



Funded by
the European Union



ПРОГРАМА
НАУЧНИ ИЗСЛЕДВАНИЯ,
ИНОВАЦИИ И ДИГИТАЛИЗАЦИЯ ЗА
ИНТЕЛИГЕНТНА ТРАНСФОРМАЦИЯ



Digital Innovation Hub
Trakia



ИНСТИТУТ ПО ИНФОРМАЦИОННИ И
КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Информационен бюлетин за киберсигурност

Бюлетин Юни 2024

Номер 13

Цели и обхват

Съдържание:

- Цели и обхват
- Фокус на изданието

Хибриден модел на обучение по киберсигурност и сертификация

- Как Европа помага на предприемачите?
- Стратегически партньорства с ЕЦИХ "Тракия"
- За цифрова и киберустойчива администрация
- Киберсигурност в публичния сектор
- ЕЦИХ "Тракия" представи услуги за европейските МСП на форум с експерти от Google и Microsoft
- Професия киберсигурност
- Уебинар по въпросите на европейските регулации в киберсигурността
- ЕЦИХ "Тракия" с практически семинар „Кибердоброволец 112“
- Експерт от ЦИХ "Тракия" призовава за повече проактивни мерки
- Новини и събития по темата киберсигурност
- Връзки
- Редакционен съвет

Настоящият брой на информационния бюлетин за киберсигурност е фокусиран в областта на е-обучението по киберсигурност. Тази тематика присъства и в планираните дейности на ЕЦИХ „Тракия“. В настоящия брой е представен хибриден модел на обучение по киберсигурност и сертификация. Подробно са описани компонентите на хибридният модел на обучение по киберсигурност и сертификация включващи: Интерактивно съдържание; Тестове; Симулации и лабиринти; Казуси и проекти; Асинхронно подпомагане; Виртуални стаи и Присъствено обучение. Показан е пример за реализиране на хибридна програма за обучение по киберсигурност и сертификация, определени са съставните компоненти и продължителността във времето. Общата схема включва: въвеждащо обучение; подробно обучение на всеки 6 месеца и годишно присъствено обучение. Накрая са маркирани и предизвикателствата, които съпътстват реализирането на описания хибриден модел за обучение по киберсигурност и сертификация.

Представени са някои от реализираните стратегически партньорства между ЕЦИХ "Тракия" и базирания в Будапеща Цифров иновационен хъб (Digital Tech EDIH) на EIT Digital, Европейския институт по иновации и технологии, както и с водещия научноизследователски и развоен институт на Румъния в сферата на информационните и комуникационни технологии - ICI Bucharest.

Представена е информация за представените от ЕЦИХ "Тракия" услуги за европейските МСП на форум с експерти от Google и Microsoft. Даден е лик за проведения уебинар по въпросите на европейските регулации в киберсигурността с участието на експерти от цифрови хъбове от България, Австрия и Хърватия, който се излъчи онлайн.

Представен е публикувания актуализиран Наръчник по киберсигурност за европейските избори, както и допълнение на Регламент (ЕС) 2019/943 на Европейския парламент и на Съвета чрез установяване на мрежов кодекс относно специфични за сектора правила за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия.

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

Фокус на изданието: Хибриден модел на обучение по киберсигурност и сертификация



инж. Ивайло Благоев

С развитието на технологиите и увеличаването на кибератаките, обучението по киберсигурност и сертификацията стават все по-важни. Създаването на добре подготвени специалисти по киберсигурност е от съществено значение за защитата на информационните системи и данни. Хибридните модели на обучение, които комбинират онлайн и присъствено обучение, предлагат ефективен и гъвкав начин за усвояване на необходимите знания и умения. Този модел включва няколко ключови компонента, които осигуряват цялостно и разнообразно обучително изживяване. В следващите секции ще разгледаме подробно тези компоненти и предизвикателствата, свързани с тяхната реализация.

1. Компоненти на хибридният модел

За да бъде ефективен, хибридният модел на обучение по киберсигурност трябва да включва разнообразни елементи, които да обхващат различни аспекти на обучителния процес. Всеки компонент играе ключова роля в изграждането на цялостно и интерактивно обучително изживяване, което е от съществено значение за ефективното усвояване на знания и умения в областта на киберсигурността.

