ISSN 2738-7089 https://doi.org/10.11610/cybsec04bg

British Embassy Sofia

Информационен бюлетин за киберсигурност

IICT Institute of Information and Communication Technologies

Британско-българско партньорство в киберсигурността за МСП и организации

Бюлетин януари 2021 Номер 4

Цели и обхват

Съдържание:

Настоящият онлайн бюлетин No 4 е фокусиран върху цифровата трансформация и движещата роля на киберустойчивостта. Представяме преглед на проект в Института по информационни и комуникационни технологии на Българската академия на науките (ИИКТ-БАН) в партньорство с академични институции, Държавната агенция „Електронно управление" и с Института за публична администрация за определяне на модела за цифровата трансформация и киберустойчивост в публичния сектор.

В дефинираните 4 квадранта и две нива на промяна в този бюлетин се акцентира върху научните изследвания и образованието като две нива в академичния квадрант, където вярваме, че е ключовата възможност да се повлияе на промяната на процесите, организациите, технологиите и хората - четирите стълба на цифровата трансформация, подкрепена от усилията за устойчивост на новия кибер-домейн. Затова поставяме фокус върху изследванията и образованието за управление на промените, свързани с цифровата трансформация и особено киберсигурността.

Логичната следваща част в изданието е представяне на четирите пилотни проекта по програма „Хоризонт 2020" на ЕС в областта на киберсигурността. Прилага се регламент за създаване на Европейски център за компетентност в областта на индустрията, технологиите и научните изследвания и Мрежата от национални координационни центрове.

Както и в предишните издания, и в този брой са представени полезни новини за киберсигурността, свързани с цифровата трансформация и изследователската и образователна дейност.

Намирайки се в периода на актуализация на българската Национална стратегия за киберсигурност и посветени да я подкрепим с Националната програма за киберсигурност, представяме накратко втората Британска програма за национална сигурност от 2016 г. като добра практика, която да следваме в България.

В подготовка за прилагането на Регламента за създаване на Европейски център за компетентност в областта на индустрията, технологиите и научните изследвания и Мрежата от национални координационни центрове, всяка държава-членка на ЕС трябва да уведоми Комисията в срок от 6 месеца за своя Национален координационен център. Затова представяме накратко българския CERT, изпълняващ отчасти такава функция, с възможност за допълнително разширяване, особено в академичната област, чрез тясно сътрудничество с ИИКТ-БАН като национална изследователска институция за кибериследвания, високопроизводителни изчисления и изкуствен интелект.

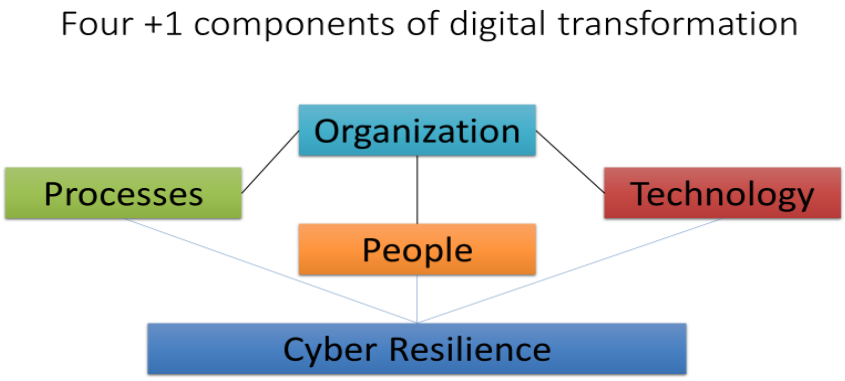
Редактори на броя: доц. д-р Велизар Шаламанов
асистент Ирена Младенова

Фокус на изданието: Цифрова трансформация и киберустойчивост

Доц. д-р Велизар Шаламанов, Зам. директор на ИИКТ по електронна инфраструктура и сигурност, редактор на изданието

