ISSN 2738-7089 https://doi.org/10.11610/cybsec21bg

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 Юни 2026 Номер 21

Цели и обхват

Настоящият брой на информационния бюлетин за киберсигурност и информационна устойчивост разглежда прехода от традиционното разбиране за киберсигурност към по-широката концепция за киберустойчивост. Водещ акцент в броя е обзорът на шестте най-нови публикации на ENISA (European Union Agency for Cybersecurity) от периода април – юни 2026 г. Чрез тях се проследява как европейският подход постепенно се измества от защита срещу кибератаки към изграждане на устойчива цифрова среда. Разгледани са теми като измерването на киберзрялостта, прозрачността на софтуерните компоненти и веригата на доставки, както и готовността на малките и средните предприятия (МСП) за прилагането на Cyber Resilience Act (CRA). Специално внимание е отделено на резултатите от проучванията сред МСП, внедряването на Software Bill of Materials (SBOM) и първите практически стъпки към изграждане на киберустойчивост.

Изданието анонсира и някои от най-важните събития, които предстоят през следващите месеци, свързани с киберсигурността, а именно започващото задължително докладване по Cyber Resilience Act чрез платформата ENISA-CRA-SRP и новия етап от прилагането на Закона на ЕС за изкуствения интелект (AI Act).

В съдържанието на настаящия бюлетин са показани реални примери за киберустойчивост чрез учения, доклади за заплахи, секторни инциденти и български инициативи. Сред тях са първият киберполигон в България, инициативата „Кибер гвардейци“ и представянето на български напредък в сигурността на DNS на европейски семинар в Брюксел. В изданието е представен и списък на някои предстоящи събития по темата киберсигурност.

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

Съдържание:

- Цели и обхват
- Фокус на изданието
- **От киберсигурност към киберустойчивост: как ENISA очертава европейския модел**
- От 11 септември 2026 г. започва задължително докладване по CRA чрез единната платформа ENISA-CRA-SRP
- Нов етап от прилагането на AI Act – 2 август 2026
- Киберустойчивост на практика: учения, заплахи и реални инциденти
- Първият киберполигон в България ще обучава студенти
- „Кибер гвардейци“: младежка инициатива за киберкултура и взаимопомощ
- ЦИХ „Тракия“ представи напредък в сигурността на DNS на европейски семинар в Брюксел
- Връзки към събития по киберсигурност и информационна устойчивост
- Редакционен съвет

Фокус на изданието: От киберсигурност към киберустойчивост: как ENISA очертава европейския модел

ас. д-р Зорница Димитрова

През последните години понятието „киберсигурност“ придобива по-широко значение и все по-често то не се свързва единствено със защитата от кибератаки. Това понятие обхваща също така и способността на организациите да управляват риска, да поддържат непрекъсваемостта на дейностите и възможността за бързо възстановяване след инциденти. Тази промяна ясно личи в публикациите на ENISA от периода април – юни 2026 г. Те показват, че европейският подход към киберсигурността поставя все по-силен акцент върху киберустойчивостта. Наред със защитата от заплахи, се включва измерване на киберзрялостта, сигурност на цифровите продукти, прозрачност по отношение на използваните софтуерни компоненти и практическа подкрепа за организациите.

В центъра на настоящия обзор са три практически ориентирани доклада на ENISA, свързващи европейските политики с реалната готовност на организациите, а именно ENISA NIS360, SME CRA Survey Report и SBOM Adoption State of Play. ENISA NIS360 анализира нивото на киберзрялост на секторите с висока критичност, определени в Директивата NIS2. SME CRA Survey Report насочва вниманието към малките и средните предприятия, като разглежда как те възприемат новите изисквания на Cyber Resilience Act, доколко са подготвени за тяхното прилагане и от каква подкрепа се нуждаят. SBOM Adoption State of Play допълва тази картина чрез темата за прозрачността на софтуерните компоненти и зависимостите.

Към тях се добавят и три по-методологични публикации: National Capabilities Assessment Framework 2.0, ENISA Technology and Innovation Radar Methodology и Technical Competence Requirements for CRA Notified Bodies. Те допълват общата картина, като показват как ENISA насърчава измерването на киберзрялостта, ранното наблюдение на технологичните промени и изграждането на компетентност за оценяване на цифрови продукти.

Така ENISA очертава по-широка посока на развитие: от киберсигурност, разбирана предимно като защита, към киберустойчивост, основана на измеримост, управление, прозрачност и практическа готовност.