- **Интерактивно съдържание** – Интерактивното съдържание включва мултимедийни материали, видеоклипове, анимации и интерактивни елементи, които ангажират обучаемите и улесняват усвояването на сложни концепции. Тези материали предоставят динамично и ангажиращо учебно изживяване, което помага на обучаемите да запомнят и разберат по-добре информацията.
- **Тестове** – Регулярните тестове са ключов елемент за оценка на напредъка и разбирането на обучаемите. Те предоставят възможност за самостоятелна оценка и обратна връзка, което помага за по-добро усвояване на материала. Тестовите могат да бъдат както онлайн, така и в присъствена форма.
- **Симулации и лабиринти** – Симулациите и лабиринтите предоставят реалистични сценарии, в които обучаемите могат да приложат на практика своите знания и умения. Това помага за изграждането на практически опит в контролирана среда. Например, симулациите могат да включват хакерски атаки, които обучаемите трябва да предотвратят или разрешат.
- **Казуси и проекти** – Реалните казуси и проекти предоставят възможност за задълбочено изучаване на конкретни проблеми и предизвикателства в областта на киберсигурността. Те насърчават критичното мислене и творческия подход към решаването на проблеми. Обучаемите могат да работят по проекти, свързани с актуални въпроси в киберсигурността, което ги подготвя за реални ситуации.
- **Асинхронно подпомагане** – Асинхронното подпомагане включва предоставяне на материали и ресурси, до които

обучаемите могат да имат достъп по всяко време. Това позволява на обучаемите да учат със собствено темпо и в удобни за тях моменти. Асинхронното подпомагане може да включва форуми за дискусии, електронни книги, вебинари и други ресурси.

- **Виртуални стаи** – Виртуалните стаи предоставят възможност за провеждане на онлайн сесии и дискусии в реално време. Те улесняват взаимодействието между обучаемите и преподавателите, което е важно за ефективното усвояване на материала. Виртуалните стаи могат да се използват за лекции, семинари, групови дискусии и индивидуални консултации.
- **Присъствено обучение** – Присъственото обучение предоставя възможност за директна комуникация и взаимодействие между обучаемите и преподавателите. То е особено полезно за практически занятия и лабораторни упражнения. Присъственото обучение също така насърчава сътрудничеството и обмена на опит между обучаемите.

2. Пример за реализиране на хибридна програма по киберсигурност

За ефективното обучение и сертификация по киберсигурност, е важно да се разработи и приложи хибридна програма, която комбинира различни форми на обучение. В този пример ще разгледаме как може да се реализира такава програма, включваща въвеждащо обучение, регулярно обучение на всеки шест месеца и годишно присъствено обучение.



Фиг. 1 Пример за реализиране на хибридна програма по киберсигурност

2.1. Въвеждащо обучение (първа седмица)

Цел: Запознаване на новоназначените служители с основите на киберсигурността и вътрешните политики на компанията.

Компоненти:

- **Онлайн интерактивно съдържание:** Мултимедийни презентации и видеоклипове, които обясняват основните принципи на киберсигурността. Интерактивни модули за обучение по вътрешните политики и процедури на компанията.

- **Присъствено обучение:** Провеждане на лекции и семинари, водени от специалисти по киберсигурност. Дискусии и въпроси-отговори за разясняване на ключови точки и осигуряване на обратна връзка.

Период: Първата седмица от назначаването.

2.2. Подробно обучение на всеки 6 месеца

Цел: Надграждане на знанията и уменията по киберсигурност и подготовка за справяне с нови предизвикателства.

Компоненти:

Онлайн компоненти:

- *Интерактивно съдържание* - Разширени модули за обучение по актуални теми в киберсигурността. Видеокурсове с експерти, които споделят най-новите тенденции и технологии.
- *Тестове:* Регулярни тестове за проверка на разбирането и усвояването на материала.
- *Симулации и лабиринти:* Практически упражнения, които симулират реални кибератаки и сценарии. Лабиринти за решаване на проблеми, свързани с киберсигурността.
- *Казуси и проекти:* Работа по реални казуси и проекти, които изискват прилагане на научените знания и умения.

Активно подпомагане:

- *Асинхронно подпомагане:* Форуми за дискусии.
- *Виртуални стаи:* Провеждане на онлайн сесии в реално време за дискусии, семинари и индивидуални консултации.
- *Присъствено обучение:* Практически сесии и лабораторни упражнения, водени от експерти по киберсигурност.