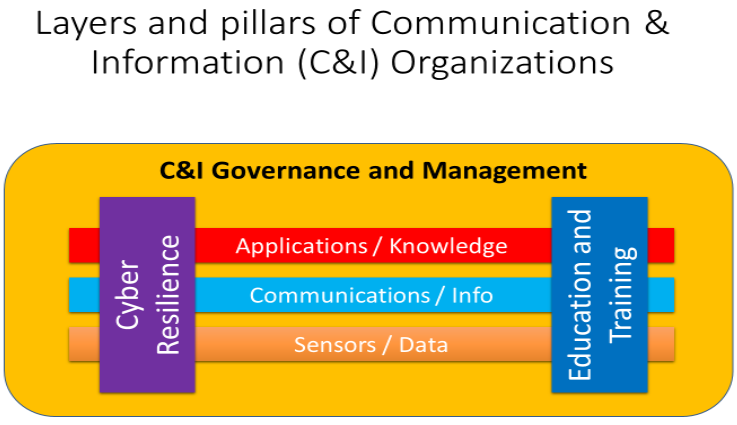
Асистент Ирена Младенова, Софийски университет „Св. Климент Охридски“, Стопански факултет, редактор на изданието

Разглеждайки трансформацията като спирален процес на управление на промените в четири области - процеси, технологии, организация и хора (фиг. 1), определено бихме могли да добавим киберустойчивостта като специфичен пети домейн. Решаващо значение за успеха на цялостната трансформация е цифровата трансформация и промените в тази област, тъй като ние създаваме истинско ново глобално общо пространство – киберпространство, изцяло проектирано от нас, хората, и ние носим отговорността да осигурим структурата му.



Фиг. 1. Кибер устойчивостта като допълнителен компонент за цифрова трансформация

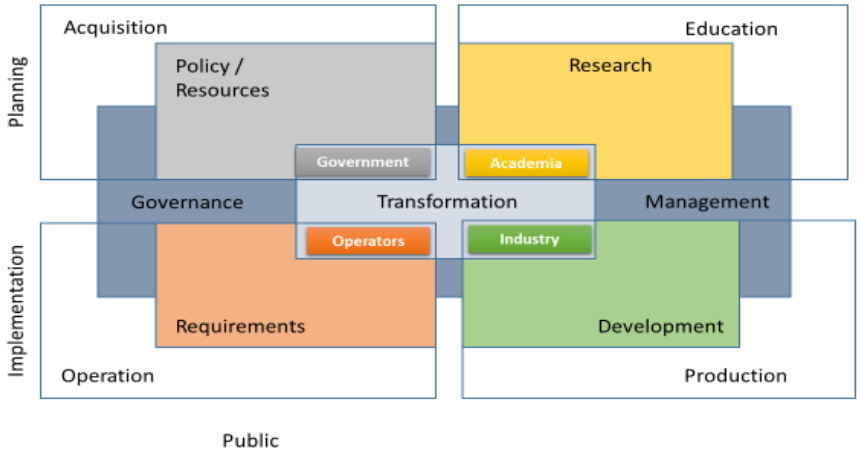
Сърцевината на цифровата трансформация са разработените системи за комуникация и информация (C&I) за подпомагане на процесите във всички области на човешката дейност и осигуряване на коренно нова организация на нашия живот. Той създава много нови зависимости и уязвимости, така че фокусът да е върху киберустойчивостта на структурата с непрекъснато усъвършенстване, особено на човешкия елемент на това ново пространство чрез образование и обучение. По този начин на фиг. 2. бихме могли да разгледаме киберустойчивостта и образованието, обучението като стълбове на системите за C&I, състоящи се от своя страна от три слоя: сензори/данни, комуникации и компютърна инфраструктура и приложения/знания.



Фиг. 2. Слоеве и стълбове на C&I системи

От решаващо значение за успеха в цифровата трансформация и експлоатацията на произтичащите от това системи за управление е пакетът администриране и управление. Така се гарантират

оптимални решения и тяхното прилагане при използване на ИКТ ресурси за постигане на бизнес целите. За да бъде успешна, трансформацията изисква участие на различни заинтересовани страни, както е показано на фиг. 3 на две спирални нива - изследвания, политика, изисквания, развитие от една страна, и производство, образование, придобиване, експлоатация от друга.



Фиг. 3. Спирален процес на промяна в 4 квадранта

Тази спирала на трансформация изисква най-ефективен и ефикасен модел на управление в мрежова среда, тъй като елементът на цифровата екосистема принадлежи към различните по природа сфери - административни, академични, бизнес, професионални оператори.

