ISSN 2738-7089 https://doi.org/10.11610/cybsec17bg

Funded by the European Union

ПРОГРАМА НАУЧНИ ИЗСЛЕДВАНИЯ, ИНОВАЦИИ И ДИГИТАЛИЗАЦИЯ ЗА ИНТЕЛИГЕНТНА ТРАНСФОРМАЦИЯ

Digital Innovation Hub Trakia

ИИКТ
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Информационен бюлетин за киберсигурност и информационна устойчивост

Бюлетин Юни 2025 Номер 17

Цели и обхват

Съдържание:

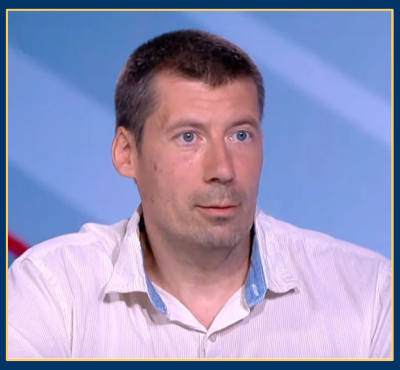
Настоящият брой на информационния бюлетин за киберсигурност и информционна устойчивост е с водеща тема, свързана с федерирането на кибер полигони в България. За осигурявана на надеждна киберсигурност е задължително провеждането на практически обучения чрез кибер полигоните, представляващи специализирани платформи за разработване, доставка и използване на интерактивни симулационни среди, представящи ИКТ, мобилните и физически системи на една организация, включително симулация на атаки, потребители и техните дейности, както и всякакви други услуги, от които симулираната среда може да зависи. В настоящият брой са представени кибер полигона на УНСС, изграден върху отворената платформа KYPO; усилията на Висшето училище по телекомуникации и пощи (ВУТП) за създаване на собствен кибер полигон; възможностите на платформата ThinkCyber Bulgaria и симулатора Cyberium Arena, както и европейския контекст и ролята на ECSO за дефиниране и стимулиране развитието на киберполигони и съвместими европейски платформи. С цел подобряване качеството на обучението по киберсигурност и повишаване на националния капацитет в тази сфера се появява и необподивостта от федериране на съществуващите кибер полигони, които ще позволи да се споделят специфични ресурси или симулации, намиращи се на различни физически локации, като част от едно общо учение или упражнение.

Идеята за федериране на кибер полигоните в България бе подкрепена и на проведена национална кръгла маса на тема „Киберсигурността в защита на хората, образованието и обществото", организирана от Академията на МВР и ВУСИ – Пловдив, в партньорство със Съвета на ректорите на висшите училища. В резултат на срещата е учредена работна група, която да обедини експертизата на висшите училища с оглед изработване на стратегия за развитие на сектора и предложения за нормативни промени. Тази визия предполага бъдеща федерация на кибер полигони – взаимно свързване на инфраструктури и лаборатории между университетите в единна система.

В бюлетина традиционно са представени важни събития и полезни връзки за общността през изминалия тремесечен период..

Редактор на броя: **проф. д.н. Даниела Борисова**

Фокус на изданието: Федериране на кибер полигони в България: Възможности и перспективи



Гл. ас. д-р Иван Благоев
ИИКТ-БАН

В съвременната цифрова ера киберсигурността се утвърждава като критичен компонент за защита на хората, образованието и обществото. В световен мащаб и в Европа се налага практическото обучение чрез кибер полигони – специализирани платформи за симулация на кибератаки и отбрана в контролирана среда. Според дефиницията на Европейската организация по киберсигурност (ECSO) „кибер полигонът е платформа за разработване, доставка и използване на интерактивни симулационни среди, представящи ИКТ, мобилните и физически системи на една организация, включително симулация на атаки, потребители и техните дейности, както и всякакви други услуги, от които симулираната среда може да зависи“. Тези платформи позволяват безопасно тестване устойчивостта на цифровите системи срещу кибератаки и усъвършенстване уменията на специалисти и студенти в реалистична обстановка. През последните години в Европа се появиха множество кибер полигони, някои от които като комерсиални решения с готови сценарии, други с отворени платформи и с по-ограничени вградени функционалности, но безплатни или с ниска цена за потребителите. За крайните ползватели (като университети), изборът на подходящ полигон е сложна задача, затова ECSO разработва насоки и Checklist с ключови характеристики за сравнение на европейските платформи. В България нараства интересът към изграждане на собствени кибер полигони в университети и организации, като целта е подобряване качеството на обучението по киберсигурност и повишаване на националния капацитет в тази сфера. Настоящият анализ разглежда:

