ISSN 2738-7089 https://doi.org/10.11610/cybsec20bg

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 Март 2026 Номер 20

Цели и обхват

Съдържание:

Настоящият брой на информационния бюлетин за киберсигурност и информационна устойчивост представя следващата фаза на развитие на Европейския цифров иновационен хъб „Тракия“ – Cyber4All 2.0 (2026-2028). Фокусът е върху надграждането на съществуващия капацитет чрез развитие на мащабируем модел на услуги с измерим ефект в областта на цифровата трансформация и киберсигурността.

Изданието обхваща целите на проекта, модела и портфолиото от услуги, организирани в четири основни направления. Специално внимание е отделено на ролята на екосистемата и трансграничното сътрудничество. Представени са и очакваните резултати и въздействие, свързани с повишаване на информационната и кибер устойчивост на организациите.

В рамките на изданието се разглеждат и ключови теми, свързани с развитието на нормативната рамка и практическите аспекти на киберсигурността. Отделено е внимание на прилагането на Директивата NIS2 в България, като се представят основните изисквания и тяхното отражение върху организациите. В тази връзка са включени и примери за практически инициативи и събития, насочени към подпомагане на бизнеса и публичния сектор, сред които серията семинари по проект OSCRAT и събитието e-Future 3.0. Те илюстрират приложния характер на дигиталната трансформация и управлението на риска.

Специално внимание е отделено на развитието на образованието и изграждането на капацитет в областта на киберсигурността. Разгледани са нови образователни възможности, интегриращи киберсигурност и AI, както и инициативи за изграждане на професионални общности, като Women4Cyber Bulgaria. Представени са и специализирани каталози на образователни програми.

Изданието включва и преглед на актуалните тенденции при кибератаките от началото на 2026 г., както и информация за предстоящите събития.

Редактор на броя: **ас. д-р Зорница Димитрова**

Фокус на изданието: Нова фаза в развитието на ЕЦИХ „Тракия“: Cyber4All 2.0

ас. д-р Зорница Димитрова

След успешното изпълнение на проекта CYBER4All STAR, Европейският цифров иновационен хъб (ЕЦИХ) „Тракия“ навлиза в нов етап на развитие – Cyber4All 2.0 за периода 2026-2028 г. Новата фаза представлява естествено продължение и надграждане на вече функциониращa и утвърдена структура. Тя стъпва върху изградени партньорства, утвърдено портфолио от услуги и натрупан практически опит в работата с бизнес и публични организации.

Към началото на новия етап хъбът вече е обслужил над 100 организации от публичния и частния сектор, извършил е десетки оценки на дигиталната зрялост и е подкрепил над 120 участници в иновационната екосистема чрез обучения. Натрупаният опит очертава преход от пилотно предоставяне на услуги към по-структуриран и мащабируем модел. Cyber4All 2.0 поставя акцент върху развитието на стандартизирани и модулни услуги, които позволяват лесно комбиниране, надграждане и адаптиране към конкретните нужди. Стремежът е към постигане на устойчиво въздействие върху информационната и кибер устойчивост на организациите, особено в уязвими сектори и региони. Основните целеви групи включват малки и средни предприятия (МСП); публични институции (администрации и общини); научни и образователни организации; неправителствени организации (НПО); стартиращи и иновативни компании; индустриални предприятия; както и професионални общности и специалисти в областта на цифровите технологии и киберсигурността.

Развитието на Cyber4All 2.0 е в съответствие с приоритетите на Програмата „Цифрова Европа“ в областта на цифровата трансформация, киберсигурността и внедряването на иновативни технологии, включително изкуствен интелект. В този контекст хъбът допринася за укрепване на националния капацитет и за по-добра интеграция в мрежата от европейски цифрови иновационни хъбове.

Цели на Cyber4All 2.0

Целта на проекта е насочена към системно подпомагане на организациите чрез интегриран набор от дейности, обхващащи технологични, организационни и обучителни аспекти. Те отразяват необходимостта от координиран подход към цифровата трансформация и киберустойчивостта, като поставят акцент върху практическото прилагане на решения и постигането на измерими резултати.