Период: Веднъж на всеки шест месеца.

2.3. Годишно присъствено обучение

Цел: Осигуряване на задълбочено обучение и практически опит чрез интерактивни сесии и лабораторни упражнения.

Компоненти:

Присъствено обучение: Интензивни курсове и семинари, водени от водещи специалисти в областта на киберсигурността. Практически упражнения и симулации в лабораторни условия. Обсъждане на актуални казуси и проекти с цел прилагане на наученото в реални ситуации.

Период: Веднъж годишно.

Тази хибридна програма предоставя комплексен подход за обучение по киберсигурност, съчетавайки онлайн и присъствени компоненти за максимална ефективност. Въвеждащото обучение през първата седмица осигурява бързо запознаване с основните принципи и политики, докато подробното обучение на всеки шест месеца и годишното присъствено обучение предоставят възможности за надграждане и задълбочаване на знанията и уменията. Такава програма изисква комплексна инфраструктура и внимателно планиране, но предоставя значителни предимства, включително гъвкавост, ефективност и възможност за персонализиране на обучението според нуждите на всеки обучаем.

За успешната реализация на хибридният модел е необходима комплексна инфраструктура за обучение, която да обхваща всички посочени компоненти. Тази инфраструктура включва платформи за онлайн обучение, софтуер за симулации и виртуални стаи, както и материали за асинхронно подпомагане. Ключовите предимства на хибридният модел включват гъвкавост, ефективност и възможността за персонализиране на обучителния процес според нуждите на всеки обучаем. Тези предимства правят хибридният модел изключително подходящ за обучение по киберсигурност, където бързото и ефективно усвояване на знания и умения е от съществено значение.

3. Предизвикателства при реализирането на хибриден модел

Въпреки множеството предимства на хибридният модел, съществуват и редица предизвикателства, които трябва да бъдат преодоляни за успешното му прилагане. Разбирането и справянето с тези предизвикателства е от съществено значение за постигането на ефективно и устойчиво обучително решение.

- **Липса на L&D екипи** - Липсата на екипи за обучение и развитие (L&D) може да затрудни създаването и внедряването на ефективни обучителни програми. Наличието на квалифицирани специалисти е от съществено значение за успешното прилагане на хибридният модел. L&D екипите играят важна роля в разработването на съдържание, управление на учебните процеси и предоставяне на обратна връзка.
- **Липса на съдържание** - Липсата на подходящо и актуално съдържание може да представлява сериозно препятствие. Необходимо е създаване на качествени обучителни материали, които да отговарят на нуждите и изискванията на обучаемите. Съдържанието трябва да бъде актуализирано редовно, за да отразява последните тенденции и развития в областта на киберсигурността.
- **Времеемки административни дейности** - Административните дейности, свързани с организирането и координирането на обучителните програми, могат да бъдат изключително времеемки. Ефективното управление на тези процеси е от съществено значение за успешното реализиране на хибридният модел. Автоматизацията и използването на специализирани софтуерни решения могат да помогнат за улесняване на тези задачи.
- **Трудно създаване и редакция на съдържание** - Създаването и редакцията на обучителни материали изисква време и усилия. Необходимо е използване на специализирани инструменти и технологии за улесняване на този процес. Важно е да се осигури качествено съдържание, което да бъде лесно разбираемо и ангажиращо за обучаемите.

Хибридните модели на обучение по киберсигурност и сертификация предлагат множество предимства, като съчетават гъвкавостта на онлайн обучението с ефективността на присъственото обучение. Комбинацията от интерактивно съдържание, тестове, симулации, казуси и проекти, асинхронно подпомагане, виртуални стаи и

присъствено обучение предоставя ефективен и гъвкав подход за усвояване на знания и умения в областта на киберсигурността. Въпреки предизвикателствата, свързани с липсата на L&D екипи, съдържание и времеемките административни дейности, този модел има потенциала да бъде изключително успешен при правилно управление и планиране. С правилното планиране и използване на наличните ресурси, хибридният модел може да предостави високо качество на обучението и да подготви специалисти, способни да се справят с предизвикателствата на съвременния киберсвят.

Как Европа помага на предприемачите?



