ISSN 2738-7089 https://doi.org/10.11610/cybsec06bg

British Embassy Sofia

# Информационен бюлетин за киберсигурност

ИИКТ
Институт по информационни и комуникационни технологии

## Британско-Българско партньорство в киберсигурността за МСП и организации

Бюлетин Март 2021 Номер 6

## Цели и обхват

Съдържание:



Настоящият онлайн бюлетин е фокусиран върху теми, свързани с висшето образование в киберсигурността. Областите на образование и обучение са специално разгледани в рамките на инициативите, свързани с киберсигурността на Европейската комисия и Европа като цяло.

Програмите и курсовете за образование и обучение са сред основните теми на проекта за киберсигурност Atlas и неговата онлайн платформа, която картографира институциите и техните възможности в рамките на предложената европейска таксономия за киберсигурност. Регламентът за създаване на Европейски център за компетентност по киберсигурност в областта на индустрията, технологиите и научните изследвания (R630) подчертава специално значението на образованието и обучението като ключови активи за прилагането на политиката за киберсигурност. Образованието, обучението и уменията за киберсигурност също са сред актуалните въпроси в процеса на създаване на Европейската общност за компетентност в областта на киберсигурността.

Агенцията за киберсигурност на Европейския съюз ENISA, предприема най-подходящата инициатива да създаде база данни за висшето образование по киберсигурност (CyberHEAD). Базата данни е представена накратко в първия раздел на бюлетина. Представени са данните за бакалавърските и магистърските програми по управление на киберсигурността и е идентифицирана необходимостта от различни възможности. Представен е и инструментът за онлайн картографиране на проекта CONCORDIA.

Въвежда се подходът на Университета за национално и световно стопанство (УНСС), за предоставяне и интегриране на различни възможности в магистърската програма по управление на киберсигурността. Разглеждат се профилите на висшите учебни заведения и как да се улесни сътрудничеството и интеграцията.

Изданието включва кратък доклад за онлайн интерактивно обучение, посветено на ролята на главния информационен директор (CIO) за Българската академия на науките и големите български университети, ръководено от професор по системна сигурност в университета в Ковънтри.

Представени са сертифициращите институции и националните образователни фондове във Великобритания и България.

Както и в предишните издания на бюлетина, се предоставят връзки към онлайн новини и събития (и техните източници). Специално внимание е отделено на актуализациите в българската национална стратегия за киберсигурност.

Редактори на изданието: **доц. д-р Георги Пенчев**
**доц. д-р Константин Пудин**
**главен асистент Атанас Димитров**

# Фокус на изданието: Интегриране на образователните възможности в програмите за управление на киберсигурността

**доц. д-р Георги Пенчев, Катедра „Национална и регионална сигурност“ (КНРС), УНСС, София, редактор на броя**

**доц. д-р Константин Пудин, КНРС-УНСС, София, редактор на броя**

**Главен асистент Атанас Димитров, КНРС-УНСС, София, редактор на броя**

Основният източник на информация за образователните програми по киберсигурност е онлайн базата данни за висше образование по киберсигурност (CyberHEAD). Базата данни е създадена и се поддържа от ENISA. Това усилие не е единичен акт за събиране и разпространение на данни. Няколко инициативи и документи, свързани с образователната политика на ЕС за киберсигурност, могат да се разглеждат като основа за създаването на CyberHEAD (според публикацията на уебсайта ENISA):

- Първата стратегия на ЕС за киберсигурност, публикувана от Европейската комисия през 2013 г. Комисията приканва държавите членки да увеличат усилията си за образование и обучение по темите за мрежова и информационна сигурност, както и да участват в програма за доброволно сертифициране на ИТ специалисти, с цел насърчаване усъвършенстването на умения и валидиране на компетентностите им.
- Съвместният труд „Устойчивост, възпиране и отбрана: Изграждане на силна киберсигурност за ЕС“, публикуван през 2017 г. от Европейската комисия и „Върховния представител на ЕС по въпросите на външните работи и политиката на сигурност“, декларира, че „ефективната киберсигурност разчита силно на уменията на засегнатите хора“.
- Доклад „Развитие на умения за киберсигурност в ЕС“, фокусиращ се върху състоянието на образователната система по киберсигурност и трудностите при привличането на повече студенти. Докладът търси начини как може да се увеличи броя на завършилите студенти с приложими знания и умения по киберсигурност.