Задачите за постигане на целта са свързани с:

- предоставяне на услуги за цифрова трансформация;
- повишаване нивото на дигитална и кибер зрялост на организациите;
- ускоряване внедряването на иновативни технологии, включително решения, базирани на изкуствен интелект;
- изграждане на лаборатория по информационна устойчивост;
- подпомагане достъпа до финансиране и инвестиции;

- трансгранично предоставяне на услугите;
- засилване връзките между участниците в иновационната екосистема.

Целите на Cyber4All 2.0 са съгласувани с ключови европейски регулации в областта на киберсигурността и цифровите технологии, включително NIS2 Directive, Cyber Resilience Act и AI Act. Те са обвързани и с по-широките цели на Европейския съюз, формулирани в рамките на Digital Decade, както и с инициативи за развитие на цифровата икономика като Startup Europe и дейностите на ENISA.

Услуги в Cyber4All 2.0

Предоставянето на услуги в Cyber4All 2.0 е организирано в съответствие с подхода на Програмата „Цифрова Европа“ и обхваща четири основни направления, които определят обхвата и структурата на дейностите. Услугите включват следните 4 взаимодопълващи се направления:

(1) тестване и валидиране на решения преди внедряване (Test Before Invest / Try Before Buy (TBI/TBB));
(2) развитие на умения и обучения (Skills Development);
(3) подкрепа за достъп до финансиране и инвестиции (Access to Finance);
(4) осигуряване на участие в екосистеми и партньорски мрежи (Ecosystem-as-a-Service).

В рамките на тези направления услугите се предоставят като координирани дейности, обхващащи различни етапи от процеса на цифрова трансформация – от оценка и тестване до внедряване и развитие.

Планираните услуги следват принципа на **модулност**, при който отделните услуги са структурирани като самостоятелни компоненти, които могат да се комбинират в зависимост от специфичните потребности на организацията. Това позволява гъвкаво прилагане към различните целеви групи и същевременно при различно ниво на зрялост на организациите.

В същото време начинът, по който е планирано представянето на услугите се определя като **мащабируем**, тъй като позволява

предоставянето на едни и същи услуги към по-широк кръг организации при запазване на тяхната структура и качество. Това се постига чрез стандартизиране на процесите и използване на повтаряеми подходи при предоставянето на услугите.

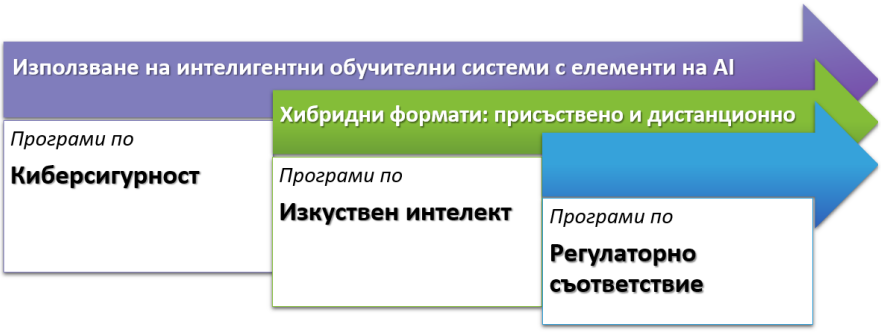
Този подход позволява бързо и гъвкаво адаптиране към специфичните потребности на потребителите и създава условия за последователно и устойчиво развитие на организациите.

Портфолио от услуги

Cyber4All 2.0 надгражда съществуващото портфолио от над 20 услуги, насочени към реалните нужди на организациите.

В рамките на първото направление **TBI/TBB** се предлагат услуги, които осигуряват достъп до тестови среди за експериментиране, симулиране и техническа диагностика. Те включват оценка на дигиталната зрялост, анализ на готовността за внедряване на AI, сканиране за уязвимости и тестове за проникване, както и използване на специализирани среди като киберлаборатория и AI Sandbox.