В Лабораторията по информационна и кибер устойчивост в ИИКТ-БАН, работейки по проекти EDIH, CoDE, ННП сигурност и отбрана, бюджетни проекти на БАН в ИИКТ се търси интеграцията по вертикала и по хоризонтала на решенията за коберсигурност, разузнаване по открити източници и противодействие на дезинформацията, използването на ИИ при вземане на решения с цел създаване на цялостна рамка за устойчивост при цифровата трансформация за публичния сектор, а и МСП, които разчитат на подкрепа от държавата и модел на споделени услуги.

Бележка: *Фигурите и графиките в темата са преведени и адаптирани по данни и визуални материали от разглежданите документи на ENISA.*

Измерване на киберзрялост: първа стъпка към киберустойчивост

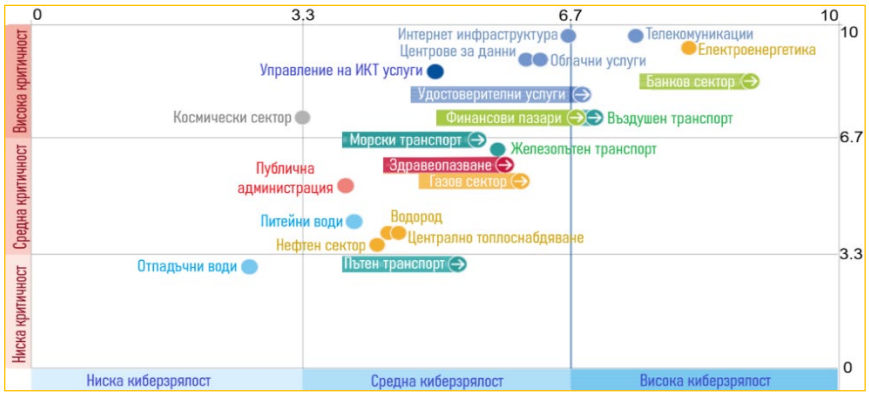
Когато киберустойчивостта се превръща в управленска цел, възниква важен въпрос: как тя може да бъде оценена с цел управление и подобрение? Публикациите на ENISA поставят силен акцент именно върху измерването. Организациите, секторите и държавите трябва не само да прилагат мерки за сигурност. Те трябва да знаят доколко тези мерки са последователни и резултатни.

Киберзрялостта не се изчерпва с наличието на стратегия или формално изпълнение на изисквания. Тя включва управление, ясно разпределение на отговорностите, ресурси, координация, измерване на напредъка и непрекъснато подобрение. В този смисъл киберсигурността се разглежда като дългосрочен процес, а не като еднократна техническа задача.

Тази логика стои и в основата на ENISA NIS360. Докладът съпоставя нивото на киберзрялост на секторите с тяхната критичност. Под „критичност“ се разбира значението на даден сектор за функционирането на обществото, икономиката и основните услуги. Така се вижда не само кои сектори са важни, но и доколко са подготвени да управляват киберрискове. Киберзрялостта се разглежда през няколко измерения. Сред тях са политическата и регулаторната рамка, управлението на киберриска, обменът на информация и оперативната готовност за реакция и възстановяване.

Съвсем отделно са въпросите за киберсигурност в сектор отбрана и сигурност, където изискванията са още по-високи, но и решенията могат да служат за пример в други сектори. Не на последно място – киберсигурността в сектора за сигурност е основа за развитие на киберсигурността във всички други сектори. Именно затова в Лабораторията по информационна и киберустойчивост на ИИКТ-БАН се търсят механизми за взаимно подпомагане на усилията за устойчивост в този и другите сектори.

ENISA отчита, че киберзрялостта на критичните сектори в ЕС постепенно се повишава. Напредъкът обаче не е равномерен. Банковият сектор, електроенергетиката и телекомуникациите остават сред най-зрелите и най-критичните сектори. Към групата на секторите с висока киберзрялост вече се присъединяват и доверителните услуги, авиацията и финансовите пазарни инфраструктури.



Напредък на секторите по отношение на киберзрялостта.

В същото време част от секторите остават в по-рискова позиция. Това са области, при които значимостта за обществото и икономиката е висока, но киберзрялостта остава под средното равнище. Сред тях са здравеопазването, железопътният и морският транспорт, ICT management services, космическият сектор, публичната администрация, питейните и отпадъчните води.

Съпоставка между киберзрялост и критичност на секторите.

Практическият извод е ясен: киберустойчивостта започва с оценка на текущото състояние за определяне на приоритети, за планиране на инвестиции и доказване на напредък. Това важи не само за държавите и критичните сектори, но и за всяка организация, която иска да повиши своята готовност за киберинциденти.