ENISA разработи и доклада за развитието на уменията за киберсигурност в ЕС, за да се обърне внимание на състоянието на образователната система по киберсигурност. Докладът идентифицира пропуски и недостиг на образована и обучена работна сила. Анализът се основава на опита на четири държави - Австралия, Франция, Обединеното кралство и САЩ.

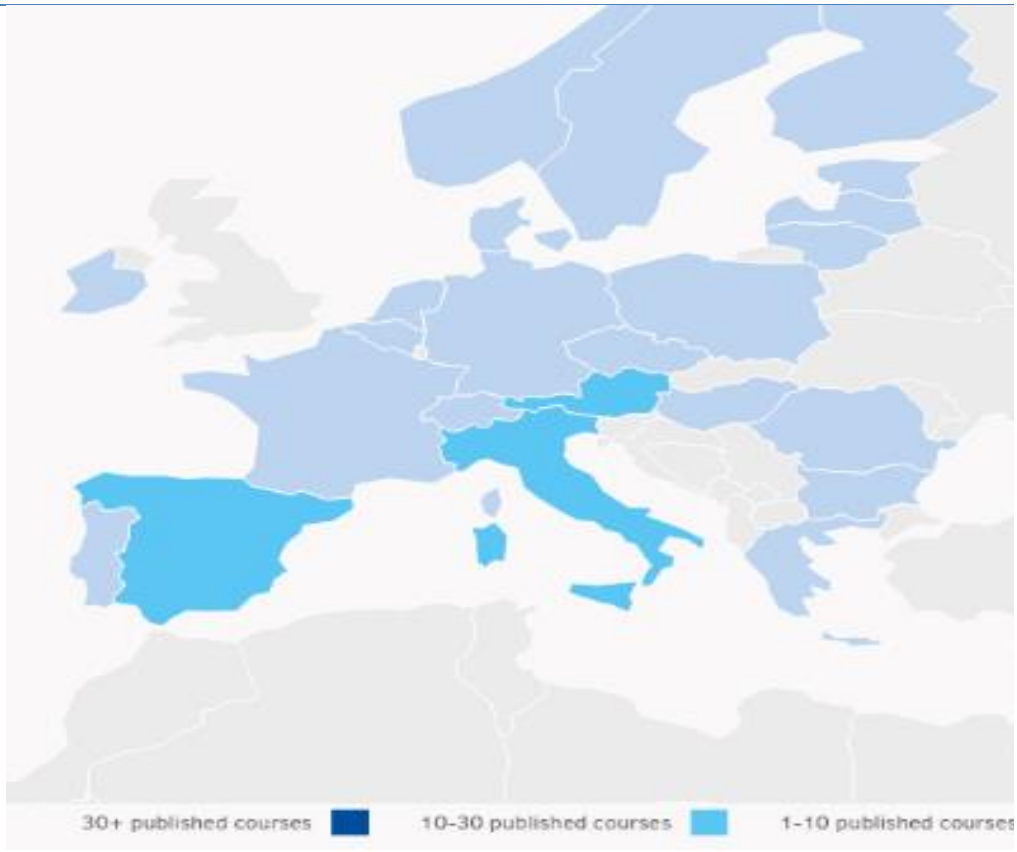
CyberHEAD може да се разглежда и като инструмент, подпомагащ развитието на Европейската рамка за умения по киберсигурност, който има за цел да създаде общо разбиране за ролите, компетенциите, уменията и знанията, използвани във всички аспекти на киберсигурността - физическите лица, работодателите и т.н.

Учебните програми по киберсигурност 2017, разработени от „Съвместната работна група за образование по киберсигурност“, се използват като основна справка за образователните програми по киберсигурност в базата данни CyberHEAD.

Като цяло CyberHEAD е онлайн платформа за регистриране на програмите за висше образование по киберсигурност. Регистрацията е валидирана от ENISA. Целта на базата данни е дефинирана по следния начин: „Това беше основната отправна точка за всички граждани, които искат да подобрят знанията си в областта на киберсигурността. Тази база данни позволява на младите таланти да вземат информирани решения относно разнообразието от възможности, предлагани от висшето образование в областта на киберсигурността и помага на университетите да привлекат висококачествени студенти, мотивирани да поддържат Европа кибер-сигурна.“

От март 2020 г. са регистрирани 130 програми в 24 държави и на сайта на платформата е посочено, че това е „най-голямата валидирана база данни за висше образование в киберсигурността в ЕС и страните от

EACT". Пространственото разпределение на регистрираните и валидирани програми в цяла Европа е представено на фигурата по-долу.




