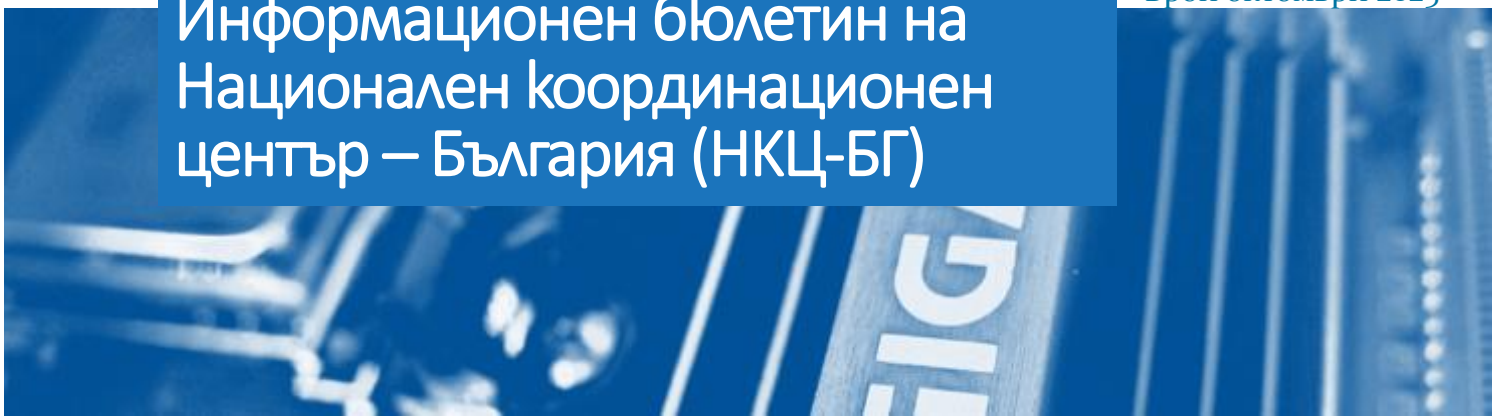
Министерство на електронното управление

Съфинансирано от Европейския съюз

Брой октомври 2025

Информационен бюлетин на Национален координационен център – България (НКЦ-БГ)



УПРАВИТЕЛНИЯТ СЪВЕТ НА ECCC И МРЕЖАТА ОТ НАЦИОНАЛНИ КООРДИНАЦИОННИ ЦЕНТРОВЕ СЕ СРЕЩНАХА В ЛЕОН, ИСПАНИЯ

Дата: 15-16 октомври 2025 г.

14-тото заседание на Управителния съвет на Европейския център за компетентност в киберсигурността (ECCC) се проведе в Леон, Испания, заедно със заседанието на Мрежата от национални координационни центрове (NCC). Дискусиите бяха фокусирани върху изпълнението на програмите „Цифрова Европа“ (DEP) и „Хоризонт Европа“, финансираните проекти и разработването на трансгранични оперативни центрове за сигурност. Специално внимание беше обърнато на ролята на ECCC в следващата многогодишна финансова рамка и Европейския фонд за конкурентоспособност, с цел укрепване на европейските способности за киберсигурност. Освен това беше подчертана стойността на обмена на експертен опит и беше представен Atlas - европейската платформа за насърчаване на сътрудничеството в киберсектора. Повече информация можете да намерите на уебсайта на ECCC: https://cybersecurity-centre.europa.eu/news/eccc-governing-board-and-network-national-coordination-centres-met-leon-spain-2025-10-17_en .

Източник: ECCC

Европейски център за компетентност в областта на киберсигурността - ECCC

ECCC има за цел да увеличи капацитета и конкурентоспособността на Европа в областта на киберсигурността, като работи съвместно с Мрежа от национални координационни центрове (НКЦ) за изграждане на силна общност за киберсигурност.



КОНФЕРЕНЦИЯ ЗА КИБЕРСИГУРНОСТ „BCC 2025“, БУКУРЕЩ, РУМЪНИЯ



Министерството на електронното управление взе участие в Конференция по киберсигурност BCC2025, която се проведе в периода 5 - 9 октомври 2025г. в Букурещ, Румъния. Събитието беше организирано от Румънската Национална дирекция по киберсигурност (DNSC), с подкрепата на NCC RO (НКЦ Румъния), ANSSI Румъния, в сътрудничество с Агенцията на Европейския съюз за киберсигурност (ENISA) и Европейския център за компетентност в областта на киберсигурността (ECCC).