Новите технологии изискват ранно наблюдение

Освен от текущото състояние на организациите, тяхната киберустойчивост зависи и от способността им да разпознават навреме нови технологични промени. Част от тези промени създават възможности. Други могат да отворят нови повърхности за атака.

В тази посока докладът ENISA Technology and Innovation Radar Methodology поставя акцент върху ранното наблюдение на нововъзникващи технологии. В основата на този подход е понятието „сигнал“. В методологията на ENISA сигналът е наблюдаем признак за възникваща промяна — например нова технология, инструмент, платформа или тенденция, която може да повлияе на киберсигурността. Тези сигнали могат да бъдат слаби или силни. Слабите сигнали са ранни признаци за развитие, което все още не е широко разпространено. Силните сигнали вече имат повече доказателства за практическо приложение или пазарно навлизане. И в двата случая целта е една: по-добро предвиждане на бъдещите рискове и възможности с цел възпиране и ранно предупреждение, а при реализация на заплахата – решително справяне.

Методологични стъпки на Technology and Innovation Radar.

Практически извод: не е достатъчно реагирането само на известни заплахи, важни са и технологичните тенденции като изкуствен интелект, автоматизацията, облачните услуги, свързаните устройства и новите модели на цифрови услуги. Наблюдението е важна част от киберустойчивостта, защото позволява на организациите да се подготвят преди рисковете да се превърнат в реални инциденти.

Cyber Resilience Act: сигурност през целия жизнен цикъл

Една от важните посоки в европейската политика е сигурността на цифровите продукти, пряко обвързана с Cyber Resilience Act.

Регламентът поставя изисквания към продукти с цифрови елементи и насочва вниманието към сигурността през целия жизнен цикъл. Това означава, че сигурността не трябва да се разглежда само в момента на пускане на продукта на пазара. Тя трябва да бъде заложена още при разработването. След това трябва да се поддържа чрез управление на уязвимости, актуализации, документация, проследимост и реакция при инциденти.

За производителите на цифрови продукти това създава по-високи очаквания. Нужни са ясни процеси за сигурна разработка и управление на уязвимости. Необходима е и по-добра техническа документация. Организацията трябва да може да покаже, че продуктът е разработван и поддържан по сигурен начин.

Публикацията на ENISA Technical Competence Requirements for CRA Notified Bodies допълва тази картина. Тя показва, че прилагането на CRA изисква не само правила за производителите, но и компетентни оценители. Така фокусът се измества от отделния продукт към целия процес около него. Сигурността вече трябва не само да се заявява, а да може да бъде доказана.

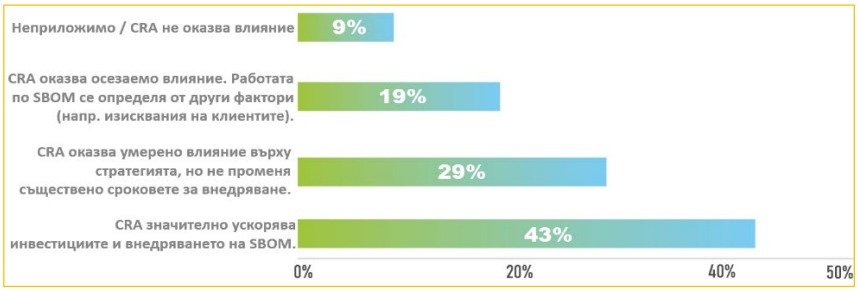
Практическият извод е, че: за организациите, разработващи софтуер, IoT устройства или други продукти с цифрови елементи, подготовката за CRA не е само юридически въпрос. Тя налага промени в процесите, документацията и организацията на работа. Сигурността трябва да може да бъде доказана чрез компетентна оценка, ясна документация и устойчиви процеси за поддръжка.

SBOM: прозрачност в софтуерната верига на доставки

Съвременният софтуер рядко се създава изцяло от нулата. Той обикновено включва множество библиотеки, външни компоненти, open-source зависимости, инструменти и услуги, което прави управлението на софтуерната верига на доставки все по-важна част от киберсигурността.

