационни операции, базиран на теорията на доказателствата на Демпстър-Шейфър. Работата, представена тук, е част от проекта Cyber Rapid Analysis for Defense Awareness of Real-time Situation - CyRADARS.

II.3.107 Todor Tagarev; Salvatore Marco Pappalardo; **Nikolai Stoianov**, **A LOGICAL MODEL FOR MULTI-SECTOR CYBER RISK MANAGEMENT,** Научно-приложен доклад, Information & Security: An International Journal, Volume 47, Issue 1, p.13-26 (2020)

Нарастващото използване на цифрови инфраструктури прави цели сектори на икономиката и обществените услуги уязвими на атаки през киберпространството. Постигнат е известен напредък в разбирането на уязвимостите и начините за намаляване на киберриска на подсекторно ниво. Докато секторното ниво остава значително предизвикателство, това проучване отива отвъд, като се занимава и с киберриска, произтичащ от междусекторните и многосекторните взаимозависимости в последователен логически модел. Документът представя обхвата на този логически модел, очертава проблема с оценката на риска, структуриран около триплета „Заплахи – Уязвимости – Въздействие“ и структурирането на смекчаването на риска около видовете мерки за намаляване на риска, целта на вземането на решения относно риска и начините на приложение. Предоставени са примери за прилагането на логическия модел, лежащ в основата на рамката за многосекторна оценка на ЕСНО и завършва, като подчертава предимствата, които предоставят логическият модел и рамката.

II.3.108 Velizar Shalamanov, **Nikolai Stoianov**, Yantsislav Yanakiev, **ICT GOVERNANCE, HUMAN FACTORS AND CYBER SITUATIONAL AWARENESS**, Научно-приложен доклад, Information & Security: An International Journal, Volume 46, Issue 1, p.7-10 (2020)

Статията обобщава резултатите от четирите сесии по време на Втората международна научна конференция Дигитална трансформация, киберсигурност и устойчивост DIGILIENCE 2020. Това са изграждане и управление на ИКТ за дигитална трансформация, Киберситуационна осведоменост и обмен на информация, Подход за интегриране на човешки системи към киберсигурността и Образование и Обучение за киберустойчивост.

II.3.109 **Nikolai Stoianov**, Maya Bozhilova, **EXPERT'S STUDY ON SITUATIONAL AWARENESS OF OPERATIONS DIRECTED AT THE WIDE DISSEMINATION OF MALICIOUS INFORMATION**, Научно-приложен доклад, Conference Proceedings, MODS2020, Chernihiv, Ukraine (2020)

В доклада са представени резултатите от експертно изследване в контекста на проект CyRADARS за нуждите на т.нар. крайни потребители при разработване на системата за мониторинг на злонамерени дейности в киберпространството. На основата на изследването са дефинирани направленията за развитие на системата.

II.3.110 T. Tagarev, **N. Stoianov**, **SCOPING THE SCENARIO SPACE FOR MULTI-SECTOR CYBERSECURITY ANALYSIS**, Научно-приложен доклад, "Studies in Big Data, Volume 84, Pages 203 - 217, 2021

Докладът представя резултатите от проекта Horizon 2020 ECHO, подпомагащ идентифицирането и разработването на сценарии за кибератаки. Той изследва сценарийното пространство в четири измерения: (1) критични инфраструктури и основни услуги, критично зависими от ИКТ инфраструктурата; (2) видове злонамерени участници и техните възможности; (3) използвани уязвимости; и (4) краткосрочен спрямо по-дългосрочен хоризонт. Изследването служи за цялостно обхващане на пространството на сценариите. Авторите представят частичен списък от избрани сценарии, сюжетни линии и случаи на употреба, които се използват в последващи изследвания за определяне на ключови компоненти на изискванията за способности: технологични пътни карти, рамка за киберумения, обмен на информация и изисквания за сертифициране.

II.3.111 П. Василев, **Н. Стоянов**, Ц. Цонев, **ПОДХОД ПРИ ИЗГОТВЯНЕТО НА ИНОВАТИВНИ ПРОГРАМИ ЗА ОБУЧЕНИЕ ПО КИБЕРСИГУРНОСТ,** Научно-приложен доклад, Сборник доклади международна научна конференция съвременни изследвания и технологии за отбраната, ARTDef – 2021, 29 - 30 юни 2021 г., ВВМУ „Никола Йонков Вапцаров" - Варна, ISSN 2815-2581, 2021, II-186

Този доклад представя подход за създаване на иновативни програми за обучение по киберсигурност в областта на авиацията, енергийните мрежи и

военноморските сили, избрани в проекта FORESIGHT на Европейската комисия и разглежда предимствата на този подход.