- кибер полигона на УНСС, изграден върху отворената платформа KYPO;
- усилията на Висшето училище по телекомуникации и пощи (ВУТП) за създаване на собствен кибер полигон;
- възможностите на платформата ThinkCyber Bulgaria и симулатора Cyberium Arena – нейната архитектура, сценарии, реализъм, обучение и международна сертификация, както и партньорствата с български университети;
- европейския контекст и ролята на ECSO за дефиниране и стимулиране развитието на киберполигони и съвместими европейски платформи.

Готовността на организации като ThinkCyber Bulgaria, УНСС и ВУТП за федериране на разработените полигони в единна система би допринесло не само за споделяне на ресурси, но и за постигане на по-високо качество на обучението, по-добро сертифициране и стандартизация, както и за улесняване на съвместни изследвания и трансфер на знания.

Кибер полигон на УНСС на базата на платформата KYPO

Един от първите практически примери за университетски кибер полигон в България е този на Университета за национално и световно стопанство (УНСС). В последните години УНСС разработва кибер лаборатория, изградена върху отворената платформа KYPO Cyber Range Platform. KYPO (Know Your Enemy), създадена в Масариковия

университет в Чехия по проект CONCORDIA (H2020), е първият европейски отворен код за кибер полигон. Платформата предоставя гъвкава и мащабируема виртуална среда за обучение и упражнения по киберсигурност. Фокусът на KYPO е образованието, поради което е предпочитана от академичните среди, тъй като позволява изграждане на собствени сценарии и упражнения, без лицензионни такси. За внедряването ѝ е необходимо изграждане на частен облак с OpenStack и използване на OpenID Connect за управление на достъпа. Това техническо изискване предполага наличие на първоначална инфраструктура и експертиза, но в замяна изследователите получават пълен контрол върху платформата.

Кибер полигонът на УНСС е представен като част от усилията на университета да обогати практическото обучение по киберсигурност. Базиран на KYPO, той позволява на студентите да се изправят срещу симулирани кибератаки в изолирана среда, възпроизвеждаща реални ИТ инфраструктури. Например, могат да се упражняват сценарии като отразяване на мрежови прониквания, разследване на инциденти, реагиране при рансъмуер атака и др. Отвореният характер на платформата дава възможност на преподавателите от УНСС да разработват учебни сценарии, съобразени с конкретните курсове и актуалните заплахи. Същевременно, KYPO предоставя основни инструменти – виртуализация, изолирана корпоративна мрежа, емулация на интернет среда и атаки, върху които може да се надгражда. Използването на подобна доказана платформа дава на УНСС предимството да предлага обучение, съизмеримо с най-добрите европейски практики, и да участва в обмен на сценарии и опит със сродни академични институции.

Следователно, успехът на кибер полигон, реализиран на KYPO, зависи от активността на инструкторите в създаването и споделянето на съдържание. Ето защо инициативата на Съвета на ректорите за споделяне на ресурси е особено ценна, защото това би позволило да се обменят различни разработени сценарии, виртуални образи на системи и най-добри практики, така че да не се дублират усилията и да се повиши ефективността на обучението.