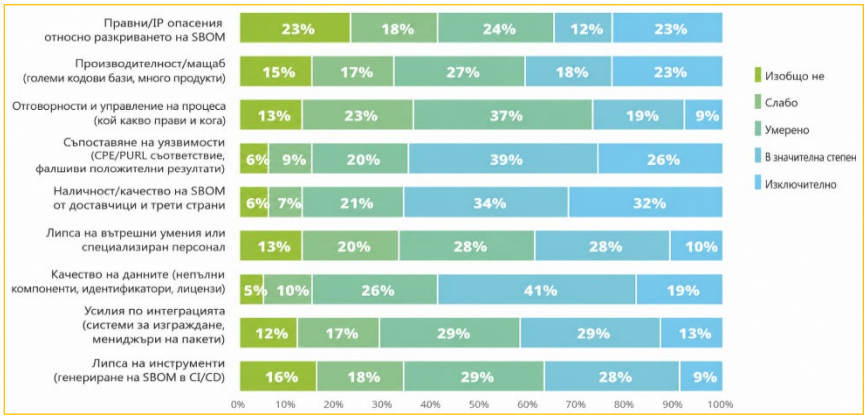
В доклада SBOM Adoption State of Play – 2026 ENISA разглежда състоянието на внедряване на Software Bill of Materials. Най-общо, SBOM представлява опис на софтуерните компоненти, които изграждат даден продукт. Той помага на организациите да знаят какво използват, откъде идват отделните компоненти и дали сред тях има уязвими или неподдържани елементи.

Практическата стойност на SBOM е особено ясна при новооткрити уязвимости. Ако в дадена библиотека се появи сериозна уязвимост, организацията трябва бързо да разбере дали я използва. Без такава видимост реакцията се забавя. Със SBOM проверката може да бъде по-бърза и по-точна. Темата е тясно свързана с Cyber Resilience Act и данните на ENISA показват, че CRA вече влияе върху инвестициите в SBOM инструменти и автоматизация. 43% от анкетираните организации посочват, че регламентът значително е ускорил тези инвестиции. Още 29% отчитат умерено влияние. Внедряването на SBOM вече е започнало при голяма част от организациите. 78% от анкетираните посочват, че са започнали своя път към използване на SBOM. Част от тях обаче са още в пилотна или ограничена фаза. 44% са именно на такъв етап. 25% съобщават, че SBOM вече се използва широко в техните продукти.



Влияние на CRA върху инвестициите в SBOM инструменти и автоматизация.

Само 9% посочват зряло внедряване, подкрепено от автоматизация. Това показва, че SBOM вече навлиза в практиката, но все още не е равномерно развит процес. Основните пречки не са само технически. Сред най-сериозните са липсата или ниското качество на SBOM информация от доставчици и трети страни, трудностите при съпоставяне на уязвимости с конкретни компоненти, както и проблемите с качеството на данните.



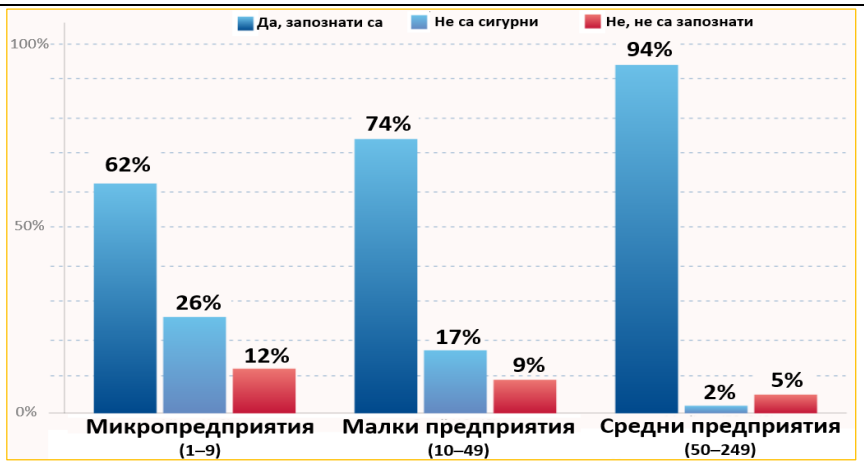
Основни пречки пред внедряването на SBOM.

Практическият извод е, че: SBOM не трябва да се възприема само като допълнителен документ за съответствие. Той е инструмент за по-добра видимост, по-бърза реакция при нови уязвимости и по-ефективно управление на риска в софтуерната верига на доставки.

МСП: между осведомеността и реалната готовност

МСП са в центъра на практическото прилагане на CRA. В тази връзка ENISA представя резултати от проучване сред 194 организации от 31 държави и географски групи в доклада SME CRA Survey Report. Целта е да се оцени доколко МСП познават CRA, как разбират изискванията и какви трудности очакват при подготовката за съответствие.

