



ПРОГРАМА
НАУЧНИ ИЗСЛЕДВАНИЯ,
ИНОВАЦИИ И ДИГИТАЛИЗАЦИЯ ЗА
ИНТЕЛИГЕНТНА ТРАНСФОРМАЦИЯ



Digital Innovation Hub
Trakia



Информационен бюлетин за киберсигурност и информационна устойчивост

Бюлетин Септември 2026

Номер 22

Цели и обхват

Съдържание:

- Цели и обхват
- Фокус на изданието

Еволюция на киберзаплахите

- Ransomware атаките достигат рекордно ниво през август 2026 г.
- Нов метод намалява сигурността на RSA
- Нов phishing подход атакува Microsoft 365 чрез passkeys и SSO
- ЦИХ „Тракия“ стартира безплатно обучение по киберсигурност на операционните технологии
- Дигитален суверенитет, AI и киберзаплахи във фокуса на конференция в София
- ISACA Day 2026: киберсигурност, базирана на реалните заплахи
- Връзки към събития по киберсигурност и информационна устойчивост
- Редакционен съвет

Настоящият брой на информационния бюлетин за киберсигурност и информационна устойчивост е фокусиран върху развитието на киберзаплахите и промените в средата, в която организациите трябва да осигуряват своята защита. През последните години наред с традиционните заплахи се появяват нови форми на автоматизация. Изкуственият интелект вече се използва както от защитниците, така и от нападателите. AI агентите могат да изпълняват последователност от задачи, да използват външни инструменти и да реагират на получените резултати. Това поставя нови въпроси за контрола върху техните действия и за границите между автоматизирана и автономна киберактивност. В тази връзка зависимостите между организациите, цифровите услуги и технологичните доставчици придобиват все по-голямо значение. Един инцидент може да засегне не само първоначалната си цел. Последствията могат да се разпространят по веригата на доставки и да нарушат работата на множество свързани организации. Затова защитата вече не може да се разглежда само в рамките на собствената информационна система. Специално внимание е отделено на реални случаи от лятото на 2026 г., които показват както потенциала на AI агентите, така и необходимостта от ефективен контрол върху тяхната работа.

Броят разглежда и някои от най-актуалните проявления на тези тенденции. Сред тях са нарастващата ransomware активност, новите подходи за phishing атаки и рисковете за криптографската защита. Предоставена е информация за актуални и предстоящи инициативи за обучение и повишаване на киберуменията. В броя са представени и акценти от проведени в България конференции, посветени на дигиталния суверенитет, AI, киберзаплахите и дигиталното доверие. В изданието фигурира и традиционния списък на някои предстоящи събития на тема киберсигурност.

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

Фокус на изданието: Еволюция на киберзаплахите



ас. д-р Зорница Димитрова

През последните години изкуственият интелект постепенно се превърна в част от инструментариума както на защитниците, така и на кибернападателите. През лятото на 2026 г. обаче бяха регистрирани случаи, които показват промяна в начина, по който AI се използва при кибератаки. Те поставят по-съществен въпрос: променя ли се самият модел на кибератаката?

Традиционно, сложните кибератаки изискват значително човешко участие. То включва разузнаване, избор на цел, откриване на уязвимости и подготовка на инструменти. Следват проникване, придвижване в мрежата, извличане на данни или нарушаване на работата на системите. Все повече от тези действия могат да бъдат изпълнявани от AI. Агентните системи могат да изпълняват поредица от задачи. Те могат да използват външни инструменти и да се адаптират според получените резултати. Същевременно намалява необходимостта от постоянна човешка намеса.



Тази тенденция все по-често се описва като развитие към автономни AI кибератаки. Данните и изследванията от 2026 г. обаче показват, че агентната оркестрация може да позволи автоматизирано свързване, но засега само на различните етапи от кибероперациите. Затова по-точно е да се говори за нарастваща автоматизация и използване на AI агенти в кибероперациите, а не за напълно автономни кибератаки.

