ISSN 2738-7089 https://doi.org/10.11610/cybsec18bg

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 Септември 2025 Номер 18

Цели и обхват

Съдържание:

Настоящият брой на информационния бюлетин за киберсигурност и информционна устойчивост е с водеща тема върху одита на киберсигерноста. Одитът на киберсигурността като структурирана проверка и оценка на информационните системи, процеси и политики в една организация цели да установи актуалното ниво на сигурност, наличие на уязвимости и съответствие със стандартите, идентифициране на силни страни и възможности за развитие. Чрез оценка на техническите аспекти, физическата сигурност и човешките практики, одитите разкриват слабости, които биха могли да доведат до нарушения на данните или нарушения на съответствието, предоставяйки практически препоръки за смекчаване и намаляване на риска, както и използване на силните страни, развитието на системата за киберустойчивост. Поради всичко това, одитът на киберсигурността е особено важен, тъй като помага да се предотвратят атаки, изтичане на данни или прекъсвания на дейността, както и укрепване на устойчивостта.

За да разбере по-добре разликата между одит на киберсигурността и оценка на киберсигурността е направено сравнение между тях. Оценка на киберсигурността, известна като анализ на пропуските, се фокусира върху идентифицирането на съществуващите уязвимости в инфраструктурата или системата на организацията. При този вид оценка се включва тестване на технологии, бизнес и човешки процеси, за да се установи дали те са достатъчно устойчиви, за да издържат на кибератаки. Крайната цел е да се идентифицират потенциални заплахи и да се предоставят препоръки за подобряване на сигурността на организацията.

При оценката и одита важен инструмент е и разузнаването по открити източници (OSINT) за анализ на средата, както и използването на изкуствен интелект за автоматизация на оценката/одита, планиране на подобряване на устойчивостта.

В бюлетина са представени събития и полезни връзки за общността през изминалия тримесечен период, както и кратка информация за проведения междинен преглед на проекта CYBER4ALLSTAR от координаторите на европейските центрове за дигитални иновации.

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

Фокус на изданието: Одит на киберсигурността – какво да очакваме, как да го изпълним и какво да правим с резултатите

Проф. Даниела Борисова

Киберсигурността е състояние, но и съществен процес, чрез който предприятията могат да оценят своята позиция по отношение на сигурността в киберпространството, чрез който могат допълнително да подобрят своята устойчивост в отговор на усложнения пейзаж на киберзаплахите. Ефективните одити на киберсигурността могат да се разглеждат като критични инструменти за откриване на слабости в програмата за сигурност и гарантиране, че тези слабости ще бъдат отстранени. Какво всъщност трябва да постигне един одит за киберсигурност и какви възможности в технологии, персонал и ангажираност са необходими, за да направят одитите полезна дейност? Това са въпроси, на които всеки Главен мениджър по информационна сигурност би трябвало да може да отговори.

Каква е целта на одитите за киберсигурност?

Одитите на киберсигурността са систематичен анализ на агентите, политиките и процедурите на организацията, с помощта на който могат да се идентифицират несъответствията, рисковете и уязвимостите в организирането на информационните системи и спазването на стандартите. Основната роля на одита на киберсигурността е да осигури надеждна гаранция, че ИТ инфраструктурата на организацията е непроницаема и готова да изолира кибератаки. Тук трябва да се обединят различни части на киберсигурността, мрежовата сигурност, контрола на достъпа, защитата на данните и стратегиите за справяне с инциденти. Следователно одитът може да се извърши или вътрешно от групата за ИТ сигурност на организацията, или външно от независими одитори от трета страна. Докладът от одита представлява заключителните констатации, където се изброяват силните и слабите страни и се предлагат предложения за подобрение като път напред.

Одитът на киберсигурността проверява дали текущи политики, процедури и контроли ефективно се справят със заплахите за киберсигурността на компанията. Доста често отговорът е „не“. Това може да се дължи на факта, че контролите имат недостатък в дизайна (например, неуспешно внедряване на многофакторно удостоверяване в даден необходим момент) или защото компанията е изправена пред някакъв нов риск, който контролите никога не са били предназначени да адресират. Възможно е също така бизнес операциите да са се променили (да са преместени ключови системи в облака или да се събират нови видове данни) и контролите, които са работили ефективно в миналото, вече не работят ефективно сега.