III. НАУЧНОИЗСЛЕДОВАТЕЛСКА И РАЗВОЙНА ДЕЙНОСТ

II.4.22. Методология за предвиждане на тенденции в развитието на военните технологии и влиянието им върху изграждането на отбранителните способности на Република България, Министерство на отбрана - Програма 7.1, Национален научен проект, ИО, 2019 г.

Основната цел на проекта е да се разработи и експериментира методология и да се предложат виждания и препоръки за осъществяване на постоянен мониторинг за идентифициране на нововъзникващи технологии и тяхното влияние върху развитието на отбранителните способности в дългосрочен аспект.

II.4.23. Придобиване на сензорна информация от наземни, водни и безпилотни летателни средства и визуализирането ѝ в зала за вземане на решения, Министерство на отбрана - Програма 7.1, Програма 7.2, Програма 1.7.7, Национален научен проект, ИО, 2018 г.

Целта на проекта е да се изследва и осигури възможност за добиване, изпращане и визуализиране на информация от местността в реално време от район на оперативна (кризисна) информация чрез използване на подвижни наземни, водни и безпилотни летателни средства (автомобили с повишена проходимост, радиоуправляеми лодки, дронове и др.) и последваща компютърна обработка на получената сензорната информация и визуализация в център за вземане на решения.

II.4.24. Изграждане на прототип на високонадеждна облачна (Cloud) архитектура, осигуряваща платформа за информационни услуги и защитен обмен на информация в система от центрове за данни, Министерство на отбрана – Програма 7.1, Програма 7.2 и Програма 1.7.7, 2016 - 2019 г., Национален научен проект, ИО, 2016 г.

Основната цел на проекта е чрез използване на съвременни технологии за виртуализация да се изгради прототип на високонадеждна (High Availability) облачна архитектура за осигуряване на платформа за информационни услуги и на защитен обмен (репликация) на информация в система от центрове за данни за нуждите на МО и БА.

II.4.25. Malicious Network Activities Monitoring and Data Analysis (MAMA), Министерство на отбрана - Програма 7.1 "Научно-изследователски дейности и проекти", 2019 - 2022 г. Национален научен проект, ИО, 2019 г.

Проектът има за цел да изгради средства за прихващане и анализиране на кибератаки, за да се проучат потенциалните киберзаплахи в три, свързани с Интернет ведомствени мрежи – на Институт по отбрана „Проф. Цветан Лазаров“, на Министерство на отбраната и на Националната лаборатория по компютърна вирусология – БАН. Идеята е в трите мрежи да се инсталира един и същ тип Honeypot. Този Honeypot ще се конфигурира да наблюдава заплахите от Интернет. Данните, събирани от Honeypot, ще се съпоставят със системните журнални записи, като по този начин ще се получи картина на злонамерените атаки, съответно към мрежите на трите организации.

На базата на статистически анализ на събраната информация ще се подобри ситуационната осведоменост за заплахите в националното киберпространство, ще се идентифицират източниците на заплахи, както и най-честите типове атаки. Резултатите от анализа ще позволят разработването на теоретични основи, методи и препоръки за киберзащита на компютърните мрежи в МО и БА.

В контекста на нарастващите по количество, интензивност и нанесени щети от кибератаки, резултатите от проекта са изключително важни за придобиване на способността - киберотбрана.

II.4.26. Homemade Explosives and Recipes characterisations (HOMER) EU project, FP7-SECURITY, Grant agreement ID: 312883, EC-2012.1.3.2, Coordinated by Police Service of Northern Ireland United Kingdom, 2013-2016, Международен научен проект (FP7), Институт по отбрана, 2016 г.

Целта на проекта HOMER е да се приложи цялостно, съгласувано европейско проучване на домашно произвеждани експлозиви, включително идентифицирането, откриването на експлозиви, предотвратяването на заплахите от домашно произвеждани експлозиви и за лесното идентифициране на фабрики за бомби.

II.4.27. GAP - Gaming for Peace, H2020, Grant agreement ID: 700670, H2020-BES-2014-2015, DOI https://doi.org/10.3030/700670, Международен научен проект (H2020), Институт по отбрана, 2018 г.