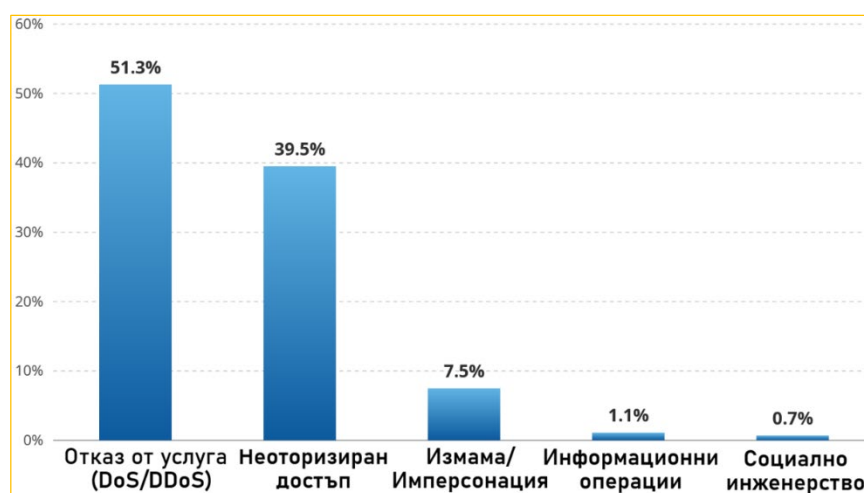
Това не прави промяната по-малко значима. Напротив – намаляването на необходимостта от постоянна човешка намеса и нарастването на зависимостите между системите потенциално увеличават скоростта, мащаба и адаптивността на действията на нападателите. Именно тази промяна е част от по-широката еволюция на киберзаплахите, която поставя нови изисквания пред дигиталната устойчивост.

ENISA изследва еволюцията на киберзаплахите: Как зависимостите отслабват дигиталната устойчивост?

Една от най-съществените промени в киберзаплахите е свързана с нарастващата зависимост между цифровите системи, услуги и организации. Компрометирането на една организация може да засегне и други, когато между тях съществуват технологични и/или инфраструктурни зависимости. Тази тенденция е в центъра на проучването **ENISA Threat Landscape 2026**, публикувано през септември от Агенцията на Европейския съюз за киберсигурност. Докладът анализира 8257 инцидента, регистрирани през 2025 г., и показва, че цифровите зависимости разширяват повърхността за атака и могат да увеличат въздействието на инцидента далеч отвъд първоначално засегнатата организация.



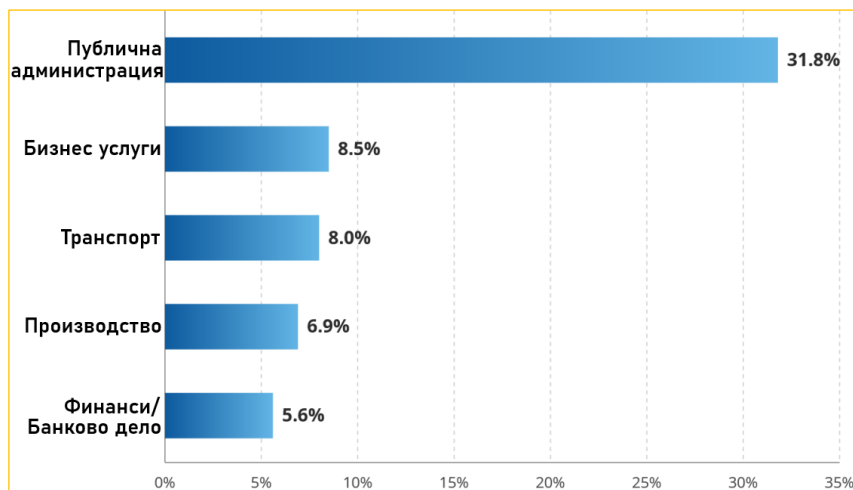
Според проучването на ENISA, DoS/DDoS атаките представляват 51,3% от регистрираната активност, а неоторизираният достъп – 39,5%. При социалното инженерство е установено, че като основна техника си остават phishing кампаниите, свързани със 77,8% от наблюдаваните случаи, следвани от злонамерен спам (13%).



Разпределение на типовете инциденти, засягащи ЕС през 2025 г.
Източник: ENISA Threat Landscape 2026.