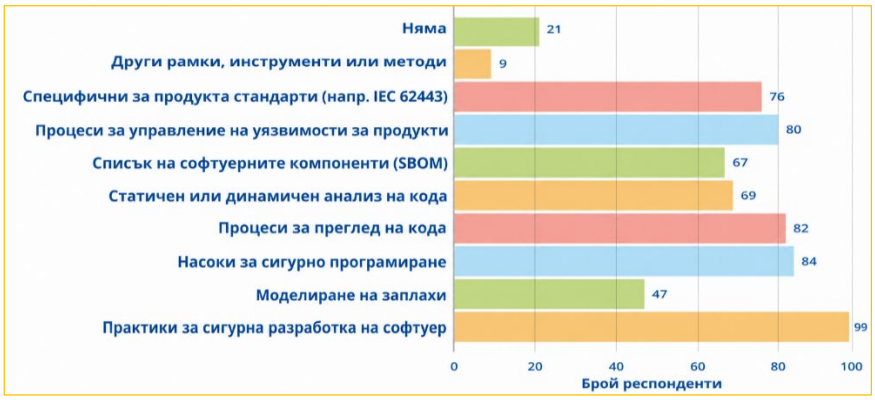
Докладът показва ясно разминаване между общата осведоменост и практическата готовност. Около 66% от анкетираните посочват, че са чували за CRA преди проучването. Но това не означава, че разбират конкретните задължения. Осведомеността зависи и от размера на предприятието. Средните предприятия са най-добре информирани (94%), следвани от малките предприятия (74%) и микропредприятията (62%). Най-слабо е разбирането на изискванията за техническа документация и процедурите за оценяване на съответствието. Само 13% от анкетираните съобщават за добро или много добро разбиране на изискванията за документация. За процедурите за оценяване на съответствието този дял е 14%, което е важен сигнал за бизнеса.



Предварителна осведоменост за CRA според размера на предприятието

За много МСП предизвикателството не е само да разберат, че CRA съществува. По-трудната задача е да превърнат изискванията в конкретни процеси, документи и технически практики. Важен остава и въпросът за обхвата на CRA. 70% от анкетираните смятат, че попадат в него, 20% не са сигурни, а 10% смятат, че не попадат. Несигурността е по-голяма при вносители, дистрибутори и доставчици, където отговорностите зависят от веригата на доставки.

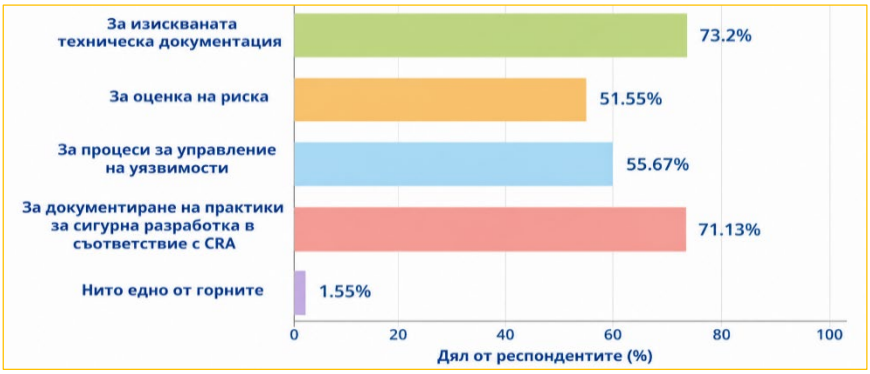
В същото време по-специализирани подходи като SBOM и threat modelling все още се използват по-ограничено. Според данните 99 от анкетираните посочват, че прилагат практики за сигурна разработка. 84 използват насоки за сигурно програмиране, а 82 използват процеси за преглед на кода. Управление на уязвимости прилагат 80 от анкетираните. В същото време SBOM се използва от 67, а threat modelling – от 47 анкетирани.



Прилагани технически практики и стандарти.

Размерът на предприятието се оказва съществен фактор. 93% от средните предприятия имат вътрешен служител, който отговаря за киберсигурността. При микропредприятията картината е различна – 57% от тях нямат определена отговорност за киберсигурността. Това обяснява защо едни и същи изисквания могат да имат различна тежест. За средно предприятие подготовката може да бъде въпрос на подобряване на вече съществуващи процеси. За микропредприятие тя често започва от нулата.