Проектът GAP предлага итеративен процес на разработване и усъвършенстване на учебна програма за военни, полицейски и цивилен персонал, които оценяват играта и вградената основна/базова учебна програма, като играят играта и по този начин внасят своя собствен опит в играта. По този начин

допълнително развиват учебната програма на СРРВ и съответните меки умения. Играта може да бъде достъпна навсякъде през интернет и няма ограничение за броя на персонала, който може да бъде обучен. Играта може да бъде персонализирана на ниска цена от различни заинтересовани страни. Консорциумът GAP е мултидисциплинарен с опит в социалните науки, компютърните науки, крайните потребители (включително армия и полиция) и МСП специализирали в дизайна на игри, разработването на учебни програми и стандартизирането и хармонизирането на уменията.

II.4.28. SOLOMON - Strategy oriented analysis of the market forces in EU defence"H2020, Grant agreement ID: GA 831379 – SOLOMON, PADR-STF-02-2018" Международен научен проект (PADR), Институт по отбрана, 2021 г.

Проектът SOLOMON възнамерява да обедини двете допълващи се визии на голямата стратегия (както произтича от гео/политическите/икономически позиции на ЕС) и бизнес стратегията (както произтича от теорията за веригата на стойността на Майкъл Портър), за да очертае възможните пътни карти за справяне с риска от доставки за въоръжените системи на ЕС в свят на променящи се стратегии, нововъзникващи технологии и променящи се правителствени ограничения.

II.4.29. PYTHIA - Predictive methodology for technology intelligence analysis, H2020, Grant agreement ID: GA 800893 –PYTHIA, PADR-STF-01-2017, Международен научен проект (PADR), Институт по отбрана, 2019 г.

Проектът PYTHIA има за цел да създаде новаторска методология за стратегическо технологично предвиждане, способна да предоставя чести „прогнози“ по въпроси, свързани с технологиите, включително откриването на основни тенденции в избрана област.

II.4.30. ROBORDER - Autonomous swarm of heterogeneous robots for border surveillance "H2020, Grant agreement ID: 740593, H2020-SEC-2016-2017, DOI https://doi.org/10.3030/740593, Международен научен проект (H2020), Институт по отбрана, 2022 г.

Проектът ROBORDER има за цел да разработи и демонстрира напълно функционална автономна система за наблюдение на границите с безпилотни мобилни роботи, включително въздушни, надводни, подводни и наземни превозни средства, способни да функционират както самостоятелно, така и в рояци, който ще включва мултимодални сензори като част от оперативно съвместима мрежа. Системата е оборудвана с адаптивни сензорни и роботизирани технологии, които могат да работят в широк диапазон от оперативни и екологични настройки. За да осигури пълна и подробна картина на ситуационна осведоменост, мрежата от сензори включва статични мрежови

сензори като радари за наблюдение на границите, както и мобилни сензори, персонализирани и инсталирани на борда на безпилотни превозни средства.

II.4.31. Национална научна програма "Сигурност и отбрана", Министерство на образованието, Национална научна програма, Министерски съвет, МОН, 2022 г.

Осигуряване на сигурна и благоприятна среда за развитие на обществото и държавата чрез провеждане на координирани и целеви фундаментални и приложни научни изследвания в областта на сигурността и отбраната и създаване на устойчиво партньорство между включените научни и образователните организации в програмата за съвместно участие в национални и европейски международни изследователски мрежи, програми и проекти.

II.4.32. CyRADARS - Cyber Rapid Analysis for Defense Awareness of Real-Time Situation, Science for Peace and Security, NATO, 2017-2021, Международен научен проект (NATO SPS), Институт по отбрана, 2021 г.

В проекта са разработени нови теоретични постановки, методи и изследователски прототипи на софтуерни инструменти за създаване на ситуационна осведоменост за големи киберкампании: операции, насочени към широко разпространение на злонамерена информация.

II.4.33. ODYSSEUS - Preventing, countering, and investigating terrorist attacks through prognostic, detection, and forensic mechanisms for explosive precursors, H2020, European Commision Международен научен проект (H2020), Институт по отбрана, CORDIS, 2021 г.

Борбата с тероризма изисква арсенал от инструменти. Едни от тях са знанията за прекурсорите на експлозиви – химични вещества, които могат да се използват за законни цели, но също така могат да бъдат използвани за незаконно производство на самоделни експлозиви. В този контекст финансираният от ЕС проект ODYSSEUS ще разработи ефективни и ефикасни инструменти за прогнозиране, откриване и разследване за подобряване на превенцията, противодействието и разследването на терористични инциденти, включващи домашно направени експлозиви. Знанията ще помогнат при разработването на инструменти за наблюдение на веригата за доставка на химикали и отчитане на прекурсори за експлозиви (почти) в реално време. Инструментите ще бъдат тествани на място в три случая на оперативна употреба.