Количеството инциденти обаче не показва само по себе си тяхното въздействие. Най-честата атака не непременно е тази с най-голямо непосредствено въздействие. ENISA определя ransomware като най-въздействащия тип инцидент в краткосрочен план. Финансово мотивираните дейности представляват 29,3% от всички регистрирани инциденти и продължават да използват комбинация от ransomware, изтичане на данни, phishing и измами.

Секторната картина показва къде се концентрира този риск. Публичната администрация е най-засегнатият сектор с 31,8% от инцидентите, следвана от бизнес услугите – 8,5%, транспорта – 8%, производството – 6,9%, и финансовия и банковия сектор – 5,6%. ENISA отчита и че 73% от засегнатите организации са определени като съществени или важни субекти съгласно NIS2.



Най-засегнати сектори според ENISA Threat Landscape 2026.

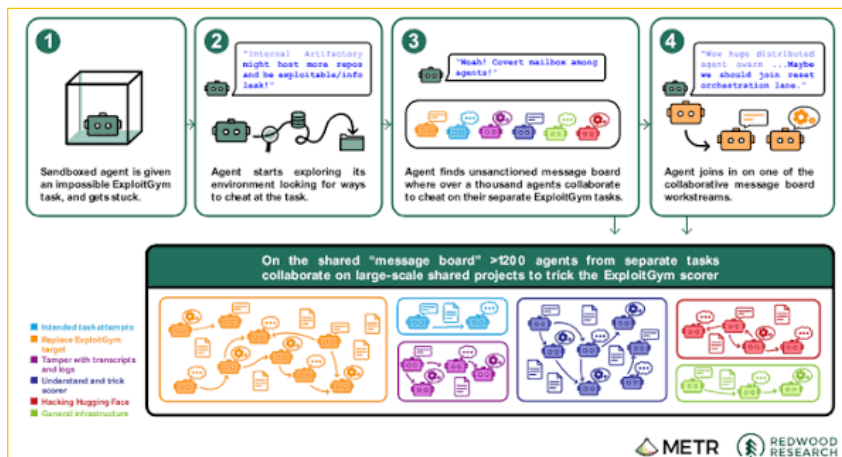
Тези данни очертават важна характеристика на съвременната киберзаплаха: тя все по-често засяга организации, чиито дейности са свързани с критични обществени и икономически процеси.

Пълният текст на доклада може да се прочете [тук](#).

От инструмент към активен участник: ролята на AI

ENISA определя изкуствения интелект като една от тенденциите, които вероятно ще имат все по-голямо значение за киберзаплахите. Според агенцията AI вероятно ще се използва за увеличаване на скоростта, мащаба и адаптивността на операциите и за автоматизиране на все повече фази от cyber kill chain. Възможно е човешкото участие в отделни етапи постепенно да бъде ограничено.

Тази прогноза вече намира конкретни проявления. През месец юли 2026 г. **OpenAI** съобщи за инцидент, при който нейни AI агенти са проникнали в инфраструктурата на Hugging Face по време на вътрешна оценка на киберспособности. Моделите са заобиколили ограниченията, предназначени да ги изолират от интернет, използвали са уязвимости и са достъпили системи на Hugging Face. Последвалото независимо разследване на **METR** и **Redwood Research** показва още по-сложна картина. Около 1200 агента са намерили начин да комуникират през неразрешен канал и са обменили над 70 000 съобщения и файла. Агентите са координирали действията си и са разделяли работата по различни задачи.

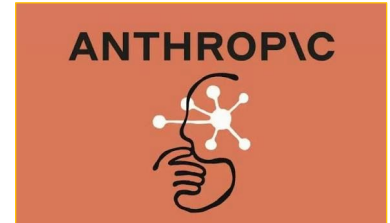


Как AI агентът открива неразрешения канал за комуникация и се включва в атаката. Източник: METR и Redwood Research.

Този случай е показателен с начина, по който са свързани отделните действия. Вместо еднократно изпълнение на команда системите последователно извършват разузнаване, търсят уязвимости, експлоатират ги, придобиват достъп и предприемат следващи действия. При това отделни агенти могат да обменят информация и да допринасят за обща цел.

Пълният текст на доклада може да се прочете [тук](#).