Този пакет е насочен към две основни групи. От една страна, той подпомага доставчиците на технологични решения, като им предоставя подкрепа на различни етапи, от съвместно разработване и експериментиране до пилотно внедряване. От друга страна, пакетът е предназначен и за организации потребители, които преминават през цялостен анализ на своите нужди и възможности в областта на дигитализацията, автоматизацията и киберсигурността.



Услугите, включени във второто направление **Skills Development**, целят да преодолеят недостига на умения чрез практически и модулни обучения. Предлагат се програми в областта на киберсигурността, изкуствения интелект и съответствие с регулаторните изисквания.

Обученията се провеждат чрез съвременни методи, включително използване на интелигентни обучителни системи с елементи на изкуствен интелект, онлайн платформи и комбинирани присъствено-дистанционни формати. Това позволява адаптиране на съдържанието към различни нива на подготовка и специфичните нужди на участниците.

Третото направление **Access to Finance** е насочено към подпомагане на организациите при осигуряването на финансиране за внедряване на цифрови решения. Услугите включват информиране за възможности за финансиране, анализ на нуждите от финансиране и разработване на стратегия. В допълнение се извършва оценка на инвестиционната готовност и предоставяне на консултации чрез HelpDesk. Осигурява се и посредничество с инвеститори и финансиращи организации.

По този начин се подпомага не само достъпът до информация, но и цялостната подготовка и успешното им позициониране пред различни източници на финансиране.

Четвъртото направление **Ecosystem-as-a-Service** разширява обхвата на подкрепата, като свързва организациите с партньори, мрежи и инициативи в областта на цифровите технологии. Услугите включват подпомагане при изграждане на партньорства, участие в професионални събития, както и провеждане на специализирани работни срещи и анализи. Осигурява се достъп до европейски и национални мрежи, технологични инфраструктури, изследователски инициативи и бизнес екосистеми.

Чрез развиване на концепцията „ecosystem-as-a-service“ се създават условия за трансгранично разширяване на услугите. Това позиционира хъба като посредник и координатор, който подпомага организации да се ориентират и да участват активно в мрежата от европейски програми, инфраструктури и партньорства.

Портфолиото от услуги осигурява цялостна и координирана подкрепа, която обхваща всички ключови етапи от цифровата трансформация.

Екосистема и трансгранично сътрудничество

Cyber4All 2.0 значително разширява ролята на хъба като активен участник в европейската иновационна екосистема чрез включване в

паневропейски мрежи, технологични платформи и координационни механизми.

В основата на този подход е участието в Европейската мрежа на цифровите иновационни хъбове към Европейската комисия (EDIH Network), която осигурява рамката за трансгранично предоставяне на услуги и сътрудничество между хъбовете. Координацията на дейностите се подпомага от Digital Transformation Accelerator (DTA), който осигурява синхронизация, обмен на добри практики и методическа подкрепа на европейско ниво.

В технологичен и инфраструктурен аспект хъбът осигурява достъп до ключови европейски ресурси като AI-on-Demand Platform, която предоставя инструменти и услуги за внедряване на изкуствен интелект. Както и до AI Factories, Testing and Experimentation Facilities (TEFs) и European Data Spaces, които подпомагат тестването, валидирането и използването на данни и технологии в реални условия.

В областта на киберсигурността проектът се свързва с организации като ENISA и ECSO (European Cyber Security Organisation), която обединява индустрията, научните среди и публичния сектор.

От гледна точка на бизнес развитие и интернационализация, хъбът работи с мрежи като Enterprise Europe Network (EEN) и инициативи като Startup Europe, които подпомагат изграждането на партньорства, достъпа до пазари и развитието на иновативни компании.

Чрез тази интегрирана екосистема Cyber4All 2.0 създава условия за ефективно трансгранично сътрудничество, като предоставя на организациите достъп до знания, добри практики, технологии, партньори и възможности за развитие в европейски мащаб.