Проучването показва и каква подкрепа очакват МСП. Най-често се търсят практически шаблони, контролни списъци, насоки стъпка по стъпка, обучения и финансово подпомагане. Над 73% от анкетираните искат шаблони за техническа документация. 71% посочват нужда от шаблони за документиране на практики за сигурна разработка. Близо 56% търсят шаблони за процеси за управление на уязвимости.



Най-търсени шаблони и контролни списъци за подпомагане на съответствието с CRA.

Практическият извод е, че: подготовката за CRA трябва да бъде поетапна. За МСП тя не може да се сведе до еднократно юридическо или техническо действие. Необходими са разбираеми указания, достъпни инструменти, обучение и реалистичен план за въвеждане на процеси, съобразени с размера и ресурсите на организацията.

Какво могат да направят организациите още сега?

Публикациите на ENISA показват, че киберустойчивостта не се изгражда с еднократно действие. Тя изисква последователен подход, добра организация и постепенно подобрение. Това е особено важно за МСП, които често разполагат с ограничени ресурси и малки екипи. Основните практически стъпки, които организациите могат да предприемат са:

- ✅ Оценяване на текущото ниво на киберзрялост;
- ✅ Описание на основните цифрови активи и зависимости;
- ✅ Проверка дали притежаванията попадат в обхвата на CRA;
- ✅ Поетапно ориентиране към изискванията на CRA;
- ✅ Поетапно въвеждане на SBOM;
- ✅ Идентифициране и оценка на рисковете;
- ✅ Въвеждане на процеси за управление на уязвимости;
- ✅ Използване на шаблони за сигурна разработка;
- ✅ Редовно актуализиране на софтуера;
- ✅ Актуализиране на техническата документация;
- ✅ Определяне на отговорности при киберинцидент;
- ✅ Обучение на ключови служители;
- ✅ Следване на насоките на ENISA, NIS2 и CRA.

Така преходът към киберустойчивост може да започне с реалистични и изпълними действия. Най-важното е организацията да не чака инцидент или регулаторен натиск, за да започне подготовка.

От 11 септември 2026 г. започва задължителното докладване по CRA чрез единната платформа ENISA-CRA-SRP

От 11 септември 2026 г. започват да се прилагат изискванията за докладване по Cyber Resilience Act. Производителите ще трябва да уведомяват за активно използвани уязвимости и за сериозни инциденти, които засягат сигурността на продукти с цифрови елементи. Докладването ще се извършва чрез CRA Single Reporting Platform (SRP) – единна електронна платформа, създадена и поддържана от ENISA.

Основната цел на SRP е да опрости процеса. Производителят ще подава уведомлението само веднъж, вместо да информира отделно различни национални органи. Платформата ще насочва информацията към съответния CSIRT координатор и към ENISA. След това CSIRT ще я разпространява към други релевантни CSIRT екипи и, при необходимост, към органите за надзор на пазара. Платформата трябва да включва мерки за сигурност и защита на поверителността на подадената информация, защото уведомленията могат да съдържат чувствителни технически данни за уязвимости, продукти, клиенти и предприети коригиращи действия. Сроковете са кратки. При установяване на активно използвана уязвимост или сериозен инцидент се подава ранно предупреждение до 24 часа. До 72 часа се подава по-пълно уведомление. Окончателният доклад се подава до 14 дни след налична коригираща мярка при уязвимост или до 1 месец при сериозен инцидент.

За организациите това означава, че подготовката трябва да започне преди датата на прилагане. Необходимо е да има ясно разпределени отговорности, процес за откриване и оценка на уязвимости, готовност за бързо събиране на информация и процедура за реакция при инциденти. Това е особено важно за МСП, които разработват или доставят софтуер, IoT устройства, индустриални решения или други продукти с цифрови елементи.

ENISA поддържа страница и FAQ за CRA Single Reporting Platform, където се публикува информация за платформата, процеса на докладване, полетата в уведомленията, тестовия период и подготвителните материали за обучения и dry-run упражнения.

Още по темата може да прочетете тук.

Нов етап от прилагането на AI Act – от 2 август 2026

От 2 август 2026 г. започва нов важен етап от прилагането на Закона на ЕС за изкуствения интелект (AI Act). Регламентът е първата цялостна правна рамка за изкуствен интелект в света. Неговата цел е да насърчи надежден, безопасен и ориентиран към човека изкуствен интелект. Той вече е в сила от 1 август 2024 г. и се прилага поетапно. Част от забранените AI практики и задълженията за AI грамотност се прилагат от февруари 2025 г. Правилата за моделите с общо предназначение започнаха да се прилагат през август 2025 г. От август 2026 г. AI Act става приложим в по-голямата си част, с някои изключения.