Усилия на ВУТП за изграждане на собствен кибер полигон

Висшето училище по телекомуникации и пощи (ВУТП) в София е пионер в академичното киберсигурност обучение у нас и е първият университет, който създава бакалавърска програма „Киберсигурност на високите технологии“ още през 2018 г. (с прием на ~60 студенти) и открива специализирана лаборатория по киберсигурност за нуждите на тази програма. Лабораторията, открита с подкрепата на международни партньори, осигурява на студентите достъп до сървъри и мрежово оборудване за изпълнение на практически задачи. В периода след 2018 г. ВУТП продължава да развива материалната си база и експертизата на преподавателите в тази област. През 2025 г. ВУТП застава в центъра на националните усилия за колаборация в киберсигурността, тъй като ректорът проф. Темелкова оглавява Съвета на ректорите и инициира работната група за обединяване на университетските ресурси. В този контекст, следваща стъпка за ВУТП е изграждането на собствен кибер полигон, който да се впише във визията за университетска мрежа. Макар конкретните технически детайли все още да се уточняват, логично е

ВУТП да се насочи към решение, съвместимо с останалите партньори – например внедряване на същата отворена платформа (KYPO) или интегриране с външна платформа чрез партньорство. Действително, Съветът на ректорите обсъжда системно единство между профилираните университети, което предполага известна стандартализация. Затова може да се очаква, че полигонът на ВУТП ще бъде изграден с мисъл за федерация, така че неговите ресурси (сървъри, виртуални среди, сценарии) да могат да се споделят с другите академични полигони.

Академията ThinkCyber Bulgaria и симулаторът Cyberium Arena

Един от ключовите играчи в страната, допринасящ за обучението и подготовката по киберсигурност, е ThinkCyber Bulgaria – организация, която предлага интегрирана тренировъчна платформа от ново поколение. ThinkCyber Bulgaria е част от международната мрежа на ThinkCyber и има амбицията да утвърди България като лидер в киберсигурността в Европа. Основният продукт на ThinkCyber е симулаторът Cyberium Arena – цялостна, динамична обучителна платформа, захранвана от иновативната технология Specto. Като основни акценти на симулатора могат да се разглеждат неговия концептуален модел и архитектура на Cyberium Arena, реализъмът на сценариите, възможностите за обучение и сертифициране, както и взаимодействието с българските университети.

Концептуален модел и сценарии на Cyberium Arena

ThinkCyber разработва свой обучителен модел, комбиниращ теория, практика и реалистични симулации, с цел да развива както техническите, така и аналитичните умения на участниците. В основата на модела са сценариите, базирани на реални заплахи – симулират се инциденти като рансъмуер атаки, пробиви в мрежата или уязвимости във веригата на доставки въз основа на реални случаи, анализирани чрез платформата Specto AI. По този начин съдържанието непрекъснато се обновява спрямо най-новите хакерски техники, гарантирайки, че обучаемите се изправят пред съвременни предизвикателства.

В симулациите участниците влизат в различни интерактивни роли, например нападател (офанзивен), защитник (синия екип) или анализатор на дигитални следи. Чрез подхода „учене чрез правене“ те развиват практически умения за вземане на решения и стратегическо мислене, необходими в динамичната област на киберсигурността. Платформата интегрира и елемент на обучение в реално време – Specto технологията представлява глобална мрежа от honeypot-ове (капани за атаки), които събират данни за атаките по света и ги анализират. Тези актуални заплахи могат да бъдат внедрени в сценариите на Cyberium Arena почти незабавно. Реалновременната интеграция означава, че обучаемите работят с най-актуалната информация за противниковите техники, вместо само да се базират на исторически данни. В резултат, симулациите доближават максимално реалността - например, ако в момента се наблюдава нов тип фишинг кампания или уязвимост в популярна система, платформата може да включи аналогичен инцидент в упражненията.

ThinkCyber обогатява обучението и чрез допълнителни ресурси: участниците имат достъп до лабораторни упражнения (labs), които им

позволяват практическо пробване на инструменти в безопасна среда, както и до проекти, изискващи разработка на собствени скриптове или мини-инструменти за киберзащита. Налице е и богат набор от учебни материали (книги, видеа, примери от реални проекти), които подпомагат усвояването на знанията. Обучението е структурирано модулно, с възможност за прогресия от основни към все по-сложни задачи, което дава гъвкавост според нивото на аудиторията.