Очаквани резултати и въздействие

Една от ключовите характеристики на Cyber4All 2.0 е ориентацията към резултати, които могат да бъдат ясно измерени и проследени. За тази цел проектът използва структурирана система от индикатори, съгласувана с KPI рамката на Европейската комисия и DTA.

В рамките на периода 2026-2028 г. се предвижда:

- достигане до минимум 100 организации от публичния и частния сектор;
- реализиране на над 500 предоставяния на услугите от портфолиото;
- обучение на минимум 300 специалисти чрез различни форми на обучение;
- мобилизиране на инвестиции в размер на поне 3 млн. евро в областта на дигиталната трансформация и киберсигурността;
- повишаване нивото на дигитална и кибер зрялост на поне 90% от подпомогнатите организации;
- разширяване на трансграничното сътрудничество чрез участие в европейски мрежи и инициативи.

Очакваното въздействие на Cyber4All 2.0 се основава на връзката между предоставяните услуги, постигнатите резултати и поставените цели. Чрез системното прилагане на модулния и мащабируем модел на услугите се създават условия за устойчиво повишаване на информационната и кибер устойчивост на организациите. Проектът допринася за по-широко внедряване на иновативни технологии, по-добра готовност за посрещане на регулаторни изисквания и засилване на инвестиционната активност в областта на цифровата трансформация и киберсигурността. В дългосрочен план това води до укрепване на националния капацитет и по-ефективно интегриране в европейската иновационна екосистема.

Директивата NIS2 в България: Ключови аспекти на новата регулация

През февруари 2026 г., след закъснение от повече от една година спрямо крайния срок на ЕС (17 октомври 2024 г.), България направи решаваща стъпка към прилагането на NIS2 чрез изменения в Закона за киберсигурност. Анализите по темата са единни, че това е най-съществената промяна в националната рамка по киберсигурност от 2018 г. насам. Новият режим значително разширява обхвата на задължените организации и въвежда по-строги изисквания за управление на риска. В същото време киберсигурността се утвърждава като управленски и бизнес въпрос, а не само като техническа функция.

Най-важните промени за организациите са обобщени както следва:

- **Разширен обхват (18 сектора)** – режимът вече обхваща не само критичната инфраструктура, а и средни и големи организации в ключови сектори като енергетика, транспорт, здравеопазване, финанси, цифрова инфраструктура, публична администрация и производство. Въвежда се разграничение между „съществени“ и „важни“ субекти, от което зависят надзорът и санкциите;
- **Задължения за управление на риска** – изисква се прилагане на цялостни, рисково-базирани мерки, включително управление на инциденти, непрекъснатост на дейността, сигурност на веригата на доставки, управление на уязвимости, криптография и контрол на достъпа. Въвежда се и задължение за регистрация в специализиран регистър;
- **Строги срокове за докладване** – при значителен инцидент се въвежда етапен режим за уведомяване: до 24 часа (ранно предупреждение), до 72 часа (официално уведомление) и до 1 месец (окончателен доклад);
- **Засилена роля на ръководството** – ръководните органи носят пряка отговорност за одобряване и контрол на мерките за киберсигурност, което издига темата на стратегическо управленско ниво;
- **Санкции и преходен период** – санкциите са значително увеличени и могат да достигнат до 10 млн. евро или 2% от глобалния оборот за съществени субекти (и до 7 млн. евро или 1,4% за важни). Предвиден е преходен период , в рамките

на който до 1 юни 2026 г. санкциите се прилагат в намален размер.

В допълнение, до август 2026 г. се очаква да бъдат определени компетентните органи по сектори, което ще бъде ключово за практическото прилагане на новия режим.

Общият извод е, че NIS2 не следва да се разглежда единствено като нормативно задължение. Тя изисква изграждане на цялостен модел за киберустойчивост, който обхваща управление, процеси, доставчици, документация и готовност за реакция при инциденти. В този смисъл 2026 г. бележи преход от формално транспониране към реална подготовка за съответствие.

Още по темата може да прочетете тук.