Разпределението, до датата на текущия брой на бюлетина, е почти равностойно между само три държави, включени в графата на „10-30 публикувани курса".

Изискванията за регистрация на учебна програма, са както следва:

- За **бакалавърска степен**: поне 25% от преподаваните модули да са по теми за киберсигурност;
- За **магистърска степен**: поне 40% от преподаваните модули да са по теми за киберсигурност;
- За **следдипломна специализация**: поне 40% от преподаваните модули да са по теми за киберсигурност и програмата да има минимум 60 кредита, в съответствие с ECTS;
- За **докторска степен**: дисертацията трябва да е на тема киберсигурност.

Най-интересните данни от базата данни CyberHEAD, са относно Европейската система за трансфер и натрупване на кредити (ECTS), както и ECTS кредитите, посветени на отделните дисциплините в курса като процент от общия размер на ECTS на курса. Разполагайки с тези данни, можем да сравним курсовете и програмите за управление, с тези ориентирани повече към техническите аспекти на киберсигурността.

CyberHEAD не ни предоставя опции за изтегляне на пълния набор от данни. Можем да експериментираме с ключовата дума „управление" и търсенето да ни върне 24 магистърски и бакалавърски програми, свързани малко или много с управлението на киберсигурността, риска и технологиите.

Националният център за киберсигурност на Великобритания е органът, който сертифицира бакалавърските и магистърските програми по киберсигурност. Информацията за програмите се предоставя като списък, който можете да намерите онлайн тук.

## Курсове и обучения за професионалисти

Четирите пилотни проекта, които са в основата на създаването на общност за компетентност в областта на киберсигурността, също имат силен фокус върху образованието - например проектът ECHO се фокусира върху рамката за умения по киберсигурност, таксономията, обучението и сертифицирането. Проекта CONCORDIA е тясно свързан с обучението на професионалисти в областта на киберсигурността.

Четирите пилотни проекта са представени в бюлетин №4.


CONCORDIA поддържа и уеб платформа за регистриране и картографиране на курсовете и обученията за професионалисти в цяла Европа. Картата на текущите регистрирани курсове в платформата е представена по-горе. Повече за картата на курсовете на CONCORDIA можете да намерите тук и тук.

## Профили на организации и институции

Настоящата социална среда се характеризира с динамичните процеси на дигитална трансформация във всички сфери. Ежедневието на хората е немислимо без използването на компютърни технологии и комуникационни мрежи. Всеки от нас, независимо от причината - работа, образование или просто забавление, прекарва все повече и повече време в киберпространството, особено по време на пандемия.

Този интензивен процес на виртуализация на нашето ежедневие е придружен от различни предизвикателства пред сигурността. Много възникнали кибер заплахи съществуват и в наши дни. Засягайки мрежите и компютърните системи, те имат способността да нарушават кибер устойчивостта на индивидуално, организационно или национално ниво, причинявайки огромни материални и морални негативни последици. Киберпространството се превърна в поле за война и различни престъпления. Ето защо разработването и поддържането на адекватен капацитет за противодействие е от решаващо значение. Всичко това определя значението на образованието и обучението по киберсигурност като един от начините за развитие на такъв капацитет.

Целта на обучението по управление на киберсигурността е да предостави на студентите знания, свързани със същността и особеностите на киберсигурността. Също така, студентите развиват умения да анализират вътрешната и външната среда на субектите, да избират и прилагат подходи за избягване на кибер заплахи и подходи за гарантиране на кибер устойчивост на техните организации.