От 2018 г. в ИИКТ-БАН проектът стартира с цел да консолидира "островите" на компетентност за цифрова трансформация и киберустойчивост в академичната общност на България и да го организира в съвместна мрежа за предоставяне на услуги, финансирани от публичната администрация, МСП и други потенциални клиенти за подобряване на иновационния капацитет и повишаване на конкурентоспособността на българските публични институции и МСП. Освен това тази консолидация върви ръка за ръка с по-дълбоката интеграция на българската академична общност в изследователската общност на ЕС и научното сътрудничество между членовете на НАТО.

Визията на проекта е да оптимизира управлението на научноизследователските дейности в областта на БАН като център за съвместна академична мрежа от компетенции на ИКТ в подкрепа на цифровата трансформация и киберустойчивостта на публичните институции (включително сектора на сигурността), МСП и други клиенти за подобряване на иновациите и конкурентоспособността на българската цифрова екосистема. Разработването на солидна рамка за управление и осигуряване на стратегическо и бизнес планиране, разработване на партньорство, управление на каталози, управление на иновации на съответната инфраструктура за научноизследователска и развойна дейност и развитие в областта на цифровите технологии ще бъде основата на академичната част на националната (ЕС, НАТО) цифрова екосистема.

Стратегията, която трябва да се следва, започва с консолидирането на единиците в ИИКТ и БАН като цяло, за да се създаде център за привличане и обединяване на академични „острови" на компетентност в областта на ИКТ от университети и

институти извън БАН, както и от иновативни компании и стартиращи фирми. С първоначалното финансиране на този проект академичната мрежа трябва да постигне зрялост на проектирана и ориентирана към услуги организация с капацитет да поддържа развитието си като се финансира от клиенти с ограничен (текущи нива на централно бюджетно финансиране) основен бюджет за справяне с изискванията за управление и без високи режийни разходи за проектите и предоставяните услуги.

Изследвания, образование и обучение по киберустойчивост и управление на промените

Изследвания, образование и обучение по кибер устойчивост и управление на промените

Както беше представено по-горе в четирите квадранта на трансформация, този, който бихме могли да разгледаме като отправна точка и сериозен двигател за спиралите на промяната, е академичният квадрант в две нива: изследвания и образование/ обучение. За да разберем изискванията и перспективата за развитие на този квадрант, трябва да го поставим в контекста на управлението на промените и непрекъснатото подобряване на цифровата екосистема.

Когато се опитваме да дефинираме изследователската програма в областта на цифровата трансформация и киберустойчивостта, очевидно не можем да останем само в областта на C&I технологиите, а трябва да се справим и с предизвикателствата на управлението. Този сложен процес на цифрова трансформация ни води в киберпространството с всички потенциални уязвимости, рискове и реални заплахи, с които да се справим чрез програмата за киберсигурност/устойчивост.

Управлението на промяната все повече се превръща в едно от ключовите управленски умения, за да се отговори на - както и да се влияе върху – средата и предизвикателствата и възможностите, които тя предлага. Съществува богат набор от академични и практически изследвания, които се обединяват около това кои са факторите, влияещи върху успеха на една инициатива за промяна. Те включват яснота на визията, достатъчно гъвкава структура и процеси, трансформационно лидерство, овластени агенти за промяна, коалиция от поддръжници.

Цифровата трансформация и киберустойчивостта поставят ясно очертана визия с последици в редица сектори, системи и институции. Кризата с COVID-19 значително стимулира цифровата трансформация, дори в сектори, за които се очакваше да отнеме много повече време, за да се цифровизират – сред които училища, университети, правителства. Но също така подчерта колко уязвими могат да бъдат те в киберпространството и даде да се разбере, че решенията са сложни. За да се увеличи сложността, различни и многобройни играчи участват в създаването на цялостната програма за киберсигурност и устойчивост - на организационно, национално и европейско ниво. Необходимата промяна може да се разглежда на най-малко две нива: мезо (организации) и макро (държави, ЕС).

На *макро ниво* очертаването на стратегията за прилагане на визията и след това успешното ѝ изпълнение е инициатива за трансформационни промени, засягаща голяма система. Тя би изисквала развитие и обучение на агентите за промяна и трансформационните лидери, които да я осъществят. Следователно, за да се разработва и внедрява системата за

управление на национално и европейско ниво, образованието и обучението по управление на промените са също толкова необходими, колкото и образованието и обучението по решения, практики и политики за киберсигурност.

Съществуват редица изследвания за промяната в големи системи, виртуални организации и мрежи за сътрудничество, но с нарастването на значението на такива структури разбирането им ще трябва да се задълбочи. Механизмите, темпото и обхватът на промяната в такива структури се различават от традиционните организации и това налага коригиране на подходите.