Особено нововъведение на Cyberium Arena е системата за оценка и обратна връзка. Всеки обучителен модул включва механизми за оценяване, сред които ключов е Cyberium Effectiveness Score (CES) – интегриран показател, който измерва ефективността и адаптивността на участниците. CES агрегира различни измерители на представянето – отбранителни умения, офанзивни умения, умения за разследване, време за реакция, активност, успешно изпълнени задачи и др., за да формира глобален индекс на ефективността. Например, в един сценарий може да се отчита колко бързо и точно е реагирал даден екип на инцидент, колко атаки е предотвратил и дали е идентифицирал първопричината на пробива. Системата генерира персонализирани отчети и препоръки – посочва силните и слаби страни на участника и дава насоки за подобрение. По този начин обучаемите не само преминават през упражнения, но и ясно разбират къде да се усъвършенстват, което стимулира непрекъснато подобрение на уменията.

Европейски контекст и роля на ECSO в развитието на кибер полигони

В европейски мащаб интересът към кибер полигоните бележи значителен ръст, подкрепен от политики и инициативи на ЕС. European Cyber Security Organisation (ECSO), като водеща пан-европейска асоциация в сферата, има ключова роля за обединяване на усилията около кибер тренировъчните среди. ECSO създава специализирана общност – European Cyber Range Community, към която могат да се присъединят доставчици и ползватели на кибер полигони. Целите на тази общност са консолидация на подходите при услугите, базирани на полигони, създаване на добри практики и насоки, които да дефинират „Европейския кибер полигон“, както и стимулиране на внедряването на подобни платформи в различни сектори.

Конкретен принос на ECSO е изготвянето на Checklist с ключови характеристики на кибер полигоните, представен като удобен инструмент за крайни ползватели (например университети, компании, държавни агенции) при формулиране на изисквания и критерии за избор на платформа. Този списък обхваща функционалности като типове поддържани сценарии (образование, тренинг, тестване, състезания и т.н.), мащабируемост, надеждност, режим на внедряване (локален, облачен, хибриден) и много други аспекти. Чрез стандартизиране на критериите, ECSO улеснява организациите в Европа да изберат подходящи решения според нуждите си, като едновременно с това поощрява местните европейски доставчици. Действително, част от мисията на ECSO е да изгради каталог на европейските доставчици на кибер полигони – за пръв път да бъде събран на едно място списък на тези платформи и техните характеристики. По този начин, ако даден университет търси решение, той може да се информира за налични продукти (както комерсиални, така и отворени) в рамките на ЕС, вместо да прибягва към изцяло

външни (например американски) платформи. Това е в синхрон с общата стратегия за цифров суверенитет на ЕС – да се използват и развиват собствени технологии, особено в ключова област като киберсигурността.

Друг аспект на европейския контекст е насърчаването на съвместими и свързани полигони. Проекти като CONCORDIA, CyberSec4Europe и др. в рамките на програма „Хоризонт 2020“ работят върху изграждане на мрежи от федеративни киберлаборатории. Самата идея за федериране се ражда от нуждата да се достъпват специфични ресурси или симулации, намиращи се на различни физически локации, като част от едно общо учение или упражнение. Например, при мащабно кибер учение може да е необходимо включването на симулация на електроенергийна мрежа, хоствана в лаборатория на един университет, и едновременно с това симулация на телекомуникационна мрежа, намираща се в друг център. Федерацията на кибер полигони позволява такъв тип интероперативност – множеството отделни платформи да работят заедно като една, обменяйки данни и сценарии в реално време. ECSO признава важността на тази концепция и чрез общността си стимулира разработването на решения за автоматизирано свързване на полигони (напр. чрез стандартни протоколи за VPN тунели, споделяне на сценарни обекти и др.).