Основната логика на AI Act е рисково-базираният подход. Това означава, че изискванията зависят от риска, който дадена AI система може да създаде. Някои практики са забранени. Високорисковите системи подлежат на по-строги изисквания. Системите, при които е важна прозрачността, изискват потребителите да бъдат информирани, че взаимодействат с изкуствен интелект или че дадено съдържание е генерирано от AI. За организациите това означава, че подготовката не трябва да се отлага.

Първата практическа стъпка е да се изготви **регистър на използваните AI системи**. В него е добре да се включат вътрешни инструменти, външни платформи, пилотни проекти, AI функции в SaaS продукти и решения, използвани от доставчици. За всяка система трябва да е ясно за какво се използва, кой е отговорен, какви данни обработва и дали попада в рискова категория.

Следващата стъпка е **класифициране на риска**. Организацията трябва да прецени дали дадена система е забранена, високорискова, подлежи на изисквания за прозрачност или е с минимален риск. Тази оценка не бива да бъде еднократна. Тя трябва да се актуализира при въвеждане на нов инструмент, промяна на доставчик или промяна във функцията на системата.

Особено важни стават изискванията за **прозрачност**. Хората трябва да бъдат информирани, когато взаимодействат с AI система, например чатбот. AI-генерираното съдържание трябва да бъде разпознаваемо. Deepfake изображения, звук или видео, както и AI-генериран текст по теми от обществен интерес, трябва да бъдат ясно обозначени. Тези правила започват да се прилагат през август 2026 г.

Практически това изисква по-добро **вътрешно управление**. Организациите трябва да определят кой одобрява използването на AI, кой отговаря за всяка система и как се ескалират проблеми. Добре е да се подготвят правила за използване на AI, процедури за преглед на доставчици, доказателства за AI обучение на служителите и записи за взети решения. Това превръща съответствието с AI Act в управленски процес, а не в еднократна юридическа проверка.

Важно е да се уточни, че не всички изисквания започват едновременно. За част от високорисковите AI системи са предвидени по-дълги преходни срокове. Според актуалната информация на Европейската комисия правилата за високорискови системи в области като биометрия, критична инфраструктура, образование, заетост, миграция и граничен контрол ще се прилагат от 2 декември 2027 г. За AI системи, вградени в регулирани продукти, срокът е 2 август 2028 г.

Какво е полезно да предприемат организациите още сега:

- ✅ да изготвят регистър на използваните AI системи;
- ✅ да определят за каква цел се използват;
- ✅ да класифицират рисковете за всяка система;
- ✅ да въведат правила за информиране на потребителите;
- ✅ да обозначават AI-генерирано съдържание;
- ✅ да документират кой отговаря за използването на AI;
- ✅ да следят насоките на Европейската комисия и AI Office.

Още по темата може да прочетете тук.

Киберустойчивост на практика: учения, заплахи и реални инциденти

Изграждането на киберустойчивост не се изчерпва с приемането на нови регулации. През последните месеци европейските институции публикуваха редица доклади и проведоха инициативи, които показват как новите правила се превръщат в реални действия. Общата тенденция е ясна – повече подготовка, повече координация и по-добро разбиране на развиващите се заплахи.

Една от най-мащабните инициативи беше Cyber Europe 2026, организирана от ENISA. Учението събра над 5000 участници и симулира кибератаки срещу железопътния и морския транспорт. Основната цел беше да се провери доколко държавите, операторите на критична инфраструктура и компетентните органи могат да реагират координирано при мащабни инциденти.

В същото време Europol IOCTA 2026 предупреждава, че киберпрестъпността използва все по-усъвършенствани техники. Изкуственият интелект, криптирането, прокси услугите и криптовалутите улесняват измами, социално инженерство и прикриване на престъпна дейност. Особено важна за организациите е тенденцията към по-убедителни фишинг и измамни кампании.

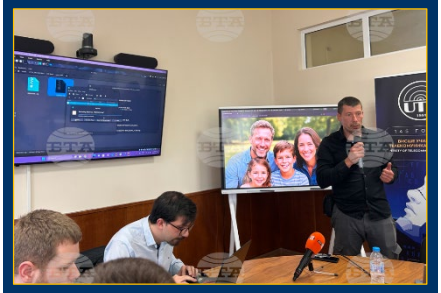
Подобна тенденция се вижда и в България. През май 2026 г. ГДБОП съобщи за фишинг съобщения от името на МВР, институции и куриерски компании. Кампанията е достигнала до десетки хиляди потребители, а целта е била източване на лични данни и банкови сметки. По данни на МВР в помощ на престъпната дейност е използван и изкуствен интелект. Този и други случаи са показателени за промяната в социалното инженерство. Измамите вече не се ограничават до класически имейл фишинг. ГДБОП описва различни форми като фишинг, **smishing** чрез SMS и **vishing** чрез телефонни обаждания. Общото между тях е имитирането на легитимни организации и създаването на чувство за спешност, страх или доверие.