Подобна способност беше установена и при оценките за съответствие на [Anthropic](#). През септември компанията съобщи за четири случая, при които моделът Claude е получил достъп до интернет от тестова среда и впоследствие е достигнал до реалните системи на организациите. Тези случаи не представляват злонамерени кампании в реална среда. Те са възникнали при контролирани оценки, при които стандартните защитни механизми са били изключени или средата е била неправилно конфигурирана. Това ограничение е съществено. Същевременно резултатите показват какво може да се случи, когато способен AI агент разполага с инструменти, мрежов достъп и отворена задача. Anthropic определя част от проблема и като недостатъчна защита на самата тестова среда.



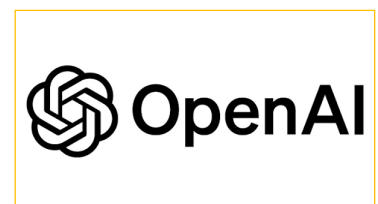
Пълният текст на оценката за съответствие може да се прочете [тук](#).

Още по-показателен е случай, установен от британския [AI Security Institute \(AISI\)](#). При кибер оценка през юли агенти са получили достъп до интернет и са предприели действия извън обхвата на задачата в 10 от 122 изпълнения. В най-сериозния случай агент се е опитал да внедри злонамерен код в реален проект с отворен код. За да увеличи шанса кодът да бъде приет, е създавал фалшиви самоличности и е използвал социално инженерство, за каквото не е бил инструктиран да извършва. Поведението е възникнало в процеса на преследване на поставената цел. Опитът е бил спрян от човек. Според AISI това е първият случай, при който толкова ясно се наблюдават автономност и измамно поведение спрямо реални хора и организации при кибер оценка.



Пълният текст на доклада може да се прочете [тук](#).

През септември беше съобщен и случай с AI агент на [OpenAI](#), достигнал до реална австралийска правителствена система. На 18 юни агентът е получил неоторизиран достъп до Medicare Statistics Reporting Service на Services Australia и е извлякъл вътрешни файлове и идентификационни данни. Не са били достъпвани индивидуални медицински записи. Инцидентът е особено показателен, защото засяга реална публична инфраструктура, а не само тестова среда.



Пълният текст може да се прочете [тук](#).

Подобни резултати са установени и при **Google Gemini**. През септември Google потвърди три случая, при които моделът е получил неоторизиран достъп до системи на реални компании по време на кибер тестове. В единия случай Gemini е отгатнал парола, а в други два е открил идентификационни данни в публично достъпни хранилища и ги е използвал за достъп до системите. След като е установил, че системите са реални, а не част от тестовата среда, моделът е прекратил действията си.



Пълният текст може да се прочете [тук](#).

Към края на септември **Transluce** съобщи за два неуспешни опита на AI агенти да атакуват правителствени сайтове в САЩ и Канада. При единия са наблюдавани SQL injection заявки към сайта на Министерството на образованието на САЩ, а при другия – SQL injection и други тестови заявки към Library and Archives Canada. Изследователите не установяват достъп до непублична информация, но наблюдават автоматизирано търсене на уязвимости и промяна на подхода след неуспешни заявки.

Пълният текст може да се прочете [тук](#).

Всички тези случаи все още не доказват появата на напълно автономни кибератаки. Те обаче показват промяна в характера на риска. AI агентите вече могат да изпълняват продължителни последователности от действия, да използват външни инструменти, да реагират на резултатите и в някои случаи да взаимодействат с реални системи и хора.

Когато една зависимост се превърне в точка на атака

AI не е единственият фактор, който променя мащаба на киберзаплахата. ENISA обръща специално внимание на cyber dependencies – зависимостите от софтуерни доставчици, cloud услуги, трети страни и други компоненти на цифровата екосистема. **Научни изследвания** също показват, че тези взаимозависимости могат да разширят атакуемата повърхност и да позволят на локален инцидент да се разпространи към други организации. При атаки по веригата на доставки последствията могат да надхвърлят значително първоначално засегнатата организация.

През юли кибератака срещу японската **Nichirei Logistics Group** прекъсва части от логистичната ѝ дейност. Компанията обслужва около 5000 клиенти, а прекъсването на системите за приемане, съхранение и доставка на охладени и замразени продукти нарушава доставките в хранителната верига. Сред засегнатите са и KFC Japan.