| | |
|---|---|
| | Обучението допринася за развитието на съответна култура на киберсигурност - начин на възприемане на околната среда, начин на мислене и действие по отношение на съществуващите кибер заплахи и опасности, базирани на осведомеността за киберсигурността. |
| **Пример за интегриране на възможности** | Киберсигурността е сложена материя с припокриване на няколко сфери, като например: управление, организационно поведение и психология, правоприлагане, разработване на политики, ИТ и т.н. Ето защо обучението по управление на киберсигурността има различни аспекти и обхваща различни дисциплини.<br>УНСС има две години опит в областта на образованието по киберсигурност. Учебната програма за магистър по управление на киберсигурността на УНСС показва това разнообразие от курсове, които такава програма може да включва. Продължителността на обучението е два семестъра. Учебната програма включва:<br>• Основи на киберсигурността;<br>• Системи за индустриален контрол и SCADA;<br>• Правни аспекти на киберсигурността;<br>• Управление на кризи и киберсигурност;<br>• Криптография и киберсигурност (изучавани през първия семестър)<br>и<br>• Изкуствен интелект и киберсигурност;<br>• Основи на кибер разузнаването;<br>• Добри практики в киберсигурността;<br>• Интернет сигурност (изучавани през втория семестър).<br>Сложността на киберсигурността изисква участието на преподаватели с различни знания и умения от различни организации като: университети и изследователски центрове, бизнес организации, държавни органи и други.<br>Обучението по управление на киберсигурността изисква наличието на дисциплина/дисциплини в учебната програма, свързани с управленската наука. Това се дължи на факта, че осигуряването на киберсигурността, както и всички други аспекти на сигурността, изисква извършването на управленски дейности в рамките на четирите основни функции на управлението, както следва:<br>• планиране - определяне на цели, свързани с изграждането на киберсигурност и решаване как е най-добре те да се постигнат;<br>• организиране - определяне как да се направи най-доброто групиране на дейностите и ресурсите за киберсигурност;<br>• ръководене - мотивиране на персонала да работи за интересите на организацията в контекста на поставените цели за киберсигурност;<br>• контрол - наблюдение и коригиране на текущите дейности за подпомагане постигането на целите на киберсигурността.<br>Участието на лектори със знания и опит в областта на управлението е от съществено значение, напр. университетски преподаватели и държавни служители на политическо и стратегическо ниво участват в образователния процес.<br>Киберсигурността изисква участие на опитни ИТ специалисти, запознати с функционирането на компютърните технологии и спецификата на комуникационни мрежи, знаейки техните уязвимости и начините за защита. |

| | |
|---|---|
| | Противодействията при кибер-престъпленията ангажират изцяло вниманието на правителството. Част от задълженията на правоприлагащите органи и специализираните агенции са свързани с предотвратяването, откриването и реагирането на кибер заплахи и кибер атаки.<br><br>Подготовката относно правните аспекти на киберсигурността също е много важна. Кибер-престъпленията нарушават правилата, установени от държавата. Всеки потребител, който живее и работи в киберпространството, е изложен на различни заплахи, нарушаващи някои от неговите/нейните основни права като човек и като гражданин. Познаването на правните аспекти е много важно.<br><br>Отговорна за магистърската програма по управление на киберсигурността в УНСС е Катедрата за национална и регионална сигурност (КНРС). Катедрата има повече от 30 години опит в организирането на образователни програми в сложната област на отбраната, икономиката и управлението на сигурността, интегрирайки образователни възможности от различни области на знанието.<br><br>Програмата за управление на киберсигурността обединява усилията на повече от 10 организации - университети, изследователски организации, бизнес организации. Сътрудничеството между организациите може да се основава на официални или неформални споразумения. След като организацията постигне съгласие за сътрудничество, се назначават водещите преподаватели по дисциплините. Основният фокус при такава интеграция са хората - те са доставчици на възможностите и трябва да създадат добре балансиран и ефективен екип.<br><br>Повече за магистърската програма по управление на киберсигурността можете да бъде намерено тук и тук. |
| **Как да улесним сътрудничеството** | Различни форми на взаимодействие биха могли да улеснят сътрудничеството между организациите и институциите, участващи в образователния процес по киберсигурност.<br><br>Най-често сътрудничеството се основава на двустранни споразумения за сътрудничество, подписани с други национални или чуждестранни академични институции, изследователски центрове, международни организации, държавни органи и стопански субекти.<br><br>Улеснявайки взаимодействието между страните, целта на тези споразумения е да се повиши качеството и ефективността на преподавателската и изследователската дейност чрез обмен на академичен и неакадемичен персонал, студенти и докторанти, разработване на програми за съвместна бакалавърска и магистърска степен, организиране на съвместни конференции и други научни събития, участие в съвместни изследователски проекти, обмен на опит и академична информация, учебни програми, материали и други.<br><br>УНСС провежда обучение за магистърска степен по управление на киберсигурността и е подписал споразумения за сътрудничество с Министерството на вътрешните работи на Република България, Съвместния изследователски център на Европейската комисия – Брюксел (JRC), Център за европейски университетски изследвания – Виена (CEUS), Международна агенция за атомна енергия – Виена (IAEA), Организация на ООН за индустриално развитие – Виена (UNIDO) и други.<br><br>Участието в академични съюзи и мрежи е друг начин за улесняване на сътрудничеството. Например, УНСС е член на ENGAGE.EU - алианс от водещи европейски университети в областта на бизнеса, икономическите и социалните науки, целящ да предостави на |