Развитието на заплахите се потвърждава и от CERT-EU Threat Landscape Report. Докладът отчита увеличение на проследяваните заплахи и обръща внимание на засиления интерес към интернет-достъпни устройства, веригите на доставки и техниките за социално инженерство. Това показва, че защитата на организациите все по-

често зависи не само от собствените им системи, но и от сигурността на доставчиците и използваните цифрови услуги.

Подобна тенденция се наблюдава и във финансовия сектор. Първият годишен доклад по Digital Operational Resilience Act (DORA) показва, че значителна част от докладваните ICT инциденти имат трансгранично въздействие. Това потвърждава необходимостта от по-добро управление на доставчиците, ясни процедури за докладване и координирана реакция при инциденти.

Първият киберполигон в България ще обучава студенти



Във Висшето училище по телекомуникации и пощи беше открит първият в България киберполигон за студенти. Той е разработен в партньорство с Института по информационни и комуникационни технологии към БАН и е насочен към практическо обучение чрез реалистични симулации на киберинциденти. Вместо да разчитат основно на лекции и презентации, студентите ще работят в контролирана среда, максимално близка до реалните условия.

Киберполигонът включва сценарии за анализ на мрежов трафик, защита на уеб приложения, SQL injection, цифрова криминалистика, анализ на зловреден софтуер, пенетрейшън тестове и етично хакерство. Възможно е да се симулират и по-сложни ситуации, включително атаки срещу критична инфраструктура. Сценариите могат да бъдат непрекъснато обновявани според нововъзникващите киберзаплахи, а учебната среда позволява експерименти без риск за реални информационни системи.

Цел е студентите да изградят аналитично мислене и практически умения за реакция при реални инциденти, така че след завършването си да бъдат подготвени за работа в публичния и частния сектор.

Още по темата може да прочетете тук.

„Кибер гвардейци“: младежка инициатива за киберкултура и взаимопомощ

Cyber Guardians
обучения на млади хора за оказване на взаимопомощ в сферата на киберсигурността
Инициатива в подкрепа на младежката киберосведоменост и взаимопомощ

Цифров иновационен хъб „Тракия“ поставя началото на инициативата Cyber Guardians (Кибер гвардейци) в партньорство с Ротари клуб Перник. Тя е насочена към изграждане на знания, увереност и култура за взаимопомощ в областта на киберсигурността сред младите хора.

Идеята е младежите да бъдат подготвени не само да се предпазват онлайн, но и да помагат на свои връстници, родители, учители и по-възрастни хора. Обученията включват реални

киберрискове, разпознаване на измамни съобщения, опити за манипулация и действия при съмнение за киберинцидент.

Пълният текст може да прочетете тук.

ЦИХ „Тракия“ представи напредък в сигурността на DNS на европейски семинар в Брюксел

Цифров иновационен хъб „Тракия“ представи българския принос в областта на сигурността на DNS по време на Европейския семинар за киберустойчивост в Брюксел. Хъбът е единственият български участник във Форума на заинтересованите страни за внедряване на интернет стандарти, координиран от Европейската комисия.

По време на семинара беше представен потенциалът на Protective DNS като практичен слой на киберустойчивостта. Той може да помогне за предотвратяване на свързването с известни злонамерени или високорискови домейни, свързани с фишинг, зловреден софтуер, ransomware инфраструктура, ботнет мрежи и командно-контролни сървъри.

Пълният текст може да прочетете тук.

Връзки към събития по киберсигурност и информационна устойчивост

- Справочник за събития по киберсигурнос в България (Българска Фондация за Киберсигурност)
- 31st European Symposium on Research in Computer Security (ESORICS) 2026, 14-18 September, 2026, Rome, Italy
- 12th Trust Services and eID Forum, 15 Sept., 2026, Tallinn, Estonia

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. ас. д-р Зорница Димитрова – ИИКТ-БАН
5. Ясен Танев – Цифров иновационен хъб „Тракия“
6. д-р Ирена Младенова – СУ „Св. Климент Охридски“
7. д-р Емилия Печева – Британско посолство в София

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