На *мезо ниво* подобни изисквания се прилагат за организациите - управлението на киберзаплахи и уязвимости може да изисква значителни промени в организационните процеси, системи и практики. Увереността, че работят, зависи както от техническите решения, така и от служителите, които действително ги прилагат и следват. Това може да изисква сериозна промяна на индивидуално ниво (нови умения, нови процедури), която често сее придружава от съпротива, цинизъм и в крайна сметка провал. Ето защо проектите трябва да повишат осведомеността за необходимостта от промяна, да създадат усещане за неотложност и желание, да предоставят информация и инструменти на засегнатите от промените хора, да премахнат преградите и да получат подкрепа.

Технологичната промяна в организациите е широко изследвана област. И все пак често цитиран факт е, че повечето инициативи за промяна не успяват да постигнат своите желани резултати. Контекстът и организационните специфики изискват подходи, съобразени с конкретните изисквания, и напредъкът в изследванията на организационните промени може да предостави ценни данни.

Предоставянето на необходимите умения и инструменти за ефективно и успешно ръководство на промяната на трансформационните лидери и агентите на промяната - както на мезо, така и на макро ниво - трябва да бъде неразделна част от научните изследвания, образованието и обучението в подкрепа на кибер-програма за сигурност/устойчивост.

Четири пилотни проекта на ЕС в областта на киберсигурността и Европейски център за компетентност по киберсигурност

Усилията за научноизследователска и развойна дейност на ЕС в киберсигурността

Четири пилотни проекта - ECHO, CS4E, CONCORDIA и SPARTA бяха финансирани по програма „Хоризонт 2020" с цел да се свържат и подобрят споделянето и изграждането на знания в различни области и държави-членки. Очакванията са четирите пилотни проекта заедно да помогнат за оформянето на способностите за киберсигурност и устойчивост в Европа и да разработят обща стратегия и екосистема за киберсигурност. Проектите споделят една и съща визия, но се различават по обхванатите аспекти и области.

Европейският център за компетентност (ECC) ще бъде важна част от мрежата за компетентност в областта на киберсигурността, целяща да помогне на Европа да запази и развие капацитета, необходим за осигуряване на цифровия единен пазар.

ECHO – Европейската мрежа от центрове за киберсигурност и компетентният център за иновации и операции (ECHO) включва

30 партньора от различни области и сектори, включително здравеопазване, транспорт, производство, ИКТ, образование, изследвания, телекомуникации, енергетика, космос, здравеопазване, отбрана и граждански защита.

Основната цел на ECHO е да засили проактивната киберзащита на Европейския съюз, засилвайки технологичния суверенитет на Европа чрез ефективно и ефикасно сътрудничество между много сектори и домейни. Проектът ще разработи европейска екосистема за киберсигурност, за да подпомогне сигурното сътрудничество и развитието на европейския пазар, както и да защити гражданите на Европейския съюз от кибер заплахи и инциденти.

Основните концепции на ECHO са:

- Модел на управление: управление на насоките и ангажираност на партньори (настоящи и бъдещи)
- Рамка за многосекторна оценка на ECHO: Напречни и междусекторни оценки на потребностите и пътни карти за научноизследователска и развойна дейност
- Рамка за киберумения и учебна програма на ECHO: Референтен модел за кибер умения и свързана с нея учебна програма
- Схема за сертифициране на сигурността на ECHO: Разработване на специфични за сектора нужди от сертифициране на сигурността в рамките на ЕС за сертифициране на киберсигурността от ENISA
- Федералната кибергама на ECHO: усъвършенствана среда за киберсимулация, подкрепяща обучение, научноизследователска и развойна дейност и сертифициране
- Система за ранно предупреждение ECHO: Осигурен съвместен обмен на информация, свързана с киберинформация

CS4E – Консорциумът CyberSec4Europe (CS4E) се състои от 43 партньора и обхваща широк спектър от въпроси, свързани с киберсигурността: 14 ключови области в областта на киберсигурността, 11 елемента на технологии/приложения и девет ключови вертикални сектора.

Основната цел на CyberSec4Europe е да даде начало на консолидацията и бъдещото планиране на способностите за киберсигурност, необходими за осигуряване и поддържане на европейската демокрация и целостта на цифровия единен пазар. CyberSec4Europe превръща тази широка цел в измерими, конкретни стъпки: три цели на политиката, три технически цели и две цели за иновации.