На този въпрос отговори Христиан Даскалов от Европейски цифров иновационен хъб "Тракия" в рамките на динамичен разговор с предприемачи и експерти, които споделиха опита си пред младите хора в #Пловдив. Инструменти в помощ на предприемачите бяха представени от Красимир Лойков от Europe Direct Plovdiv и Снежина Сулева от Клуб на мениджъра. Успешният предприемачески пример на национално и местно ниво представиха съответно Гергана Станчева от La'mon и Пенко Стоев от IMD Consulting & Coworking. Младият социален предприемач Денис Петков представи своя стартъп "BrighThrive" и потърси съвет и насоки от експертите.

Стратегически партньорства с ЕЦИХ "Тракия"



Digital Innovation Hub
Trakia

Стратегическо партньорство на ЕЦИХ "Тракия" с базирания в Будапеща Цифров иновационен хъб (Digital Tech EDIH) на EIT Digital, Европейския институт по иновации и технологии.



ЕЦИХ "Тракия" подписа споразумение за сътрудничество с водещия научноизследователски и развоен институт на Румъния в сферата на информационните и комуникационни технологии – ICI Bucharest. Двете организации ще работят за създаването на споделена инфраструктура по линия на Европейската сертификационна рамка за киберсигурност на Европейската агенция за мрежова и информационна сигурност.

Генералният директор на румънската Национална дирекция за киберсигурност Дан Кимпеан: Публично-частното партньорство е ключово в киберсигурността. Работим с български компании с доказана експертиза.



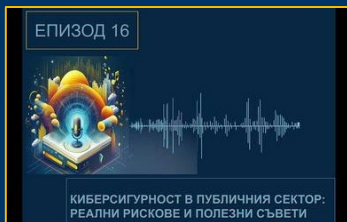
Пълният текст може да прочетете [тук](#).

За цифрова и киберустойчива администрация



Представители на иновативния бизнес, част от ЕЦИХ "Тракия" посетиха Община Самоков по покана на Регионалния съвет за развитие на Самоков. По време на срещата се обсъдиха възможностите за предоставяне на безвъзмездна помощ от Хъба за общината, бизнеса и гражданите на града. Обсъдена бе идеята на кмета и предприемачите за създаване на цифрова и киберустойчива администрация и бизнес.

Киберсигурност в публичния сектор



Експертът по кибер сигурност Ясен Танев, който е част от екипа на ЕЦИХ "Тракия", представи лекция на тема "Киберсигурност в публичния сектор: Реални рискове и полезни съвети".

Лекцията може да се види [тук](#).

ЕЦИХ "Тракия" представи услуги за европейските МСП на форум с експерти от Google и Microsoft



ЕЦИХ "Тракия" (Cyber4AllSTAR) взе участие в престижния ежегоден форум „Futurist Expo“ в периода 21-23 юни 2024, редом с представители на компании от ранга на Google и Microsoft. Сред темите на форума бяха бъдещето на генеративния изкуствен интелект и демократизацията на данните. Председателят на ЕЦИХ "Тракия" д-р Христиан Даскалов представи в рамките на програмата на събитието мрежата от над 150 дигитални хъба, предоставящи безвъзмездни консултантски и технологични услуги за европейските малки и средни предприятия с финансиране по програмата „Дигитална Европа“ на ЕК, в т.ч. и четирите български хъба, подкрепени от Министерството на иновациите и растежа, посредством управляваната от него национална Програма за научни изследвания, иновации и дигитализация за интелигентна трансформация.

Пълният текст на интервюто може да прочетете [тук](#).

Професия киберсигурност е факт, възможно е от есента да има учебни планове



Христиан Даскалов, председател на Цифровия иновационен хъб „Тракия“ и доц. Златогор Минчев, Институт по информационни и комуникационни технологии към БАН, в „Бизнес старт“ 26.03.2024 г.

Вече съществува професия киберсигурност, след като бе утвърден списъкът на професиите. Сега предстоят да се разработят учебните планове, свързани с подобна професия. Възможно е от началото на новата учебна година младите хора да имат тази възможност да се обучават по специалността. Основното усилие, за да наваксаме различни пропуски в сигурността е по линия на образованието. Гарантирането на дигитална сигурност в сложната геополитическа картина е предизвикателство. Създаването на граници в интернет е дискуссионен елемент, но това е свързано със сътрудничество, това

коментираха Христиан Даскалов, председател на Цифровия иновационен хъб „Тракия“ и доц. Златогор Минчев, Институт по информационни и комуникационни технологии към БАН, в предаването „Бизнес старт“ с водеща Роселина Петкова..