В резултат на европейските усилия, редица държави членки вече изграждат собствени национални кибер тренировъчни центрове, често подкрепени от фондове на ЕС. За България, която участва активно в инициативи като Европейския център по компетентност в киберсигурността, присъствието на добре развити полигони (като тези на УНСС, ВУТП и партньорски организации) означава, че страната ни може да се включи пълноценно в пан-европейски учения и изследователски проекти. ECSO предоставя платформа за видимост на българските постижения: например, ако обединената българска университетска мрежа от полигони предложи иновативен модел (федерация между академия, бизнес и др.), тя би могла да бъде включена в каталога на успешните европейски примери. Обобщено, европейският контекст задава рамката, в която българските институции развиват своите кибер полигони. ECSO действа като катализатор за стандартизация, сътрудничество и обмен на знания, което резонира пряко с целите, поставени на националната кръгла маса у нас – обединяване на усилията в името на по-добра киберзащита на обществото.

Заключение: България разполага с основните градивни елементи на една силна киберсигурност екосистема: университети с инициатива и инфраструктура (УНСС, ВУТП и др.), иновативна частна платформа (ThinkCyber Cyberium Arena) и подкрепящ европейски контекст (ECSO, отворени проекти). Следващата логична стъпка е тези отделни елементи да се свържат във федеративна система. Използването само на един отделен кибер полигон често не е достатъчно, когато имаме нужда от достъп до разнородни технологии и среди – затова възниква необходимостта да се свържат множество полигони, което е в основата на разбирането на “федерирането на кибер полигони”.

Организациите ThinkCyber Bulgaria, УНСС и ВУТП демонстрират готовност и капацитет да реализират подобна федерация. Първите

стъпки вече са налице: съгласието за споделяне на ресурси, изразено на национално ниво, и техническата възможност за интеграция между различни платформи. Очертават се няколко ключови ползи от колаборацията в единна система:

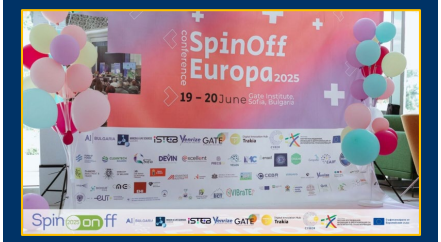
- Споделяне на ресурси и инфраструктура: Федерацията ще позволи различните институции да си споделят хардуерните и софтуерни ресурси. Например, ако УНСС има излишен капацитет на сървърите си, той би могъл да бъде използван от ВУТП при провеждане на мащабно учение, и обратно. Сценарии, разработени в един университет, ще бъдат достъпни и за останалите, което елиминира дублирането на усилия. Този подход наподобява cloud federation – общият „облак“ от кибер полигони ще е по-мощен и богат на съдържание от всяка единична лаборатория.
- По-високо качество на обучението и симулациите: Когато се обединят най-добрите практики и експертиза от различни организации, се постига синергичен ефект върху качеството на обучението. Студентите ще имат достъп до разнообразие от упражнения – от високореалистичните сценарии на Cyberium Arena с най-новите заплахи, до специализирани академични кейсове, разработени от водещи преподаватели. Също така, ще станат възможни по-големи съвместни учения – например екипи от различни университети да тренират заедно в симулирана национална кибер криза, което силно би повишило подготовката им за реални ситуации.
- По-добро сертифициране и стандартизация: Единната система ще улесни въвеждането на общи стандарти за оценка и сертифициране. Ако всички използват сходни метрики (напр. CES от Cyberium или други договорени показатели), сертификатите, издавани на обучаемите, ще бъдат съпоставими и прозрачно заслужени. Това повишава доверието на работодателите и международната общност в тези сертификати. Българските университети биха могли дори да създадат консорциум за сертифициране, признаващ постиженията на студентите, които са тренирали на федеративния полигон. Стандартизацията ще обхване и самите платформи: чрез общата работа ще се изработят най-добри практики за настройка на полигони, за изграждане на сценарии, за безопасност при симулациите и пр., които всички членове на федерацията ще спазват.
- Улесняване на съвместни изследвания и трансфер на знания: Федерацията неизбежно ще сближи различните заинтересовани страни – академични, студенти, бизнес експерти. Това създава плодородна среда за научно сътрудничество. Изследователски екипи от няколко университета могат да ползват общата инфраструктура за експерименти, да споделят данни от симулации и да тестват хипотези в по-голям мащаб. Например, ако един екип разработва нов метод за откриване на APT (напреднала персистентна заплаха), той би могъл да го валидира върху разнообразни сценарии, достъпни във федеративния полигон, и с различни групи участници, което дава по-обективни резултати. Трансферът на знания също ще се ускори – когато една институция създаде нов сценарий или техника на обучение, тя лесно може да бъде предадена на останалите чрез споделената

платформа. Това отговаря и на ангажимента, поет от проф. Темелкова, да се провокират разговори и превенция относно опасностите в киберпространството чрез създаване на университетски мрежи за споделяне.