европейските граждани набор от умения и компетенции, необходими за справяне с основните обществени предизвикателства.

Алиансът използва уникалната синергия на своите членове, издигайки съществуващото сътрудничество до ново измерение под ръководството на обща стратегия и общи цели. УНСС е член и на Асоциацията на икономическите университети от Южна и Източна Европа и Черноморския регион, Черноморската университетска мрежа, Черноморската и Средиземноморската академична мрежа и други.

## Онлайн интерактивно обучение за ролята на главния информационен мениджър (CIO)

На 18 януари 2021 г. се проведе онлайн интерактивно обучение за ролята на главния информационен мениджър (CIO) за Българската академия на науките и големите български университети.

Обучението беше организирано като продължение на по-ранна консултативна среща на високо ниво относно разработването на стратегия за дигитална трансформация и дигитализация на БАН и българските университети. Водещ на обучението беше професор по системна сигурност от университета в Ковънтри.

Заместник-вицеканцлерът и главен оперативен директор в университета Ковънтри беше консултант на тази среща (проект SIN, декември 2019 г.).

По време на обучението за CIO, чрез интерактивен урок, професорът от Обединеното кралство проведе обща сесия за възгледа на университета в Ковънтри относно критичната роля и функция на CIO в съвременните организации. Последвалата интерактивна сесия „Упражнения, базирани на сценарий за кибер заплахи" предостави възможност на българските участници да практикуват ефективна реакция на потенциалните кибер атаки.

Упражненията, базирани на реални инциденти, бяха предназначени за изграждане на информираност и по-добро разбиране на кибер рисковете и потенциално ефективни стратегии за смекчаване на последиците, за изграждане на ключови умения и договорени отговорности. Обучението завърши с обратна връзка за резултатите и обсъждане на заключенията.

Получените знания по време на събитието ще бъдат използвани от българските участници за разработване на програми за обучение на CIO в различни институции в страната.

Упражненията бяха част от изследователски проект, реализиран от университета в Ковънтри, изследващ фактори, които формират вземането на решения за киберсигурност, като се стремят да разберат как хората реагират на кибер инциденти и да предоставят насоки за действие. Отговорите на участниците на хипотетични кибер инциденти бяха оценени, за да дадат представа за взимането на решения и тенденциите за реакция.

Присъстваха български участници от широк кръг институции: Институт по информационни и комуникационни технологии - БАН; Лаборатория по телематика - БАН; Институт по органична химия - БАН; Технически университет - София; Военноморска академия - Варна; Университет за национално и световно стопанство; Университет по библиотекознание и информационни технологии; Институт по публична администрация; Национален институт по отбрана; Държавна агенция за електронно управление; Министерство на отбраната; Министерство на вътрешните работи.

Това събитие беше продължение на голямото сътрудничество между SIN България, Университета в Ковънтри и български заинтересовани страни в областта на киберсигурността в академичните среди и университетите.

## Кибер институции и инициативи във Великобритания и България

### Британски национален център за киберсигурност (NCSC)

Стартирал през октомври 2016 г., **NCSC** има седалище в Лондон и обединява експертни познания от CESG (подразделението за осигуряване на информация на GCHQ), Центъра за кибер оценка, CERT-UK и Центъра за защита на националната инфраструктура.

NCSC осигурява единна точка за контакт за МСП, по-големи организации, държавни агенции, широката общественост и отделите. Също така работи съвместно с други органи на реда, отбраната, агенциите за разузнаване и сигурност на Обединеното кралство и международни партньори.