Като изследователски проект CyberSec4Europe работи за хармонизиране на процеса по разработване на софтуерни компоненти, отговарящи на изискванията, определени от набор от краткосрочни и дългосрочни пътни карти, което води до поредица от последващи препоръки. Те са свързани с реални случаи на демонстрационна употреба на проекта, които се занимават с предизвикателствата в областта на киберсигурността във вертикалните сектори на цифровата инфраструктура, финансите, правителството и интелигентните градове, здравеопазването и транспорта.

CONCORDIA – Консорциум за киберсигурност за изследвания и иновации (CONCORDIA) се състои от 46 партньори,

представляващи водещи университети, предприятия, публични органи и организации.

Основната цел на CONCORDIA е да ръководи интегрирането на отличните европейски компетенции по киберсигурност в мрежата от експертни знания за изграждане на европейската сигурна, устойчива и надеждна екосистема.

Консорциумът има 12 цели в областта на изграждането на екосистема за киберсигурност с отворен и адаптивен модел на управление - разработване на пътна карта и решения за киберсигурност, мащабиране на научните изследвания и иновации и идентифициране на продаваеми решения, работа с множество общности, подкрепа на предприемачи и създаване на образователна екосистема.

SPARTA – Консорциумът SPARTA включва 44 партньора от различни области и сектори.

Мисията на SPARTA е да преосмисли начина, по който се извършват изследвания в областта на киберсигурността, иновации и обучение в Европа в различни области и опит (от създаването до приложението им) в академичните среди и индустрията.

SPARTA изпълнява 4 основни програми:

- T-SHARK - изследва иновативна работа с пълен спектър на ситуацията, с цел да се даде възможност за наблюдение на сложни системи в хетерогенни времеви мащаби.
- CAPE - изследва нови пътища за непрекъснато оценяване и нови инструменти и техники за работа с утрешните динамични и еластични цифрови системи.
- HAII-T - разработва основа за интелигентна инфраструктура със сигурен дизайн, изградена върху силни официални подходи, насочена към множество аспекти на киберсигурността.
- SAFAIR - разработване на подходи за повишаване на надеждността и устойчивостта на системите, използващи AI, чрез подобрено обяснение и по-добро разбиране на заплахата.

И четирите пилотни проекта работят активно с общностите и привличат нови участници.

Европейски център за компетентност в областта на киберсигурността. На 11 декември 2020 г. институциите на ЕС постигнаха политическо споразумение относно Центъра за компетентност по киберсигурност и Мрежата на националните координационни центрове (NCC) - инициатива, насочена към подобряване и укрепване на технологичния и индустриален капацитет на ЕС за киберсигурност и към спомагане за създаването на безопасна онлайн среда.

Центърът за компетентност по киберсигурност ще бъде разположен в Букурещ, и ще има за задача да подпомогне и координира работата на мрежата и да насърчи общността по компетентност по киберсигурност. За целта Центърът и Мрежата ще обединят ресурси от ЕС, държавите-членки и индустрията за подобряване и укрепване на технологичния и индустриален капацитет за киберсигурност, засилвайки отворената стратегическа автономия на ЕС.

	Задачите на Центъра са: • Създаване и подпомагане на координацията на мрежата за обмен на национални координационни центрове и общността по компетентност по киберсигурност. • Прилагане на финансова подкрепа, свързана с киберсигурността, от програмите Хоризонт Европа и Дигитална Европа. Центърът и Мрежата за компетентност в областта на киберсигурността ще помогнат на ЕС и държавите-членки да вземат проактивна, дългосрочна и стратегическа перспектива към изследванията, развитието и индустриалната политика. Този подход трябва да помогне не само да се намерят пробивни решения на предизвикателствата, с които се сблъскват частният и публичен сектор, но и да подпомогне ефективното внедряване на тези решения. Центърът и Мрежата заедно ще подобрят нашия технологичен суверенитет чрез мащабни проекти за киберсигурност в области като интелигентни киберзаплахи, киберзащитен хардуер, операционни системи и сертифициране на сигурността.