Какво да очакваме по време на одит на киберсигурността?

Одитите на киберсигурността са предназначени да извадят наяве всички споменати по-горе проблеми и го правят по няколко начина. Например, одиторите тестват контролите, за да видят колко добре работят. Одиторите разговарят с хора от организацията, за да разберат рисковете за сигурността и задълженията за съответствие, така че одиторът да може да оцени дали контролите са правилно проектирани. Най-важното е, че одитът на киберсигурността води до одитен доклад. Този доклад представлява списък с препоръчителни

стъпки за подобряване на всички слабости или проблеми, открити от одитора. По същество, одитният доклад дава план за бъдещи подобрения, следвайки и прилагайки препоръките на доклада.

Защо са необходими одити? Одитите са необходими, за да се постигне съответствие с регулаторните задължения. Например, разпоредбите, регулиращи защитата на личната здравна информация и тези, които защитават данните за кредитни карти изискват одити на програмата за защита на данните като част от спазването на съответните им стандарти.

Одитите по киберсигурност също са ценни, дори отделно от спазването на регулаторните изисквания. В днешния силно взаимосвързан свят, където организациите рутинно предоставят на доставчици на технологии и други трети страни достъп до критично важни системи и данни, трябва да се разбере дали тези трети страни имат надеждни програми за киберсигурност.

Какво обхваща одитът на киберсигурността?

Одитът на киберсигурността съпоставя съществуващите политики, процедури и контроли за киберсигурност с желаните контроли на рамката. Това е известно като анализ на пропуските чрез което се откриват пропуски, при които програмата за сигурност не е толкова надеждна, колкото рамката предполага.

Кибер одитите в ИТ инфраструктурата включват политики, процедури и практики, насочени към проверка на контрола, оценка на уязвимостите и прогнозиране на риска. Областите, обхванати от одита на киберсигурността, могат да се различават между организациите в зависимост от индустрията, в която са свързани, регулаторните изисквания, които спазват, рисковия им профил и целите на одита, които се стремят да постигнат. Въпреки това, често срещаните области, включени в одита на киберсигурността, обхващат:

Мрежова сигурност – мрежовата архитектура, конфигурацията и контрола на сигурността на организацията. Сигурността трябва да е гарантирана срещу неволен достъп, нарушения на данните и киберзаплахи. Прегледайте конфигурациите на защитната стена, системите за откриване/предотвратяване на проникванията (IDS/IPS), сегментирането на мрежата, контрола на достъпа и протоколите за криптиране, за да откриете евентуални слабости и уязвимости.

Системна сигурност – проверка на настройки на операционната система, управлението на корекции, антивирусния софтуер, предоставените от доставчиците защити на системата и др., за да се уверим, че цялата чувствителна информация и активи, критични за организацията, са правилно защитени.

Сигурност на данните – протоколи за защита на данните на организацията, за да се предотврати изтичане или промяна на поверителни и лични данни, както и всякакви онлайн или физически кражби в организацията. Разглежда се също криптирането на данни, контрола на потребителския достъп и политиките за класифициране на данни, заедно с решенията и системите за възстановяване след инциденти/бедствия, чрез които се проверява съответствието с регулаторните изисквания и най-добрите практики.

Сигурност на приложението – проверка на нивото на сигурност на уеб приложения, мобилни приложения и други софтуерни решения, за да откриете обектите, които могат да представляват голяма уязвимост, използвана от натрапниците. След завършване се извършва оценка на сигурността, прегледи на кода и сканиране на уязвимости, за да се открият познати недостатъци в сигурността, като SQL инжектиране, cross-site scripting (XSS) и неосигурени механизми за удостоверяване.

Управление на самоличността и достъпа – преглед на процесите на организацията, за да се провери дали потребителите са правилно удостоверени, дали са им предоставени правилните оторизации и дали носят отговорност за достъпа до системи, приложения и данни. Одитиране на процесите за управление на акаунти, мерките за политиката за пароли, механизмите за многофакторно удостоверяване, решенията за контрол на достъпа, базиран на роли и управление на привилегирования достъп до услугите, за да се осигури само оторизиран достъп и да се избегне ескалация на привилегиите.