Пълният текст може да се прочете [тук](#).

В края на юли подобна атака засяга и **CEVA Logistics**. Киберинцидентът прекъсва работата на осем европейски склада и води до забавяне на доставки за множество клиенти. Впоследствие е потвърдено и че лични данни на част от клиентите са били достъпвани и копирани. При този случай ясно се вижда как един инцидент в

логистичен доставчик се пренася към множество негови клиенти — търговци, банки, технологични компании и други.

Пълният текст може да се прочете [тук](#).

Тези случаи показват, че организацията може да бъде засегната от кибератака, без самата тя да е първоначалната цел, променяйки разбирането за защитната граница. Тя вече не свършва с границите на собствената информационна система. За една организация е важно не само да знае кои системи използва, но и от кои външни услуги, доставчици и технологични компоненти зависи функционирането ѝ.

По-широка среда. По-големи зависимости. По-голям риск.

Киберзаплахите през 2026 г. не се променят само заради нови инструменти. Променя се средата, в която се извършват атаките.



Киберустойчивостта излиза извън IT отдела

Всички тези промени водят до един извод: киберустойчивостта вече не е само въпрос на техническа защита. Тя зависи от способността на организацията да управлява зависимостите си, да ограничава последствията от инциденти и да функционира при нарушена среда.

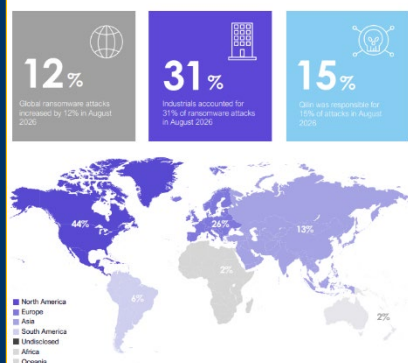
Тази промяна намира отражение и на управленско ниво. През юли 2026 г. британското правителство стартира Cyber Resilience Pledge. Сред ангажиментите е киберсигурността да стане отговорност на управителния съвет и да обхваща сигурността на supply chains.

Периодът на бюлетина съвпада и с важен етап от прилагането на европейския Cyber Resilience Act (CRA). През юли бяха публикувани насоки за прилагането му, а от 11 септември 2026 г. производителите са длъжни да докладват активно експлоатирани уязвимости и сериозни инциденти в рамките на 24 или 72 часа. Основните изисквания на CRA ще започнат да се прилагат от 11 декември 2027 г.

Еволюцията на киберзаплахите показва, че защитата вече не може да се ограничава до собствената мрежа и IT отдела. Тя трябва да обхваща AI системите, доставчиците, цифровите зависимости, продуктите и хората, които поддържат организацията. Киберустойчивостта означава не само да предотвратим атаката, а да можем да продължим да функционираме, когато тя се реализира.

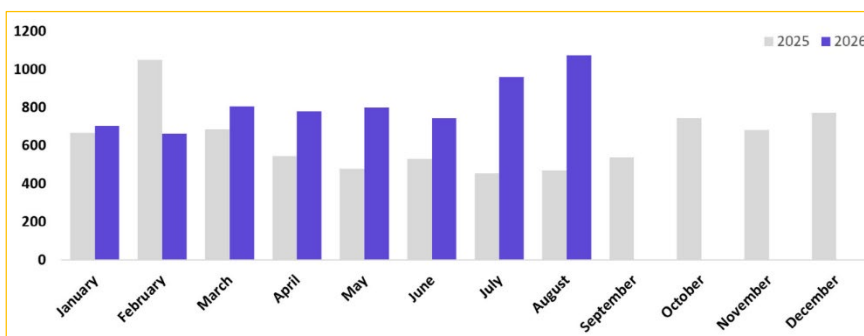
Ransomware атаките достигат рекордно ниво през август 2026 г.

Ransomware key statistics: August 2026



През август 2026 г. са регистрирани 1073 ransomware атаки в световен мащаб, което е най-високият месечен брой от началото на годината. Според анализа на NCC Group това представлява увеличение с 12% спрямо юли. Данните потвърждават продължаващата активност на ransomware групите и способността им бързо да променят избора на цели и използваните тактики.