Новини за киберустойчивост

Въздействие на COVID-19 върху SecOps: Повишени заплахи, по-големи инвестиции в автоматизацията (www.helpnetsecurity.com)	Siemplify пусна проучване, което изследва как внезапното преминаване към работа от разстояние по време на пандемията на COVID-19 е повлияло на способността на анализаторите на SecOps да изпълняват своите задачи и въздействието върху цялостните позиции на сигурността. Общата позиция на киберсигурността остава силна поради по-големите инвестиции в технологии за автоматизация на сигурността и разчитането на управлявани доставчици на услуги за сигурност (MSSP), което потенциално проправя пътя на много центрове за оперативна сигурност (SOC) да станат постоянно отдалечени, разкрива проучването. SecOps е силно сътрудническа функция, като анализаторите на сигурността работят в тясно сътрудничество във физически SOC, за да адресират десетки хиляди сигнали и инциденти със сигурността ежедневно, да търсят заплахи и да отговорят на проблемите.
Катарският изследователски център избира Леонардо за кибергама (www.defensenews.com)	Катарски кибер изследователски център избра Леонардо да осигури кибер гама и система за обучение в подкрепа на операциите по сигурността, обяви италианската фирма на 3 февруари. Катарският изследователски институт за изчисления (QCRI) е създаден от Катарската фондация за образование, наука и общностно развитие. Платформата за обучение, поръчана от QCRI, е способна да симулира кибератаки, така че потребителите да могат да оценят устойчивостта на цифровата инфраструктура.
Уязвимости в приставката WordPress на NextGEN Gallery изложиха много сайтове на риск от това да бъдат взети (www.securityweek.com)	Две сериозни уязвимости в приставката WordPress на NextGEN Gallery можеха да изложат на риск над 800 000 уебсайта от това да бъдат взети, съобщи наскоро компанията за сигурност на WordPress Defiant. Предлаганата повече от десетилетие приставката предоставя на потребителите широк спектър от възможности за управление на галерии, като групово качване на снимки, импортиране на метаданни, редактиране на миниатюри, управление на снимки и галерии и др. През декември 2020г. изследователи на сигурността с екипа на Wordfence на Defiant откриха две уязвимости за фалшифициране на заявки между сайтове (CSRF) в популярния плъгин, най-тежката от които може да доведе до дистанционно изпълнение на код (RCE) и съхраняване на скриптове между сайтове (XSS).

Американските агенции публикуват информационна таблица за Ransomware (www.securityweek.com)	Националната съвместна работна група за киберразследване (NCIJTF) наскоро публикува съвместно запечатан информационен лист за Ransomware, който подробно описва общите техники за нападение и средствата за осигуряване на превенция и смекчаване. Информационният бюлетин е разработен от междуведомствена група експерти по Ransomware от повече от 15 правителствени агенции и има за цел да спомогне за повишаване на осведомеността относно заплахата, която Ransomware представлява за критичната инфраструктура. Документът от две страници обяснява, че в допълнение към криптирането на данните на системите за жертви, за да ги направят неизползваеми, операторите на Ransomware могат също да окажат натиск върху жертвите да платят откупа, като заплашат да унищожат данните или да ги предоставят на обществеността. Атаките с Ransomware засягат всички сектори, включително държавни, местни, племенни и териториални правителства, но също така засягат болници, полиция, пожарни служби, общини и друга критична инфраструктура.
Microsoft поправя Windows Zero-Day в Patch Rollout (www.darkreading.com)	Месечните корекции на сигурността на Microsoft адресираха нулев ден на Win32k, шест публично известни недостатъка и три грешки в стека на Windows TCP/IP. Microsoft вече е коригирала уязвимостта на нулевия ден на Windows като част от ежемесечното си разпространение на Patch, което коригира относително малък брой общи уязвимости и експозиции (CVE), но което има голям брой публично известни грешки. 56-те уязвимости отново съществуват в Microsoft Windows, .NET framework, Windows Defender, Azure IoT, Azure Kubernetes Service, Exchange Server, Skype за бизнес и Lync, Office Services, уеб приложения и Microsoft Edge за Android. Единадесет от тези недостатъци са класифицирани като критични по тежест, 43 са важни и два са умерени.
Екипите на SOC прекарват почти една четвърт от деня си, обработващи подозрителни имейли (www.scmagazine.com)	Специалистите по сигурността знаят, че реагирането на безмилостни, входящи потоци от подозрителни имейли може да бъде трудоемка задача, но ново проучване, споделено предварително за SC Media, показва колко време отнема всъщност. Изследователи от фирма за защита на имейли Avanan твърдят, че са автор на „първото цялостно изследователско проучване", което определя количеството време, което служителите на Центъра за сигурност (SOC) отделят за предотвратяване, реагиране и разследване на имейли, които успешно са заобиколили сигурността по подразбиране и са маркирани от крайните потребители или други механизми за докладване.
Осигуряване на класифицирана работа от разстояние: 3 Принципи за защита на чувствителни данни (www.tenable.com)	Тъй като ограниченията на пандемията продължават, федералните агенции се подготвят за покачване на класифицираната телеработа. Ето защо непрекъснатото съсредоточаване върху основите на киберсигурността е наложително. Пандемията COVID-19 ускори преминаването към работа от разстояние над всички предишни очаквания. Въпреки че имаше много изключения от правилото в ранните дни на отговора на пандемията, виждаме, че тези изключения намаляват, когато отдалечената работна среда узрее. Внезапната нужда от сигурна работа от разстояние доведе до иновации и гъвкавост като необходими атрибути на успешния преход. Лидерите в Агенцията за информационни системи за отбрана (DISA) например коментираха, че това търсене и произтичащите от това подобрения на сигурността са нещо като „сребърна подплата" в пандемичния „облак".
AI трябва да проверява 100	Изкуственият интелект е абсолютен императив за проверка на неприлични количества данни и разузнавателни данни за киберзаплахи, до 100 милиарда елемента на ден, според експерт от