Участие взеха над 500 висши ръководители, правителствени служители, експерти от индустрията и академични експерти.

Фокусът на конференцията беше върху практическото прилагане на най-новите политики и законодателство на ЕС, включително Директива NIS2, Закона за киберустойчивост (Cyber Resilience Act - CRA), Акта за киберсигурност на ЕС и Акта за солидарност в областта на киберсигурността. Бяха засегнати теми, свързани с рисковете и стратегиите за смекчаване на риска в жизненоважни инфраструктурни сектори като енергетика, телекомуникации, сателитни системи, свързани превозни средства и здравеопазване. Бяха проведени множество дискусии относно кибератаките, подпомагани от AI, както и ролята на AI във военното дело и киберсигурността.

Министерството на електронното управление взе участие в Конференция по киберсигурност BCC2025, която се проведе в периода 5 - 9 октомври 2025г. в Букурещ, Румъния.

Фокусът на конференцията беше върху практическото прилагане на най-новите политики и законодателство на ЕС, включително Директива NIS2, Закона за киберустойчивост (Cyber Resilience Act - CRA), Акта за киберсигурност на ЕС и Акта за солидарност в областта на киберсигурността.



Първият ден от конференцията беше посветен на теми, свързани основно със стратегическите насоки и цялостната рамка на киберсигурността.

Други теми на дискусия бяха:

- Геополитически контекст и хибридни заплахи: дискусии за това как регионалните конфликти и геополитическото напрежение влияят върху киберсигурността, както и за ролята на хибридните заплахи (комбинация от кибератаки и дезинформация).

- Политика и регулация на ЕС: сесия, посветена на предизвикателствата при прилагането на новите европейски киберзакони, като Директива NIS2.

Вторият ден от конференцията беше посветен на Националния координационен център на Румъния, като бяха установени контакти с представители на домакините и с представители на пет други държави. На срещата бяха представени проектът за финансиране на малки и средни предприятия, изпълняван от НКЦ Румъния, както и бяха обсъдени редица важни въпроси, засягащи дейността на Националните Координационни Центрове (НКЦ). Друга тема беше изграждането на киберобщност – начинание, което представлява огромно предизвикателство за всички държави. На срещата беше представена Процедурата на България за „Подкрепа за подобряване на киберсигурността в малките и средни предприятия в Република България" по Програма „Цифрова Европа" 2021-2027.

В рамките на събитието беше проведена дискусия на нововъзникващи заплахи, свързани с AI и Квантова устойчивост. Темите бяха:

1. AI-подпомагани кибератаки и как изкуственият интелект променя както атаките, така и защитата.

2. Необходимостта от разработване на квантово-устойчиви системи за бъдеща сигурност.

3. Сътрудничество и изграждане на капацитет. Засилване на трансграничното сътрудничество между държавите и секторите, както и инвестициите в киберумения и регионален капацитет на Европа.



Третият ден от конференцията беше посветен изключително на Закона за киберустойчивост (CRA). Основните теми включваха:

- Изисквания за продукти с цифрови елементи: дискусии за това как CRA въвежда задължителни изисквания за киберсигурност по време на целия жизнен цикъл на продукта.
- Надзор на пазара на ЕС: рамката за надзор и как се постига съответствие с CRA.
- Възможности за иновации: балансиране на регулацията с подкрепата за бизнеса и иновациите в ерата на CRA.

ВЪЗМОЖНОСТИ ЗА ФИНАНСИРАНЕ

Нови покани за финансиране по програмата „Цифрова Европа“ за 2025 г.

По програмата „Цифрова Европа“ (DEP) са публикувани покани за набиране на проектни предложения за 2025 г. с бюджет от 50 милиона евро.