Следователно, федерирането на кибер полигоните на ThinkCyber, УНСС, ВУТП (потенциално и други в бъдеще) в единна система може да се разглежда като стратегически ход, който ще позиционира България на преден план в подготовката на кадри и иновации по киберсигурност. Реализирането на тази визия несъмнено ще изисква координация, доверие и техническа работа – например създаване на общ инфраструктурен план, осигуряване на сигурни връзки между обектите (VPN тунели, съвместими интерфейси), договорки за управление и споделяне на данни и пр. Международният опит обаче показва, че подобни усилия са оправдани: обединените кибер полигони предоставят мащаб и разнообразие, невъзможни за отделните единици. В условията на ескалиращи кибер заплахи и недостиг на квалифицирани специалисти, България може да противопостави единен фронт в обучението по киберсигурност, където университети и индустрия заедно изграждат следващото поколение кибер защитници. Това е инвестиция с дългосрочна възвръщаемост – по-сигурно дигитално общество, повишена кибер устойчивост на национално ниво и утвърждаване на страната като активен участник в европейската кибер екосистема.

Работата по проекта ECHO (един от четирите пилотни проекта на ЕК за изграждане на екосистема за киберсигурност, заедно с CONCORDIA, CS4Europe и SPARTA – обединение в Convergence) и EDIH-Trakia (CYBER4All STAR Project) създава условия за подкрепа на концепцията за асоциация на академични CERT екипи (ACERTA) като основа за устойчивост в академичната среда и модел за киберустойчивост в други сектори.

Европейски цифрови иновационни дни SpinOFF



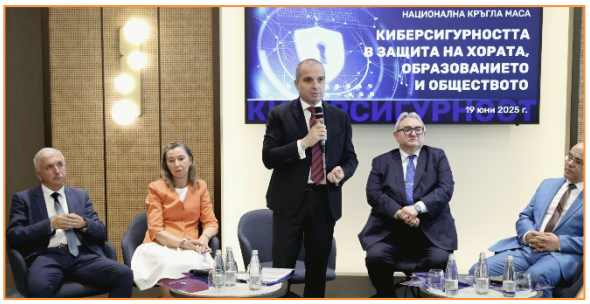
На 19 и 20 юни 2025 бяха проведени консултантски събития “Европейски цифрови иновационни дни SpinOff” организирани от Европейският цифров иновационен хъб „Тракия“, Клъстер „Здраве и науки за живота“ България и Клъстер за изкуствен интелект България, където бяха посрещнати от Институт GATE. Събитието беше посетено от над 200 участници.

В серия от силни встъпителни лекции, Дарио Зорич от външното министерство на Дания представи визията за Европейската дигитална идентичност, Стефан Добрев от Европейския институт за иновации и технологии (EIT) очерта ролята на иновациите за конкурентоспособна Европа, а доц. д-р Боян Жеков акцентира върху новите възможности по програмата Хоризонт Европа.

Програмата на събитията включваше не само основни, но и паралелни работилници и КиберТех зона за практически консултации. Програма на “Европейски цифрови иновационни дни SpinOFF” предложи не просто лекции, а завладяващ микс от визионерски идеи, практически инструменти и силни лични истории, които показаха реалния път от иновационната концепция до пазарната реализация.

Пълният текст може да прочетете тук.