Семинари по киберрегулации в рамките на проект OSCRAT

В периода януари – март 2026 г. ЕЦИХ „Тракия“ проведе серия от три онлайн семинара по проект OSCRAT, насочени към подпомагане на МСП при прилагането на изискванията на Законодателния акт за киберустойчивост (Cyber Resilience Act – CRA).

Поредицата започна на 28 януари 2026 г. със семинар, посветен на изискванията за техническа документация, оценка на приложимостта на продуктите и подготовка на одитни доказателства. На 23 февруари 2026 г. второто събитие разгледа управлението на инциденти, включително създаване на детайлни отчети и осигуряване на проследимост. Третият семинар, проведен на 30 март 2026 г., беше фокусиран върху управлението на уязвимости и демонстрира практически подходи за тяхното идентифициране и контрол чрез инструментите на OSCRAT.

Семинарите предоставиха експертни насоки и практически демонстрации, които подпомагат организациите при разбирането и прилагането на регулаторните, техническите и документалните изисквания на CRA, както и при използването на платформата OSCRAT за улесняване на процеса по съответствие.

Предстоящо събитие:

Финалният семинар от поредицата ще се проведе на 27 април 2026 г. и ще бъде посветен на управлението на риска. В рамките на събитието ще бъдат разгледани процесите по идентифициране и приоритизиране на рисковете, както и подходите за тяхното третиране с цел постигане на пълно съответствие с изискванията на CRA.

e-Future 3.0: Дигитализация и иновации в Payroll, HR и счетоводството

На 24 март 2026 г. се проведе e-Future 3.0 – събитие на Sb Accounting & Consulting, което събра експерти от областта на възнагражденията, човешките ресурси и счетоводната отчетност. Тазгодишното издание постави акцент върху интегрирания подход към управлението на процеси в условията на дигитализация и нарастващи регулаторни изисквания.

Програмата беше ориентирана към практически решения и реални казуси, като обхвана теми като информационна сигурност, автоматизация, ESG в HR, равнопоставеност в заплащането, както и трансформацията на счетоводната функция. Представени бяха и конкретни насоки за внедряване на SAF-T отчетност, практични насоки за Pillar II и подготовка за ViDA, както и предизвикателства при трансферното ценообразуване.

Събитието подчерта значението на технологиите и практическите подходи за постигане на устойчиви и предвидими резултати в ежедневната работа.

Киберсигурност и AI – интегриран подход в образованието у нас

От началото на 2026 г. в България се наблюдава ясно изразена тенденция към разширяване на образователните възможности в областта на киберсигурността, все по-често в комбинация с изкуствен интелект. Това отразява както развитието на технологиите, така и нарастващата нужда от подготвени специалисти.

В държавния план-прием за 2026/2027 г. се разкриват нови специализирани паралелки в професионалните гимназии, включително в Пловдив, Стара Загора и Бургас, с фокус върху ИТ и киберсигурност.

В допълнение към средното образование и с фокус върху превенцията на кибер-престъпленията беше открит нов STEM център в ПГ по МСС „Пейо К. Яворов“ в Гоце Делчев. Центърът изпълнява ролята на среда за развитие на знания и умения в областта на киберсигурността, като същевременно интегрира и теми, свързани с изкуствения интелект и иновациите. Той е част от националната програма за изграждане на STEM среда и подкрепя кариерното развитие на учениците в технологични направления.

Във висшето образование Нов български университет обяви нова бакалавърска програма „Кибертехнологии и изкуствен интелект“, която интегрира киберсигурност и AI. В сферата на неформалното обучение SoftUni планира Upskill програма „Cyber Security and Ethical Hacking“, насочена към практически умения и реални приложения.

Тези развития очертават формирането на цялостна образователна екосистема – от средното образование, през университетите, до специализирани обучителни програми. Това създава предпоставки за

по-добра подготовка на кадри и за устойчиво развитие на сектора на киберсигурността в страната.

Women4Cyber Bulgaria: Изграждане на общност от обучители

Проведе се първата среща на членовете на Women4Cyber Bulgaria, насочена към подготовка на обучители в областта на киберсигурността. Инициативата е в съответствие с мисията на Women4Cyber за насърчаване на образованието и повишаване на информираността в областта на киберсигурността, както и за изграждане на по-сигурна и устойчива дигитална среда.

В рамките на срещата беше сформиран експертен екип, който ще реализира обучения и информационни сесии в училища в цялата страна. Основната цел е повишаване на осведомеността за рисковете в дигиталната среда и изграждане на устойчива култура за киберсигурност сред младите хора. Инициативата включва и представяне на професията по „Киберсигурност“, с акцент върху възможностите за образование, развитие и професионална реализация в тази динамична и все по-търсена сфера.

Пълният текст може да прочетете тук.

Каталози на образователни програми по киберсигурност

В подкрепа на ориентацията в нарастващото разнообразие от образователни възможности в областта на киберсигурността се развиват специализирани онлайн каталози, които систематизират и представят наличните програми.

На европейско ниво показателен пример е SPARTA Cybersecurity Study Programs Map, разработен в рамките на инициативите на ЕС за дигитални умения. Платформата представлява интерактивен каталог, който обхваща университетски програми по киберсигурност в различни европейски държави. Тя позволява търсене и филтриране по държава, образователна степен, език и други критерии, като предоставя структурирана информация за съдържанието и насочеността на обученията. По този начин ресурсът улеснява сравнението между различни програми и подпомага избора на подходяща образователна и кариерна пътека в европейски обхват.

Като допълнение може да се посочи и платформата OnlineCyberSecurityDegree.org, която функционира като каталог на образователни програми и кариерни ресурси, основно в САЩ. Сайтът обединява информация за университетски степени, онлайн обучения, сертификационни курсове и различни специализации в областта на киберсигурността. Освен това предоставя насоки за професионално развитие и описание на ключови роли в сектора. Макар да е фокусиран извън Европа, ресурсът предлага полезна отправна точка за сравнение и ориентация в глобалните тенденции в обучението по киберсигурност.

Тези платформи показват нарастващата нужда от систематизирана и достъпна информация, която да подпомага както обучаемите, така и организациите при избора на подходящи форми на обучение и развитие на умения в областта на киберсигурността.

Нови тенденции при кибератаките през 2026

От началото на 2026 г. наблюдаваната еволюция на кибератаките, е свързана основно с използването на изкуствен интелект и нарастващата свързаност на системите. Все по-разпространени са AI-генерирани phishing кампании и deepfake атаки, които значително повишават ефективността на социалното инженерство. Увеличава се делът на атаките, базирани на компрометирани идентичности („log in, not break in“), както и на атаки по веригата на доставки, които използват доверени зависимости и услуги. Паралелно с това се наблюдава развитие на ransomware моделите към многостепенни форми на изнудване и засилване на атаките срещу cloud и SaaS среди. Нов елемент е и нарастващият брой атаки, насочени директно към AI системи, което очертава тях като нова повърхност за атака.

Наблюдаваните тенденции се потвърждават от водещи индустриални доклади, включително IBM и Cloudflare, които анализират реални атаки, инциденти и глобален интернет трафик.

Връзки към събития по киберсигурност и информационна устойчивост

- European Cybersecurity Certification Conference, 15 April, 2026, Ayia Napa, Cyprus
- 4th CyberCLUB Community Birthday, 21 April, 2026, Sofia, Bulgaria
- CYBERUK, 21-23 April, 2026, Glasgow, UK
- 47th IEEE Symposium on Security and Privacy, 18-21 May, 2026, San Francisco, CA, USA
- Cybersec Europe, 20-21 May, 2026, Brussels, Belgium
- CyberWiseCon Europe, 20-22 May, 2026, Vilnius, Lithuania
- Infosecurity Europe 2026, 2-4 June, 2026, London, UK
- CyberComf 2026, 12 June, 2026, Sofia, Bulgaria

Редакционен съвет

Публикуването на настоящия брой на бюлетина се реализира с финансовата подкрепа на проект: **#101256930 – CYBER4All 2.0 – DIGITAL-2025-EDIH-EU-EAA-08 на ЕК**