Новите покани DIGITAL-ECCC-2025-DEPLOY-CYBER-09 са фокусирани върху:

- Инструменти, технологии и услуги, базирани на изкуствен интелект - CYBER-09-CYBERAI - 15 милиона евро
- Иновативни решения за киберсигурност за МСП - CYBER-09-UPTAKE - 15 милиона евро
- Подготвителни действия - CYBER-09-COORDPREP - 10 милиона евро
- Регионални кабелни хъбове - CYBER-09-CABLEHUBS - 10 милиона евро

Предложения могат да бъдат подавани от 28 октомври 2025 г. до 31 март 2026 г.

Публикувани са нови покани за финансиране по програмата „Дигитална Европа“ за 2025 г. със срок за кандидатстване до 31 март 2026 г.

Новите покани Digital-ECCC-2025-Deploy-Cyber-09 са фокусирани върху:

- *инструменти, технологии и услуги, базирани на изкуствен интелект - Cyber-09-Cyberai - 15 милиона евро*
- *иновативни решения за киберсигурност за МСП - Cyber-09-Uptake - 15 милиона евро*
- *подготвителни действия - Cyber-09-Coordprep - 10 милиона евро*



За повече информация, моля, посетете Портала за финансиране и обществени поръчки на ЕС.

Прочетете повече: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/calls-for-proposals?isExactMatch=true&keywords=DIGITAL-ECCC-2025-DEPLOY-CYBER-09&status=31094501,31094502,31094503&order=DESC&pageNumber=1&pageSize=50&sortBy=startDate

Покани за предложения на DEP за изкуствен интелект и големи данни

Сред последните актуализации на работната програма на DEP са въведени нови покани след изменението на работната програма на DEP за 2025-2027 г.

Предложенията могат да се подават от 4 ноември 2025 г. По-долу са някои от темите и наличният бюджет:

• Консолидиране (79,2 милиона евро) и завършване (8 милиона евро) на мрежата от европейски центрове за цифрови иновации;

• Интегриране на решения с изкуствен интелект в публичните администрации (1,8 милиона евро);

• Разработване на виртуални тестови платформи в подкрепа на иновациите (17 милиона евро);

• Подкрепа за биомедицински изследвания чрез Европейската инфраструктура за геномни данни (22,5 милиона евро);

• Внедряване на решения, базирани на изкуствен интелект, за медицинско изобразяване (14,4 милиона евро);

• Разработване на модели на GenAI в производствения сектор (9 милиона евро);

• Укрепване на националните центрове на Европейската обсерватория за цифрови медии (6 милиона евро).

• регионални кабелни хъбове - Cyber-09-Cablehubs - 10 милиона евро

До 4 ноември 2025 г. могат да се подават предложения по програма DEP за изкуствен интелект и големи данни по следните теми:

• Консолидиране (79,2 милиона евро) и завършване (8 милиона евро) на мрежата от европейски центрове за цифрови иновации;

• Интегриране на решения с изкуствен интелект в публичните администрации (1,8 милиона евро);



За повече информация относно конкретни покани и крайни срокове, моля, посетете Портала за финансиране и обществени поръчки на ЕС.

Прочетете още: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home

Покани за предложения по DEP за напреднали цифрови умения

Изменението на работната програма на DEP за 2025-2027 г. доведе до въвеждането на две допълнителни покани за предложения в областта „Разширени цифрови умения“:

• DIGITAL-2026-SKILLS-09-COMPETITIONS - DIGITAL-CSA DIGITAL: целта е да се ангажират младите хора в състезания, които засилват креативността и иновациите чрез използването на авангардни технологии като изкуствен интелект, виртуални светове, полупроводници и др.

• DIGITAL-2026-SKILLS-09-LEAGUE-OF-ACADEMIES - DIGITAL-CSA DIGITAL: създаването на „Лига“ от европейски академии за цифрови умения, насочена към координиране, обединяване и разширяване на обучението в секторите на изкуствения интелект, квантовата технология, полупроводниците и виртуалния свят.

Предложения за двете покани могат да бъдат подадени от 4 ноември 2025 г., с краен срок 3 март 2026 г.

За повече информация относно поканите, моля, посетете портала за финансиране и обществени поръчки: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home

• Разработване на виртуални тестови платформи в подкрепа на иновациите (17 милиона евро);

• Подкрепа за биомедицински изследвания чрез Европейската инфраструктура за геномни данни (22,5 милиона евро);

• Внедряване на решения, базирани на изкуствен интелект, за медицинско изобразяване (14,4 милиона евро);

• Разработване на модели на GenAI в производствения сектор (9 милиона евро);

• Укрепване на националните центрове на Европейската обсерватория за цифрови медии (6 милиона евро).



Работна програма на „Хоризонт Европа“ за 2025 г.

Работна програма на „Хоризонт Европа“ за 2025 г. описва подробно възможностите за финансиране в областта на киберсигурността. По-конкретно, те са включени в Клъстер 3 и имат бюджет от 90,55 милиона евро:

• Генеративен изкуствен интелект, приложен към киберсигурността (40 милиона евро);

• Нови инструменти и усъвършенствани процеси за оперативна киберсигурност (23,55 милиона евро);

• Технологии за запазване на поверителността (11 милиона евро);

• Оценки на сигурността на постквантови криптографски системи (4 милиона евро);

• Сигурни внедрявания на PQC системи (6 милиона евро);

• Интегриране на PQC алгоритми във високо ниво протоколи (6 милиона евро).

Предложенията за проекти трябва да бъдат подадени до 12 ноември 2025 г.

За повече информация относно конкретни покани, моля, посетете портала за финансиране и търгове: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home

До 3 март 2026 г. са публикувани две допълнителни покани за предложения в областта „Разширени цифрови умения“:

• DIGITAL-2026-SKILLS-09-COMPETITIONS - DIGITAL-CSA DIGITAL: ангажиране на младите хора в състезания.

• DIGITAL-2026-SKILLS-09-LEAGUE-OF-ACADEMIES - DIGITAL-CSA DIGITAL: създаването на „Лига“ от европейски академии за цифрови умения.

МЕСЕЧЕН АНАЛИЗ НА ЗАПЛАХИТЕ НА ДИРЕКЦИЯ „МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ“

По данни, получени в Дирекция „Мрежова и информационна сигурност“ към Министерството на електронното управление, за месец октомври 2025 г. в ЕС са установени 720 докладвани заплахи, като хактивистките атаки от типа „разпределен отказ от услуги“ (DDoS) си остават най-активната заплаха. Сред първите четири целеви държави членки на ЕС са Германия, Италия, Полша и Испания, към които по-специално е насочена DDoS кампания.

Извършен от Дирекция „Мрежова и информационна сигурност“ месечен анализ показва, че в ЕС се запазва



Наблюдава се спад на докладваните инциденти към всички сектори с изключение на лек ръст на докладваните Ransomware инциденти в сектор „Цифрова инфраструктура“.



тенденцията основната част от атаките да са от типа DDoS.

Според анализът, в България основно преобладават phishing атаките.

Отчита се увеличаване на инцидентите във всички сектори, като сектор „публична администрация“ остава с най-големия брой докладвани инциденти, следван от сектори „Транспорт“ и „Цифрова инфраструктура“.

Най-много на брой са ransomware атаките от групата qilin.



Най-силно засегнати сектори в ЕС (от Ransomware и други видове заплахи)

Анализите отчитат увеличаване на инциденти във всички сектори, като сектор „публична администрация“ остава с най-големия брой докладвани инциденти, следван от сектори „Транспорт“ и „Цифрова инфраструктура“.

Най-силно засегнатите сектори от ransomware в ЕС са „Производство“, „Цифрова инфраструктура“ и „Публична администрация“.

Секторно наблюдение

Забелязва се ръст на докладваните инциденти във всички сектори спрямо предходния месец с изключение на сектор „Публична администрация“, където бройката се запазва и сектор „Транспорт“, където се забелязва спад на докладваните инциденти.

Основни видове атаки в ЕС

DDoS атаките са основният тип атака, извършена през месец октомври.

Мониторинг на вида заплахи

За докладвания период през месец октомври анализът показва, че спрямо докладвания период през месец септември, има драстичен спад на докладваните инциденти към организации на държавите членки на ЕС. Най-драстичен спад е забелязан в категорията DDoS атаки. Единствено се забелязва лек ръст в сферата на кибершпионажа.

Ransomware атаки докладвани в ЕС

Подобно на предходния месец, най-много са ransomware атаките, извършени от групата qilin. На второ и трето място са ShinyHunters и DragonForce.