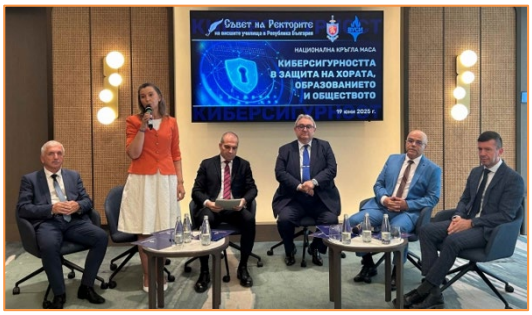
Национална кръгла маса „Киберсигурността в защита на хората, образованието и обществото“



На 19 юни 2025 г. в София се провежда национална кръгла маса на тема „Киберсигурността в защита на хората, образованието и обществото“, организирана от Академията на МВР и ВУСИ – Пловдив, в партньорство със Съвета на ректорите на висшите училища.

Форумът привлича ръководители от образованието, държавни институции и експерти от бизнеса, и цели да постави начало на ефективен диалог по проблемите и предизвикателствата в сектора. В дискусиите се подчертава, че университетите вече предлагат различни програми по киберсигурност и не бива да се разглеждат като конкуренти, а като партньори, които трябва да си сътрудничат.

Кулминацията на кръглата маса бе призивът за обединение на усилията между университетите в областта на киберсигурността. Проф. Георги Манолов (президент на ВУСИ) призовава да се създаде консорциум от български университети, обучаващи в тази сфера.



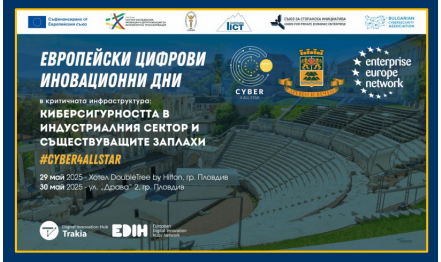
В подкрепа на тази идея, проф. д-р Миглена Темелкова – председател на Съвета на ректорите (и ректор на ВУТП), обявява учредяването на работна група към Съвета, която да обедини експертизата на висшите училища с оглед изработване на стратегия за развитие на сектора и предложения за нормативни промени. Споделянето на ресурси се откроява като основен акцент: проф. Темелкова подчертава, че ще бъдат изградени първите университетски мрежи за споделяне на ресурси, тъй като „всеки университет е профилиран и може да се изгради едно системно единство“. Тази визия предполага бъдеща федерация на кибер полигони – взаимно свързване на инфраструктури и лаборатории между университетите в единна система. В резултат от форума, висшите училища се консолидират около разбирането, че споделените платформи за обучение и симулация ще повишат качеството на подготовката по киберсигурност в национален мащаб.

За сблъсъка в киберпространството и ресурса да отблъснем кибер атаките

На 19 юни 2025 г. в предаването на БТВ „Лице в лице“ гост бе гл. асистент д-р Иван Балгоев – сертифициран експерт в областта на киберсигурността от ИИКТ-БАН.

Запис на интервюто с гл. асистент д-р Иван Балгоев може да гладате тук.

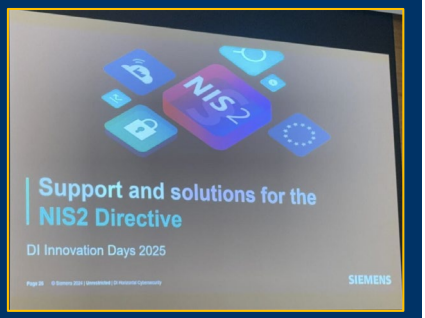
Експертни дискусии за критичната инфраструктура



На 29 и 30 май 2025 бяха проведени консултантски събития “Европейски цифрови иновационни дни в критичната инфраструктура – киберсигурността в индустриалния сектор и съществуващите заплахи” организирани от Община Пловдив и ЕЦИХ “Тракия”, с подкрепата на Търговско-промишлена камара – Пловдив по проект Cyber4AllSTAR, които бяха посветени на киберсигурността в индустриалните предприятия, основните отрасли, които поддържат жизненоважните функции на обществото.

Пълният текст може да прочетете тук.