Пълният текст на интервюто може да прочетете [тук](#).

Уебинар по въпросите на европейските регулации в киберсигурността



На 12.06.2024 се проведе международен уебинар по въпросите на европейските регулации в киберсигурността с участието на експерти от цифрови хъбове от България, Австрия и Хърватия. Събитието се излъчваше на живо от адрес: <https://convocircle.com/edih>.

ЕЦИХ "Тракия" с практически семинар „Кибердоброволец 112“



На 18.05.2024 от 11:00 часа се проведе практически семинар „Кибердоброволец 112“, който ЕЦИХ "Тракия" организира в партньорство с Доброволно формирование „Пловдив 112“. Семинарът бе насочен върху изследването на взаимодействието между дигитализацията и управлението на спасителни операции при бедствия, кризи и извънредни ситуации, както и върху използването на дигитални технологии за повишаване на ефективността при спасяването на хора.

Експерт от ЦИХ "Тракия" призовава за повече проактивни мерки: обучения, тестове за проникване и оценки на уязвимостите



Около 50% от българските компании смятат, че темата "Киберсигурност" е нерелевантна за тях. Тази статистика на "Евростат" цитира пред БНР Христиан Даскалов - председател на борда на Цифров иновационен хъб "Тракия".

Пълният текст на интервюто може да прочетете [тук](#).

Новини и събития по темата киберсигурност



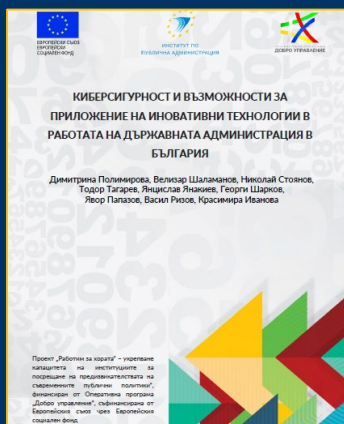
Актуализиран наръчник за това как да се опази честността на изборите от гледна точка на киберсигурността бе публикуван днес с подкрепата на Европейската комисия и на Агенцията на ЕС за киберсигурност (ENISA). Пълният текст може да прочетете [тук](#).

На 24.05.2024 г. в Официален вестник беше публикуван Делегиран регламент (ЕС) 2024/1366 на Комисията от



11.03.2024 г. за допълнение на Регламент (ЕС) 2019/943 на Европейския парламент и на Съвета чрез установяване на мрежов кодекс относно специфични за сектора правила за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия. Пълният текст може да прочетете [тук](#).

Взаимодействие с ИПА от 2018 насам



Киберсигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България.

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.

Автори: Д. Полимирова, В. Шаламанов, Н. Стоянов, Т. Тагарев, Я. Янакиев, Г. Шарков, Я. Папазов, В. Ризов, К. Иванова.

Връзки към конференции и събития по киберсигурност през 2024



- **DIGILIENCE 2024** – Digital Transformation, Cybersecurity, and Resilience (13-15 Ноември 2024)
- **International Trade Fair for Security Systems and Safeguard** – Варшава, Полша (27-29 Ноември 2024)

Редакционен съвет



1. проф. д.н. Даниела Борисова – ИИКТ-БАН
2. доц. д-р Велизар Шаламанов – ИИКТ-БАН
3. Светлин Илиев – Българска асоциация по киберсигурност
4. д-р Християн Даскалов – Цифров Иновационен хъб – Тракия
5. д-р Иван Благов – ИИКТ-БАН
6. д-р Ирена Младенова – Софийски Университет „Св. Климент Охридски“
7. д-р Емилия Печева – Британско посолство в София

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



British Embassy
Sofia



СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE



ИНСТИТУТ ПО ИНФОРМАЦИОННИ И
КОМУНИКАЦИОННИ ТЕХНОЛОГИИ



BULGARIAN CYBERSECURITY ASSOCIATION
Българска асоциация по
киберсигурност



ОБЩИНА ПЛОВДИВ