Дейностите на NCSC се определят, както следва:

- разбира киберсигурността и превръща тези знания в практически насоки, които предоставя на всички;
- реагира на кибер инциденти, за да намали вредата, която причиняват на организациите и на Обединеното кралство като цяло;
- използва промишлен и академичен опит, за да развие способността на Обединеното кралство за киберсигурност;
- намалява рисковете за Обединеното кралство чрез защита на мрежите от публичния и частния сектор.

Сертифицирани по NCSC степени

С толкова много университети в Обединеното кралство, предлагащи образователни степени по киберсигурност, за студентите и работодателите може да е трудно да оценят предлаганото качество и да определят степента, която най-добре отговаря на кариерното им развитие. Сертифицираните по NCSC степени помагат на:

- университетите да привличат висококачествени студенти от цял свят;
- работодателите да наемат квалифициран персонал и да развиват кибер уменията на съществуващите служители;
- бъдещите студенти да правят по-информиран избор, когато търсят високо оценена квалификация.

### Националната агенция за оценка и акредитация (НАОА)

Българската национална агенция за оценка и акредитация (**НАОА**) е държавен орган за оценка, акредитация и мониторинг на качеството във висшите учебни заведения и научни организации с цел подобряване на тяхното преподаване и изследванията, както и на тяхното развитие като научни, културни и иновативни организации.

Агенцията следи способността на институциите, техните основни звена и клонове да осигуряват добро качество на образование и научни изследвания чрез вътрешна система за осигуряване на качеството.

Мисията на НАОА е да насърчава висшите учебни заведения да осигуряват и подобряват качеството на образованието, което предлагат чрез поддържане на високи академични стандарти и добри образователни традиции в България.

Акредитирани висши училища

Акредитирани докторски програми по киберсигурност

## Новини за киберсигурността

### Приета е Националната стратегия за киберсигурност

Националната стратегия за киберсигурност „Кибер устойчива България 2023“ (актуализирана стратегия за киберсигурност) е приета от Министерския съвет на 31 март 2021 г.

Стратегията е разработена от междуведомствена експертна група и съгласувана със Съвета за сигурност към Министерския съвет на

| | |
|---|---|
| **„Кибер устойчива България 2023“**<br>(www.c4isrnet.com) | Република България. Проектът на стратегията беше публично обявен за консултация между 11 и 24 февруари 2021 г.<br>Пътната карта за изпълнение на Стратегията за киберсигурност се очаква в рамките на шест месеца след приемането на стратегията и ще включва всички свързани заинтересовани страни.<br>Пълният текст на стратегията може да бъде намерен тук. |
| **Позицията на национален кибер директор в Белия дом**<br>(www.lawfareblog.com) | Законът за авторизация на националната отбрана (NDAA) за фискалната 2021 г., създаде кабинета на националния кибер директор в изпълнителния кабинет на президента. Офисът ще се ръководи от първия национален кибер директор на САЩ и е предназначен да ръководи прилагането на националната кибер политика и стратегия, с акцент върху бързия напредък във вътрешната киберсигурност. Директорът ще бъде старши съветник на президента по киберпространството.<br>Създаването на кабинета на националния кибер директор идва в ключов момент в развитието на киберсигурността на нацията и по петите на един от най-широко разпространените кибер инциденти, нанасяни някога в страната. Водещата национална кибер агенция, Агенцията за киберсигурност и сигурност на инфраструктурата (CISA) към Департамента за вътрешна сигурност, продължава бавно да узрява в своята решаваща роля. Все още в разгара на президентския преход президентът Байдън започна да организира своя персонал в Белия дом, включително със създаването на заместник-съветник по националната сигурност за кибер и нововъзникващите технологии.<br>Докато Байдън ясно даде да се разбере, че киберсигурността ще бъде основен приоритет за неговата администрация, и създаването на новата длъжност заместник-съветник по националната сигурност със сигурност е показателно за това. Стечението на тези събития и създаването на кабинета на националния кибер директор доведе някои наблюдатели от администрацията, частния сектор и медиите, за да задават въпроси за същността и ролята на новия офис. NDAA предоставя ясни описания на няколко мандата на службата. Но остават въпроси относно мотивацията за създаването на офиса, неговите власти и как той е свързан с други кибер релевантни роли в Белия дом. |
| **Подкрепа за образователния сектор в Обединеното кралство след растежа на кибер атаките**<br>(www.ncsc.gov.uk) | Националният център за киберсигурност (NCSC), който е част от GCHQ, публикува предупреждение до образователните институции, в което предупреждава за увеличаване на броя на атаките на ransomware и излага стъпки, които те могат да предприемат, за да не позволят на престъпниците да попаднат в техните мрежи.<br>Въпреки че оперативните подробности не могат да бъдат разкрити, NCSC се справи със значително увеличение на броя на атаките от края на февруари, когато училищата се подготвяха да посрещнат учениците в класната стая.<br>Няма причина да се подозира, че зад всяко нападение стои един и същ престъпник, който е причинил различни нива на прекъсване, включително насочване на училищни финансови записи. |
| **78% от топ лидерите по сигурността казват, че техните организации не са подготвени за кибер атака**<br>(www.scmagazine.com) | Седемдесет и осем процента от топ лидерите в областта на информационните технологии и сигурността смятат, че техните организации нямат достатъчна защита срещу кибер атаки, според проучване, проведено от IDG Research Services от името на Insight. Високото ниво на загриженост, изразено от тези лидери, доведе до това, че 91% от организациите увеличиха бюджетите си за киберсигурност през 2021 г. – което е близо до 96% от 2020 г., когато се увеличиха разходите за ИТ сигурност. |