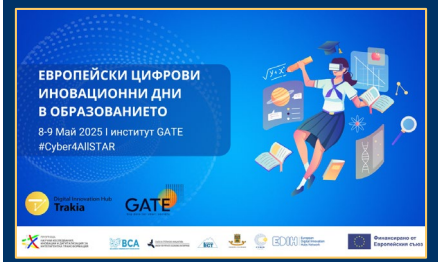
Innovation Days 2025



На 20 май 2025 г. в Пловдив се проведе Innovation Days 2025 – технологичен форум, организиран от Siemens България, с фокус върху фабричната автоматизация (Factory Automation), движение и контрол (Motion Control), процесна автоматизация (Process Automation) и електрически продукти. Събитието събра клиенти, партньори и индустриални експерти, като предложи практически работилници и възможности за нетуъркинг в съвременна индустриална среда. Сред участниците беше и експертът Денис Петков от ЕЦИХ “Тракия” (Европейски цифров иновационен хъб „Тракия“), който подкрепи партньорите на Siemens и по време на нетуъркинг сесиите представи проекта CyberSec4OT пред представители на индустрията.

Пълният текст може да прочетете тук.

Европейските цифрови иновационни дни в образованието



На 8 и 9 май 2025 г. Институт GATE към Софийския университет „Св. Климент Охридски“ (СУ) бе домакин на специалните консултантски събития „Европейски цифрови иновационни дни в образованието“, част от проекта Cyber4AllSTAR.

В двудневния форум присъстваха представители на държавни институции, академичната общност, бизнеса и гражданското общество, събитието се превърна във водеща платформа за обмяна на опит, идеи и иновативни практики за цифрова трансформация на образованието.

Пълният текст може да прочетете тук.

ЕЦИХ Тракия подписа споразумение с испанския DIGIS3

На 22 април 2025 г. финализирахме подписването на споразумение за сътрудничество с испанския Европейски цифров иновационен хъб (ЕЦИХ) за Интелигентни, устойчиви и сближаващи дигитални услуги – Smart, Sustainable and coheSive Digitalization/DIGIS³. Споразумението е в резултат на дългогодишно сътрудничество и с него Cyber4ALLSTAR, ЕЦИХ Тракия вече има подписани осем споразумения за сътрудничество с хъбове и организации.

DIGIS3 хъб се координира от AIR INSTITUTE и е подкрепен от Regional Government of Castile and León. Хъбът е стратегически партньор и обединява 6 организации, които са важни за региона: ICE, с отговорности за публичните инвестиции, финансиране и интернационализация на МСП, IoTDIH, DIHBU и DIHLEAF – 3 фунциониращи цихфрови хъба, заедно с 13 асоциирани отганизации; SCAYLE, регионалния център за HPC и ULe, като обучителен център за напреднали цифрови умения. В периода 10-11.6.2025 г. бяха проведени консултации с екип на ЕДИХ-Тракия за развитие на каталога от услуги и бизнес модела на двата хъба.

В началото на юни, 2025 година, д-р Ирена Младенова и доц. Георги Пенчев от екипа на ИИКТ-БАН, участващ в изпълнението на проект CYBER4All STAR се срещнаха с представители на EDIH DIGIS3 в Саламанка, Испания. Срещите се състояха в AIR Institute – координиращата организация на Цифровия хъб. Срещите в гр. Саламанка бяха ръководени от Йохана Морено Кателанос от Университета на Саламанка и Лаура Гранде Перез от AIR Institute, като участваха представители на ръководството на AIR Institute, Университета на Саламанка и DIGIS3. В резултат на организираните срещи беше подписан Меморандум за сътрудничество между CYBER4All STAR и DIGIS3.

Пълният текст може да прочетете тук.

Връзки към събития по киберсигурност

- Open Source Summit, 25-27 Август, 2025, Амстердам
- Nordic Cyber Summit, 10-11 Септември 2025, Копенхаген
- Gartner Security & Risk Management Summit 2025, 22-24 Септември 2025, Лондон

Редакционен съвет

Публикуването на настоящия брой на бюлетина се реализира с финансовата подкрепа на проект: **#101083793 – CYBER4All STAR – DIGITAL-2021-EDIH-01 на ЕК**