Qilin е активна ransomware група, засечена за пръв път през 2022 г.. Характерното за нея е, че използва т.нар. двойно изнудване – криптиране на данни и отправяне на заплаха за публичното им разкриване. Групата работи по модела Ransomware-as-a-Service (RaaS), като атаките често започват чрез phishing, уязвимости в публични услуги или компрометирани акаунти. След пробива се използват инструменти като PowerShell, PsExec и Cobalt Strike за придвижване и деактивиране на защити.



Qilin таргетира организации от различни сектори особено в Западна и Централна Европа и е известна с агресивен натиск върху жертвите чрез собствен сайт за публикуване на компрометирани данни в тъмната мрежа.

ShinyHunters е добре позната хактивистка и киберпрестъпна група, появила се около 2020 г., която бързо добива международна известност с масови пробиви в бази данни и продажба на откраднатa информация в тъмната мрежа. За кратко време организацията е свързана с десетки атаки срещу компании от различни индустрии – технологии, електронна търговия, образование и дори държавни институции. Сред техните жертви са били фирми от САЩ, Европа и Азия, като при някои случаи са изтекли десетки милиони потребителски профили, включително имейли, пароли, лични данни и финансови записи. За разлика от класическите „хактивисти“, които действат с идеологически или политически мотиви, ShinyHunters се смятат за по-прагматична група, фокусирана върху финансовата изгода — често продават или изнудват жертвите, за да получат откуп, преди да публикуват информацията. Въпреки това, те поддържат определен образ на „елитни хакери“ и се позиционират в онлайн пространството като наследници на по-стари групи като *Gnosticplayers*. Международни разследвания, включително от ФБР и Европол, са се опитвали да идентифицират членовете им, като през 2023 г. един предполагаем участник е арестуван във Франция. Въпреки подобни действия, ShinyHunters продължават да се свързват с нови пробиви и да символизират колко лесно информацията на милиони потребители може да се превърне в стока на черния пазар на данни.

DragonForce Malaysia е хактивистка група, възникнала около 2020 г. и известна най-вече със своите кибератаки, насочени към правителствени и корпоративни системи, често мотивирани от политически и идеологически каузи. Групата става особено популярна след 2021 г., когато организира координирани кампании срещу израелски институции и компании под лозунга „OpsBedil“— действие, което комбинира класически DDoS атаки, дефейсване на уебсайтове (неоторизирана промяна на съдържанието) и извличане на данни. DragonForce Malaysia активно използват социалните мрежи и платформи като Telegram, за да координира своите операции, да споделя пробити бази данни и да насърчава съмишленици от целия свят да се присъединят към техните кампании. За разлика от чисто криминални групи като ShinyHunters, DragonForce се представят като „кибербойци“ за социална справедливост и защита на мюсюлманските общности по света, въпреки че методите им нарушават множество международни закони. През годините те са атакували организации в различни страни, включително Индия, Израел, Сингапур и Тайланд, и продължават да бъдат активен фактор в хактивистката сцена, използвайки киберпространството като инструмент за протест и натиск.

Сектори, засегнати от Ransomware в ЕС

Най-силно засегнатите сектори от ransomware в ЕС са „Производство“, „Цифрова инфраструктура“ и „Публична администрация“.



Спрямо докладвания период през месец септември, се забелязва ръст в сектор „Цифрова инфраструктура“. В сектор „Транспорт“ се забелязва същия брой инциденти, докато в другите сектори се забелязва спад.

Регистрирани кибератаки в CERT България

Най-важните докладвани и регистрирани атаки в България за месец октомври са Malicious Code (зловреден код) и Phishing.

Заключение

В обобщение, извършеният месечен анализ показва, че в ЕС се запазва тенденцията от предходния месец като основната част от атаките са от типа DDoS. Според предоставените данни от CERT BG прави впечатление, че в България основно преобладават phishing атаките, като се забелязва много лек спад спрямо предходния месец.





Министерство на електронното управление

ул. „Ген. Гурко“ № 6

Гр. София 1000

Ел. поща: bnccc@egov.government.bg

Ел. адрес: https://ncc.egov.bg/