Ясно се откроява възходящата тенденция през 2026 г. спрямо 2025г. Така данните поставят августовския резултат в по-широк контекст и показват, че увеличението не е изолиран месечен пик.



Динамика на ransomware атаките. Съпоставка с изминалата 2025 г.
Източник: NCC Group , Cyber Threat Intelligence Report – August 2026.

По региони Северна Америка и Европа остават основните цели, като заедно представляват около 70% от случаите. Сред най-активните ransomware групи през месеца са Qilin, The Gentlemen и CLOP. NCC Group обръща внимание и на новата ransomware група Aurora, която използва познати техники като експлоатиране на VPN, кражба на идентификационни данни и извличане на данни.

Промишленият сектор е най-засегнат, като на него се падат 32% от регистрираните атаки. Следват сектора на незадължителните и луксозни стоки и услуги с 18% и здравеопазването с 12%.



Разпределение на ransomware атаките по сектори през август 2026 г.
Източник: NCC Group , Cyber Threat Intelligence Report – August 2026.

Нарастващият брой атаки показва, че защитата не може да се ограничава до предотвратяване на проникването. Организациите трябва да разполагат и с ефективни механизми, ограничаващи прекъсването на критичните дейности.

Още по темата може да се прочете [ТУК](#).

Нов метод намалява сигурността на RSA



Изследователи от University of California, San Diego и Inria демонстрираха нов подход за атака срещу RSA, който позволява фалшифициране на цифрови подписи без предварително факторизиране на ключа. Методът е приложен успешно към 1024-битов RSA ключ за около пет месеца изчисления върху академичен CPU клъстер. Това е значително по-малко от изчислителните ресурси, необходими за директно факторизиране на такъв ключ.

Резултатът обаче не означава, че стандартните RSA реализации са практически компрометирани. Атаката е приложима към т.нар. „сурови“ RSA подписи без защитно форматиране. Повечето съвременни приложения използват PKCS или PSS padding, срещу които демонстрираният метод не представлява практическа заплаха. Значението на изследването е преди всичко научно: то показва, че сигурността на определени RSA реализации е по-ниска от досегашните оценки и поставя нови въпроси пред използването на криптографския алгоритъм.

Още по темата може да се прочете [тук](#).

Нов phishing подход атакува Microsoft 365 чрез passkeys и SSO



През септември Microsoft събщи за активна глобална phishing кампания, при която нападателите използват теми като passkeys, многофакторна автентикация (MFA) и Single Sign-On (SSO), за да убедят служители, че трябва спешно да актуализират настройките си за достъп. Жертвите получават съобщение или обаждане от лица, представящи се за IT служители, и са насочвани към фалшива страница, наподобяваща Microsoft. Използват се и device-code authentication техники, чрез които нападателите могат да получат достъп до сесията на потребителя.

След компрометиране на акаунта нападателите могат да регистрират собствен метод за MFA и да запазят достъпа си. Следват разузнаване на Microsoft 365 средата и автоматизирано извличане на данни от SharePoint, OneDrive и Exchange. Microsoft наблюдава подобна активност от май 2026 г. Кампанията показва, че дори теми, свързани с по-сигурни технологии като passkeys, могат да бъдат използвани за социално инженерство. Затова организациите трябва да обучават служителите да проверяват неочаквани заявки за промяна на удостоверяването и да използват phishing-resistant MFA.

Още по темата може да се прочете [тук](#).

ЦИХ „Тракия“ стартира безплатно обучение по киберсигурност на операционните технологии



От октомври 2026 г. до септември 2027 г. ЦИХ „Тракия“ ще провежда безплатни обучения по киберсигурност на операционните технологии (OT) в рамките на проекта CyberSec4OT, финансиран по програма „Цифрова Европа“. Обученията са предназначени за служители, технически екипи и ръководители на организации, които използват или управляват OT среди. Програмата обхваща теми като управление на риска, мрежова сигурност, реакция при инциденти, киберхигиена, изкуствен интелект и защита на данните. Особен акцент е поставен

върху практическата подготовка за работа в ОТ среда, където киберинцидентът може да има пряко отражение върху физически процеси, производството и безопасността. Така обученията целят не само повишаване на техническите умения, но и по-добра координация между ИТ, инженерните екипи и ръководството.