милиарда елемента от киберзаплахи на ден (www.jpost.com)	AI на конференция, анализиращ как проблемът влияе на националната сигурност. Дерек Манки, шеф на прозренията за сигурността на глобалните съюзи за заплахи във Фортинет, направи своите забележки на виртуална конференция, спонсорирана от Института за изследване на методологията на разузнаването и отбраната на Израел.
САЩ и Естония си партниряха, за да издирят киберзаплахата от Русия (www.securityweek.com)	В модерния обрат на старомодните военни игри американската армия изпрати кибер бойци в Естония тази есен, за да помогне на малката балтийска държава да издири и блокира потенциалните кибер заплахи от Русия. Целта беше не само да се помогне на партньор на НАТО, отдавна насочен от могъщия си съсед, но и да придобие представа за руската тактика, която може да се използва срещу САЩ и изборите. Операцията на кибер командването на САЩ се проведе в Естония от края на септември до началото на ноември, разкриха наскоро служители от двете страни, точно когато САЩ работеха за защита на избирателните си системи от чужда намеса. Те запазиха изследванията на коронавируса от чуждия обсег на хакери в страни, включително Русия и Китай.
Предизвикателствата за поддържане на неоспоримо състояние в облака за сигурност (www.helpnetsecurity.com)	В интервю Бадри Рагхунатан, директор на продуктов мениджмънт за контейнерна и безсървърна сигурност в Qualys, разказва за облачната сигурност и техния подход, който позволява на глобалните CISO да се съсредоточат върху най-важното. Използването на публична облачна инфраструктура е масово и предприятията често имат отпечатък в много облаци. Въпреки това, дори след 10+ години публичен облак, предприятията все още се борят с принципа за сигурност на споделената отговорност. Това е свързано с въвеждането на архитектура за сигурност (или набор от принципи), която отговаря на нуждите на организацията и работи в света на публичния облак.

Киберинституции и инициативи във Великобритания и България

Британска национална програма за киберсигурност	**2016 Национална програма за киберсигурност.** Канцлерът е изложил визия за защита на Великобритания срещу киберзаплаха в речта на правителствената комуникационна централа (GCHQ), GOV.UK 2015-11-17 с 1,9 милиарда британски лири в разходи за 2016-2021 г. (същия период за българската национална стратегия за киберсигурност „Киберустойчива България 2020“). Националният център за киберсигурност е домът на "киберсилата" на Обединеното кралство, но за оперативният център за киберсигурност на MoD има 40 милиона паунда. В допълнение, 22 милиона британски лири са отбелязани „за издигане на нови центрове за кибер операции на армията в цяла Великобритания“. Програмата включва инвестиция в размер на 265 милиона британски лири в програма за разследвания за уязвимост в киберпространството (CVI) за MoD. Важна роля се дава на „Института за кодиране: Център за цифрови умения и компютърни науки“ и кампанията „Cyber Streetwise“/ „Cyber Aware“ (cyberaware.gov.uk) за 2015/16 г. с обща стойност 4 милиона британски лири (предишна -VAT) и 3,3 милиона британски лири през 2017/18. Шестмесечен „инкубатор за киберсигурност“, финансиран от **Департамента за цифрова култура, медии и спорт (DCMS)** - инициатива HutZero. Около 10 милиона британски лири се използват за създаване на „Фонд за кибер иновации“. В допълнение, има инвестиция от 14 милиона британски лири („до“)