II.4.34. CUIIS - Comprehensive Underwater Intervention Information System, EDIDP, European Commision, Международен научен проект (EDIDP), Институт по отбрана, 2021 г.

Обхватът на проекта CUIIS се фокусира върху иновативно цялостно системно решение в областта на подводните технологии за физическа поддръжка и възстановяване на водолази, изграждане на системи C4I за подводно управление, подводен мониторинг, ситуационна осведоменост, позициониране, навигация и обединяване между водолаз и безпилотни платформи.

II.4.35. ECHO (European network of Cybersecurity center and competence Hub for innovation and Operations, 2019, H2020, European Commision, Международен научен проект (H2020), Институт по отбрана, 2019 г.

Киберзащитата е жизненоважна за просперитета и сигурността. Проектът ECHO има за цел да предостави организиран и координиран подход за подобряване на проактивната киберзащита на Европейския съюз, позволявайки на блока да действа в очакване, защитавайки се от атака срещу компютри и мрежи. ECHO разработва мрежа, чрез която центровете за киберсигурност и компетентност на ЕС могат да бъдат най-добре координирани и оптимизирани. Това ще допринесе за трайно и устойчиво развитие на уменията за киберсигурност, включително засилени изследвания и експерименти за сертифицирани продукти за сигурност, като системи за ранно предупреждение и междусекторни технологични пътни карти.

II.4.36. CyNet - CyNET: Boosting the scientific excellence and innovation capacity in Cyber security of the Bulgarian Defence Institute (Укрепване на научните постижения и капацитет за иновации в киберсигурността на Институт по отбрана „Професор Цветан Лазаров“, Програма "Европейски научни мрежи", МОН, 2020, Международен научен проект, Институт по отбрана, 2020 г.

Целта на проекта е да повиши качеството и мащаба на изследванията в областта на киберсигурността в Института по отбрана, както и да засили връзките между изследователските институции, специализирани в тази област.

II.4.37. CyberTwin, Програма "Европейски научни мрежи", Министерство на образованието и науката, координатор − Университет по библиотекознание и информационни технологии, 2020-2022, Международен научен проект, Институт по отбрана, 2020 г.

Проектът CyberTwin има за цел да повиши изследователския и иновационен капацитет на УниБИТ и неговите български партньори СУ и ИО в областта на киберсигурността и нейните приложения (фокус върху защитата на цифровата информация) чрез работа в мрежа и „побратимяване“ с две международни водещи изследователски институции в тази област. Проектът стимулира трансфера на технологии и отворени иновационни дейности с други пар-

тньори, за да се изгради подходяща иновационна екосистема в областта на киберсигурността. Основният принцип за изграждане на капацитет е „обучение чрез изследване“. Ще бъдат организирани специални семинари за подготовка на предложения и изпълнение на проекти.

II.4.38. Web Intelligence 2019 Workshop - Security Analytics and Threat Detection on the Web, Международна конференция, Член на организационния екип, https://mklab.iti.gr/sacti2019/

Този семинар е фокусиран върху интердисциплинарна изследователска област, включваща уеб разузнаване, информатика за сигурността, анализ на големи данни, „дълбоко“ обучение/машинно обучение и киберсигурност и има за цел да разследва умишлената злоупотреба с техническа инфраструктура за подривни цели, включително (но не само): разпространението на екстремистка пропаганда, антагонистични или омразни коментари; разпространението на зловреден софтуер; онлайн измами и кражба на самоличност; атаки за отказ на услуга; и т.н. По-доброто разбиране на такива явления в мрежата (включително социалните медии) позволява тяхното ранно откриване и е в основата на разработването на ефективни модели за прогнозиране на заплахи за киберсигурността.

II.4.39. Advanced European platform and network of Cybersecurity training and exercises centres - ACTING, Международен научен проект (EDF 2021), Институт по отбрана, 2022 г.

Проектът ACTING предлага организиран и координиран подход за проактивно подобряване на ефективността на обучението и ученията по киберотбрана в Европейския съюз чрез ефективно и ефикасно многосекторно сътрудничество. 28-те партньори от 13 държави-членки, подкрепени от 6 министерства на отбраната. Проектът ACTING интегрира дейности по проучване, проектиране, прототипиране и тестване в областта на киберсигурността. За постигне на добра синхронизация между проекта ACTING и изискванията на министерствата на отбраната, ще бъдат организирани 3 семинара за валидиране.