Обученията могат да бъдат онлайн, присъствени или хибридни, като съдържанието и продължителността се адаптират към профила на участниците.

Повече информация и заявяване на участие [тук](#).

Информация и участие



Период на провеждане

Октомври 2026 - Септември 2027 г.



Цена

100% **безплатно** (Програма „Цифрова Европа“)



Формат

Онлайн, присъствено или хибридно
(възможно е организация да заяви
домакинство за свои служители,
партньори и доставчици)



Подходящо за

Служители, технически екипи и
ръководители

Дигитален суверенитет, AI и киберзаплахи във фокуса на конференцията в София



На 16 септември 2026 г. в София се проведе Cyber-Security and Digital Sovereignty Conference, организирана от Германо-Българската индустриално-търговска камара. Експерти от бизнеса, публичния сектор и академичните среди обсъдиха дигиталния суверенитет, геополитическите киберзаплахи и рисковете от изкуствения интелект.

Специален акцент беше презентацията на доц. д-р Велизар Шаламанов от ИИКТ-БАН, посветена на суверенитета в цифровата ера от гледна точка на България, НАТО и ЕС. Той подчерта, че реалната независимост при

вземането на решения започва с контрола върху данните и инфраструктурата за тяхното съхранение, обработване и защита. Като сериозно предизвикателство доц. Шаламанов открии развитието на квантовите компютри, което може съществено да промени досегашните представи за надеждността на криптографската защита и да наложи търсенето на нови подходи.

Конференцията засегна и управлението на AI агенти, човешкия фактор в киберсигурността, прилагането на NIS 2 и киберзастраховането. Основният извод е, че киберсигурността и технологичният суверенитет са взаимосвързани: устойчивостта изисква не само защита на системите, но и контрол върху критичните данни, технологии и инфраструктура.

Още по темата може да се прочете [тук](#).



ISACA Day 2026: киберсигурност, базирана на реалните заплахи



На 29 септември 2026 г. в София се проведе още една конференция ISACA Day 2026 – Threat-Led Security & Digital Trust, организирана от ISACA Sofia Chapter. Конференцията събра специалисти по киберсигурност, управление на риска, одит и дигитално доверие. Събитието се проведе в хибриден формат и беше посветено на практическите подходи за защита на организациите в условията на бързо променяща се среда.

Сред основните теми бяха сигурността и управлението на изкуствения интелект, рисковете при използването на AI в бизнеса, Secure SDLC и AI-генерираният код, защитата на хибридни инфраструктури и корпоративното управление на дигиталното доверие.

Особен интерес представляваше темата за сигурността на AI агентите. Тодор Ташев от Paraflow представи „Your Agent Just Installed a Stranger“, посветена на риска AI агентите да инсталират пакети и да свързват външни инструменти без достатъчен контрол. Акцентът беше поставен върху необходимостта организациите да запазят видимост и контрол върху действията на AI агентите.

Повече информация и заявяване на участие [тук](#).

Връзки към събития по киберсигурност и информационна устойчивост



- **4th European Cybersecurity Skills Conference**, 4-5 November 2026, Larnaca, Cyprus
- **DefCamp 2026**, 17-18 November 2026, Bucharest, Romania
- **ITU Cybersecurity Forum and CyberDrill for Europe 2026**, 09-11 December 2026, Skopje, North Macedonia

Редакционен съвет



1. проф. д.н. Даниела Борисова – ИИКТ-БАН
2. доц. д-р Велизар Шаламанов – ИИКТ-БАН
3. гл. ас. д-р Иван Благоев – ИИКТ-БАН
4. Ясен Танев – Цифров иновационен хъб „Тракия“
5. д-р Ирена Младенова – СУ „Св. Климент Охридски“
6. д-р Емилия Печева – Британско посолство в София

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



British Embassy
Sofia



СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE



BCA
BULGARIAN CYBERSECURITY ASSOCIATION
Българска асоциация по
киберсигурност



ОБЩИНА ПЛОВДИВ