Подготовка за реагиране при инциденти – оценка на организационната критичност за киберсигурността, тъй като ограничаването, реагирането и възстановяването след киберинциденти са важни. Проверка на плановете за реагиране при инциденти, протоколите и комуникациите, като посочите с кого и кога да комуникирате, преди да реагирате на нарушения на сигурността, нарушения на данните или други киберинциденти. Извършване на симулации и учения, за да оцените дали планът за реагиране при извънредни ситуации е добре изпълнен и дали сътрудничеството между заинтересованите страни отговаря на необходимия стандарт.

Осведоменост и обучение по сигурността – оценка на осведомеността за сигурността и обучението на организацията, за да се гарантира, че служителите, изпълнителите и външните доставчици са много добре обучени да разпознават и реагират на заплахи и проблеми със сигурността. Измерване ефикасността на обучителните материали за повишаване на осведомеността за сигурността, симулацията на фишинг и други средства, чрез които се насърчава култура на предпазливост по отношение на сигурността и се променя поведението в организацията.

Управление на риска от трети страни – анализ на протоколи за управление на риска от трети страни в организацията. Тези протоколи могат да включват материални или нематериални елементи, наследени от партньори, или всякакъв вид доставчици на услуги, които се използват за техните транзакции. Прегледът на договори, споразумения за ниво на обслужване и доклади от одити за сигурност от трети страни е важен, за да се гарантира, че те спазват разпоредбите за сигурност. Проучване на мерките и средствата за сигурност, предоставяни от външни доставчици за елиминиране или смекчаване на излагането на риск от инциденти като атаки по веригата за доставки и нарушения на данните.

Съответствие с нормативните изисквания – проверка, че организацията спазва приложимите регулаторни изисквания, индустриалните стандарти и общоприетите стандарти за сигурност в киберпространството. Проверка на правилата и разпоредбите като GDPR и NIST SP 800-53, които се фокусират върху защитата на данните, поверителността и сигурността, за да се уверите, че изискванията са

изпълнени. Извършване на анализи на пропуските и оценки на съответствието, за да откроите областите на несъответствие, като същевременно определяте и прилагате мерки за отстраняване.

Контролен списък за одит на киберсигурността

(1) **Политики и процедури за сигурност:** Преглед на политиките и процедурите за сигурност (напр. политика за приемливо ползване, политика за пароли); Обучение на служителите по въпросите на сигурността и сертификация; Съответствие с регулаторните изисквания (напр. GDPR); Документация и доказателства за внедряване на контроли за сигурност, политика по инвестиране в киберсигурност.

(2) **Управление на риска за доставчици и трети страни:** Оценка на контролните механизми за сигурност и договорите на доставчиците; Оценки и одити на сигурността от трети страни; Проверка на доставчиците на облачни услуги и други външни доставчици; Мониторинг и управление на достъпа на трети страни до системи и данни.

(3) **Непрекъснатост на бизнеса и възстановяване след бедствия:** Анализ на въздействието върху бизнеса и оценка на риска; Документация и тестване на план за възстановяване след бедствия (DRP); Процедури за архивиране и възстановяване на критични системи и данни; Механизми за резервиране и превключване при срив за основни услуги.

(4) **Съответствие с нормативните изисквания:** Съответствие със специфичните за индустрията разпоредби и стандарти; Документиране на контролите и доказателства за целите на одита; Редовна оценка на състоянието на съответствие и отстраняване на недостатъците; Взаимодействие с регулаторни органи и индустриални групи за насоки и актуализации.

Колко често трябва да провеждате одит на киберсигурността?

Годишният одит на киберсигурността е почти нормална мярка за повечето организации, която определя ефективността на мерките за сигурност и посочва всички възникващи уязвимости или рискове. Този годишен одит дава цялостен преглед на организационната киберсигурност и помага за постигане на съответствие с регулаторните изисквания. Освен това, организациите могат да решат да извършват по-чести одити на киберсигурността, особено в специфични ситуации. Например, когато има големи промени в ИТ средата, като например системни ъпгрейди, сливания или придобивания, или когато се разработи нова технология, може да е полезно да се извърши одит, за да се определи ефектът върху контролите за сигурност.

Одит на киберсигурността или оценка на киберсигурността

Одитът на киберсигурността е задълбочено проучване на системата за киберсигурност и ИТ инфраструктурата на организацията. Оценката сравнява практиките за сигурност на компанията с индустриалните стандарти или съответните разпоредби. Оценката на киберсигурността се различава от одита за киберсигурност по много начини. Оценката на уязвимостта е един аспект от одита за сигурност. Въпреки че одитите са всеобхватни и обхващат всички елементи на системата за сигурност, оценките често се извършват поотделно или само за една конкретна област. Одитите също така провеждат тестове и сравняват мерките за сигурност с други стандарти за съответствие.

Аспект	Одит на киберсигурността	Оценка на киберсигурността
Опреде-ление	Официален преглед от трета страна за валидиране на наличието и функционалността на контролите за сигурност.	Цялостна оценка на ефективността на сигурността, идентифициране на рискове и уязвимости.
Цел	Оценява ефективността на контролите за сигурност и идентифицира уязвимости, слабости и пропуски.	Оценява цялостното състояние на сигурността и идентифицира потенциални рискове и заплахи за сигурността.
Фокус	Осигурява съответствие със стандартите и политиките за киберсигурност.	Измерва ефективността на контрола и идентифицира пропуски в управлението на риска.
Честота	Обикновено се провежда периодично, например ежегодно или двугодишно.	Непрекъснато наблюдение в реално време.
Случаи на употреба	Валидиране на съответствие или осигуряване от доставчик.	Проактивно идентифицира заплахи, подкрепя отстраняването им и непрекъснатото подобрение.
Ползи	Изграждането на доверие между клиентите и партньорите осигурява гаранция за съответствие.	Проактивно идентифицира заплахи, подкрепя отстраняването им и непрекъснатото подобрение.
Недоста-тъци	Липса на тестване на ефективността на контрола, само моментна снимка във времето.	Изисква интеграция в по-широка стратегия за управление на риска.

Съществуват два основни вида одити на киберсигурността: вътрешни и външни. Вътрешните одити на киберсигурността могат да се провеждат от ИТ екипа на вашата организация; те имат предимството да използват задълбочени познания за вътрешните системи и процеси. Външни одити на ИТ сигурността се извършват от одитори от трети страни, които предоставят обективна перспектива чрез специализирана експертиза. Комбинацията от двата подхода често води до цялостна оценка.

Как да се възползваме от резултатите от одита на киберсигурността?

Констатациите от одита предоставят ценна информация за силните и слабите страни на вашата организация в областта на сигурността. Ето някои действия, които можем да предприемем, за да се възползваме от констатациите и да засилим защитата на организацията срещу киберзаплахи:

(1) **Приоритизиране и планиране на действията** – Категоризиране на констатациите, като използваме матрица на риска или система за оценяване. Това помага при съсредоточаване на усилията първо върху области с висок риск и критични уязвимости. След това, за всеки идентифициран проблем се разработва подробен план за действие, който адресира коренните причини и включва препоръчителното решение, възложените отговорности и график за изпълнение. Задаване на конкретни, измерими цели за всеки план за действие. Определят се етапи за проследяване на напредъка и спазване на графика за изпълнение.

(2) **Изпълнение и мониторинг** – следваме плана за действие старателно, като се уверим, че всяка стъпка се изпълнява по

план. Използвайте на автоматизирани инструменти за наблюдение в реално време, редовно преглеждайте регистрационните файлове за сигурност, извършвайте оценки на уязвимостите и коригирайте контролите въз основа на текущата ситуация със заплахите.

(3) **Оценка и непрекъснато усъвършенстване** – определеяне на ключови показатели за ефективност и показатели за оценка на въздействието на внедрените контроли и измерване на успеха. Документирайте подробно процеса на внедряване, резултатите и всички отклонения от плана. Докладвайте резултатите на заинтересованите страни, като подчертаете успехите и областите за по-нататъшно подобрение.

Въз основа на резултатите и обратната връзка, непрекъснато актуализирайте политиките, стандартите и процедурите си за киберсигурност. Това поддържа защитните механизми актуални, за да се предпазват от променящи се киберзаплахи и да са в съответствие с най-добрите практики и регулаторните изисквания.

Вместо заключение: Търсите оценка или одит на риска за киберсигурността – ЕЦИХ Тракия ще съдейства за реализирането на независими оценки, одити и услуги за подпомагане на бизнеса при внедряването на правилните решения за киберсигурност. Предоставяме цялостни и безпристрастни оценки на организации, които се нуждаят от задълбочен преглед на своите операции за цифрова сигурност, било то като част от вътрешен одит или преди да направят рискова инвестиция. Всичко това помага да се гарантира, че вашата организация е в съответствие с глобалните стандарти и разпоредби, намалявайки шансовете за кибератака.

Пълното описание на техническите и консултантски услуги в сферата на киберсигурността и дигитализацията, предостявяни от ЕЦИХ-Тракия може да намерите ТУК.

Европейски цифрови иновационни дни на Международния Пловдивски технически панаир

Европейският цифров иновационен хъб “Тракия” участва в рамките на Международния технически панаир в Пловдив, в периода 25-26 септември 2025, където бяха организирани консултантските събития “Европейски цифрови иновационни дни на Пловдивския технически панаир”. По време на двудневните събития бяха поканени гост лектори, за да разкажат важността на киберсигурността пред посетителите на международния панаир.

По време на консултантските събития се организира и “Майна Хак” – състезание по киберсигурност тип “Capture the flag”, с подкрепата на Майна Таун и Station Street fest. Състезанието започна от 24 септември и продължи до 26 септември 2025 г.

25 октомври, започна със секционен блок за консултации за финансиране, в който участваха доц. д-р Боян Жеков, Национален координатор за Хоризонт Европа и Александър Стоичков, основател на Balkan Fair Online. Темите, за които разказва бяха респективно “Приемна на Хоризонт Европа” и “Подкрепа за устойчив бизнес за социални предприятия”. В следващата сесия участваха представители от бизнеса и други организации. Иван Пепелов, изпълнителен директор на IDVKM, представилекция на тема “Постигане на

съвместимост с МИС2 чрез Identity Management", която акцентира на важните въпроси относно европейската директива за индустриалните предприятия и важността ѝ за оцеляването в новата бизнес среда. Паулина Чотрова представи Клъстер за изкуствен интелект, неправителствена организация, която иска да създаде устойчива екосистема около технологиите от изкуствен интелект. Представител на Виваком, Иван Парпулов, представи облачните услуги на компанията и възможностите им. Като за финал от в тази сесия, Десислава Терзиева от ЗК "Лев Инс" представи продуктите на компанията за киберсигурност и ползите от кибер застраховката.

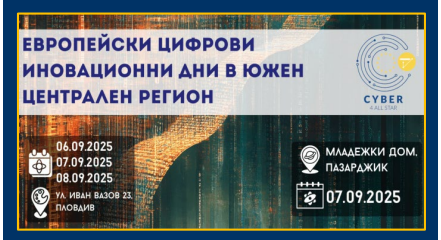
В последната сесия за деня започна с публична лекция на Ясен Танев от ЕЦИХ "Тракия", която тема бе "Кибер рискове и защити при управление на „умен" сграден фонд". По време на лекцията бяха разгледани важността на киберсигурността за умни сгради и как могат да се защитят. Пред щанда на ЕЦИХ "Тракия" бе представена и Индустриалната киберсигурност, която Сименс България предлагат на своите клиенти. Като последна тема за деня бе на Пейо Старибратов – обучител в ЕЦИХ "Тракия", който обясни за изкуствения интелект и киберсигурността как могат да работят заедно, за да предпазват и развиват предприятията.

На 26 септември, Красимир Лойков – Ръководител проект „Европа Директно – Пловдив", представи партньорската мрежа, свързваща Европа и България. Като естествено продължение и част от тази мрежа, Румяна Атанасова представи проектите "CyberSec4OT". Освен този проект, Диляна Герджикова от Търговско-Промишлена Камара - Пловдив представи възможностите на Enterprise Europe Network, които предлагат на малки и средни предприятия. Александър Ненков, търговски директор в AKAT Technologies предложи консултации за съответствие със законовите изисквания за киберсигурност. Сашка Бончева, координатор на Women4Cyber, представи инициативата пред млади дами за възможностите и мисията на фондацията.

В организираната хибридна сесия присъстваха Ива Ташева и Красимир Симонски, които представиха проект CONFIRMATE, целящ да създаде пакет от инструменти с отворен код за подпомагане постигането на съответствие на компаниите по отношение акта за киберсигурност на Европейския съюз.

В последната част на събитията, Станислав Атанасов обяви победителят на състезанието по киберсигурност "Майна Хак". Голямата награда за печелившият е конструктор с над 1700 части Lego Peugeot 9X8 24H Le Mans хибриден автомобил!

Европейски цифрови иновационни дни в Южен централен регион – Пазарджик и Пловдив



Европейски цифрови иновационни дни в Южен централен регион: Пловдив & Пазарджик се проведоха от 6 до 8 септември 2025 в двата града в партньорство с Уличен фестивал Пловдив и Булгакон 2025 както следва:

- 06.09.2025 г. 14:30-16:00 ч. в гр. Пловдив, Национално училище за музикално и танцово изкуство /НУМТИ/ „Добрин Петков",Ул. "Иван Вазов" 23, гр. Пловдив
- 07.09.2025 г. 9:30-20:00 ч. в гр. Пазарджик, Младежки дом, Ул. "Екзарх Йосиф" 6, и от 14:30-16:00 ч. в гр. Пловдив, Национално

училище за музикално и танцово изкуство /НУМТИ/ „Добрин Петков“,Ул. “Иван Вазов” 23, гр. Пловдив

- 08.09.2025 г. 14:30-16:00 ч. в гр. Пловдив, Национално училище за музикално и танцово изкуство /НУМТИ/ „Добрин Петков“ ,Ул. “Иван Вазов” 23, гр. Пловдив

Събитията бяха от Тип 4: Демонстрационни дни – Grant and Investment Advice workshops (услуга № 25 по каталога на ЕЦИХ Тракия); Demonstration Days (услуга № 28 по каталога на ЕЦИХ Тракия 8); Тип 5: Кръгли маси – Financial Engineering (услуга № 24 по каталога на ЕЦИХ Тракия); Cybersecurity B2B and B2C (услуга № 27 по каталога на ЕЦИХ Тракия) иТип 6: Публични лекции – Investor Days (услуга № 23 по каталога на ЕЦИХ Тракия); Digitalization Networking Conferences (услуга № 26 по каталога на ЕЦИХ Тракия). На събитията присъстваха общо 77 участници.

Форматът позволи в един и същи ден на сме представени в Пазарджик, където партнирахме с Българкон 2025 и в Пловдив с партньор Уличен фестивал Пловдив.

Междинен преглед на проекта от координаторите на европейските центрове за дигитални иновации

На 13 юни 2025 в бл. 2 на ИИКТ-БАН се проведе междинен преглед на проекта Cyber4AllSTAR с участието на координаторите на европейските центрове за дигитални иновации и участници по проекта. Събитието бе организирано в три основни сесии. В първата, д-р Христиан Даскалов – ръководител на проекта Cyber4AllSTAR и председател DIH Тракия направи общ преглед на напредъка на проекта, като представи също така извлечени поуки и стратегия за корекции.

Представена бе информация относно степента, до която е изпълнен работният план и изпълнението на ключовите показатели за ефективност. Представен беше приноса на членовете на консорциума и тяхното интегриране в проекта и работа на трети страни, участващи в проекта.

Фокусът на втората част от семинара включваше задълбочен анализ на ниво работен пакет – задачи, резултати, постижения и отклонения. Всеки ръководител на пакет прдстави постигнатите до момента резултати, изразени също така и в индикатори за изпълнение на проекта. Третата сесия бе определена за въпроси от предсатвителите на ЕК и отговори от участниците в проекта.

Връзки към събития по киберсигурност и информационна устойчивост

- International Conference on Cybersecurity Studies, 13 October 2025, Athens, Greece
- FUTURE RESILIENCE, 22-23 October 2025, The Dolder Grand, Zurich, Switzerland
- International Conference on Human Security Studies, 27th - 28th October 2025, Venice, Italy
- Benelux Cyber Summit, 4-5 November 2025, Novotel Amsterdam City, Amsterdam
- International Conference on Machine Learning and Cybernetics, 4-5 November 2025, Amsterdam, Netherlands
- Sofia Information Integrity Forum, 5-7 November, 2025, Sofia, Bulgaria

Редакционен съвет

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 ENTERPRI

ИИКТ
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

BCA
BULGARIAN CYBERSECURITY ASSOCIATION
Българска асоциация по киберсигурност

ОБЩИНА ПЛОВДИВ