	в лондонски център за иновации в киберсигурността (Това е финансираният от DCMS LORCA - лондонски офис за бърз напредък в киберсигурността). За центъра на кибер иновациите има 13,5 милиона британски лири. Има 50 милиона паунда ("до") за защита на правителството. Важна за партньорите е Международната програма за изграждане на капацитет за киберсигурност. Създаден е фонд за незабавно въздействие на уменията за киберсигурност (CSIIF) през февруари 2018 г. и с акцент "към края на октомври 2018 г., когато приблизително 170 лица или са участвали, или са били идентифицирани да участват в седемте инициативи, подкрепени от CSIIF." Поради ограниченията на националната сигурност принципът на финансиране чрез Националната програма за киберсигурност е, че правителството не е в състояние да детайлизира индивидуалното финансиране на NCSP по отдел или инициатива. Важен за този брой на бюлетина е фактът, че се планират до 800 000 британски лири за подкрепа на академичните институции в Обединеното кралство в комерсиализирането на иновации в областта на киберсигурността.
CERT-България	**CERT България** е Националният център за реакция при инциденти във връзка с информационната сигурност. Мисията на Центъра е да подкрепи своите потребители в активни дейности за намаляване на рисковете от инциденти по сигурността на информацията и да съдейства за разрешаването им в случай, че те вече са възникнали. Центърът предоставя централизирана база данни с информация, свързана с осигуряване защитена информационна среда. Целите, които трябва да бъдат постигнати, включват: • защита на информационните и технологичните активи; • ограничаване на прякото въздействие на инцидентите със сигурност върху информационното общество; • помощ при възстановяване след инциденти; • оценка на въздействието на инциденти, свързани със сигурността; • събиране и разпространение на техническа информация, свързана с инциденти по сигурността на информацията, както и уязвимости в сигурността на системите и начини за тяхното предотвратяване; • провеждане на изследвания, свързани с новите технологии в мрежовата и информационна сигурност; • провеждане на обучение, свързано с информационната сигурност и управлението на инциденти.
	Връзки към киберинституции/програми
Връзки към български, британски и международни органи	Националната програма за киберсигурност и изследователският съвет за инженерни и физически науки (EPSRC) съвместно признават Академични центрове за върхови постижения в изследванията на киберсигурността (ACE-CSR). След последния панел за оценка 19 университета са признати за ACE-CSR. Тези университети са изпълнили строги минимални стандарти и са доказали, че: • ангажиментите от ръководния екип на университета подкрепят и инвестират в изследователския капацитет и възможности на киберсигурността на университета • критичното количество академичен персонал е ангажирано с водещи изследвания в областта на киберсигурността

- присъства доказан опит в публикуването на силно въздействащи изследвания на киберсигурността във водещи списания и конференции
- имат трайно финансиране от различни източници, за да се гарантира продължаващата финансова жизнеспособност на дейностите на изследователския екип

Докторантски стажове: За да стимулира допълнително изследванията в областта на киберсигурността във Великобритания, NCSC подкрепя докторанти в ACE-CSR. Освен това има три центъра за докторантско обучение (CDT) по киберсигурност под знамето „Доверие, самоличност, поверителност и сигурност". CDT са на адрес:

- Университетът в Бристол с университета на Бат
- Роял Холоуей, лондонски университет
- Университетски колеж в Лондон

Кооперативният център за върховна киберзащита на НАТО е многонационален и интердисциплинарен център за киберзащита.

Военноморската академия „Никола Вапцаров" е най-старата техническа образователна институция в Република България.

Нейната история, минали и настоящи постижения утвърждават институцията като най-престижния център за обучение на морски специалисти в страната. Наскоро Академията откри Център за кибер операции и стартира бакалавърска програма по киберсигурност.

Обратна връзка

За въпроси и препоръки

Имейл: 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

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

DIGILIENCE Conference Series https://digilience.org