| | |
|---|---|
| **Хак над Microsoft: Байдън стартира спешна работна група за справяне с кибер атаката**<br>(www.theguardian.com) | Администрацията на Байдън стартира спешна работна група за справяне с агресивна кибер атака, която засегна стотици хиляди клиенти на Microsoft по целия свят - втората голяма хакерска кампания, която удари САЩ след изборите.<br>Атаката, съобщена за първи път от изследователя по сигурността Брайън Кребс на 5 март, позволи на хакерите да получат достъп до имейл акаунтите на поне 30 000 организации в САЩ.<br>Тези обратни канали за отдалечен достъп могат да засегнат кредитните съюзи, градските управи и малкия бизнес и оставиха американските длъжностни лица да се превърнат жертви, а ФБР в неделя ги призова да се свържат с правоприлагащата агенция. |
| **Северна Корея е обвинена в хакване на Pfizer за данни относно ваксината срещу Covid-19**<br>(www.bbc.com) | Северна Корея се опита да открадне технологията за ваксините срещу Covid-19 от американската фармацевтична компания Pfizer, според служители на южнокорейското разузнаване. Понастоящем не е ясно какви данни са откраднати, ако има такива.<br>Националната агенция за разузнаване на Южна Корея информира частно законодателите за предполагаемото нападение, съобщи местната информационна агенция Yonhap.<br>BBC поиска от Pfizer коментар, но все още няма такъв. |

## Обратна връзка

| | |
|---|---|
| За въпроси и препоръки | E-mail: acerta@bas.bg |

## Редакционен съвет

| | |
|---|---|
| Академична CERT (ACERTA) организация съгласно споразумение, подписано от група академични органи (ИИКТ, ИО-МО, ЕСИ-ЦИЕ, като начало), за засилване на сътрудничеството в изследванията, свързани с киберсигурността | 1. доц. д-р Велизар Шаламанов – зам. Директор на ИИКТ-БАН<br>2. проф. д-р Тодор Тагарев – ИИКТ-БАН<br>3. проф. д.н. Даниела Борисова – ГИМ, ИИКТ-БАН<br>4. доц. д-р Златогор Минчев – ГМИС, ИИКТ-БАН<br>5. полк. доц. д-р Николай Стоянов – зам. Директор на Института по отбрана към МО<br>6. д-р Георги Шарков – управител на фондация Европейски софтуерен институт – Център Източна Европа<br>7. Светлин Илиев – Съюз за стопанска инициатива |

Публикуването на бюлетина се реализира с финансовата подкрепа на Британското посолство в София.

Бюлетинът отразява гледната точка на авторите.

British Embassy Sofia

IICT Institute of Information and Communication Technologies

Bulgarian Defense Institute

ESI European Software Institute Center Eastern Europe

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE