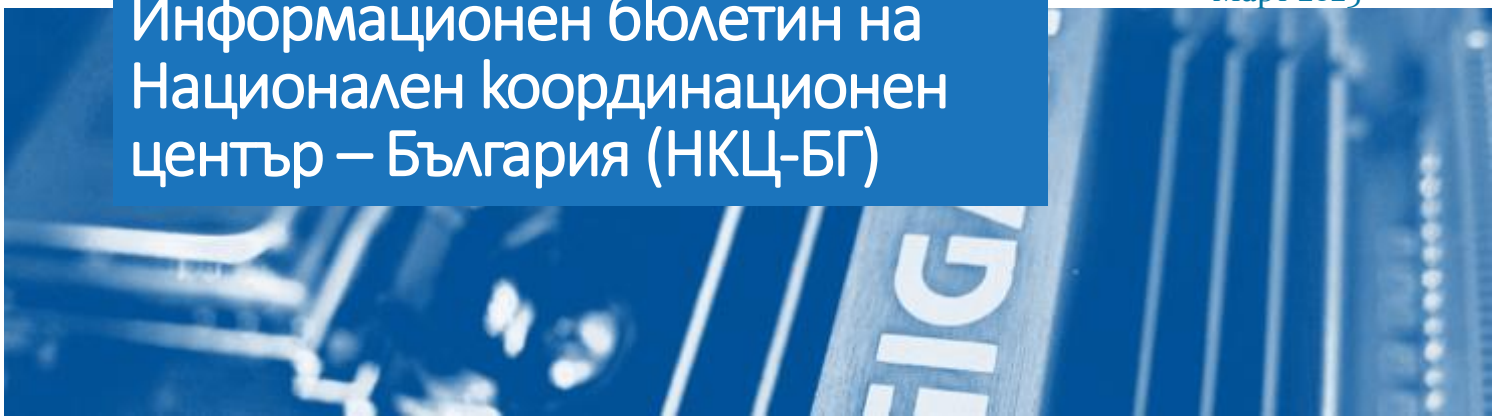
Министерство на електронното управление

Съфинансирано от Европейския съюз

Март 2025

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



## АНАЛИЗ ЗА ИЗБОР НА ТЕМИ ЗА ФИНАНСОВА ПОДКРЕПА НА ТРЕТИ СТРАНИ

В този брой на бюлетина ще представим разработен в рамките на Проект 101128086 "Национален координационен център – България – NCC-BG" анализ за избор на теми за финансова подкрепа на трети страни на база проведено проучване през платформата на ЕС EU Survey в периода от 24.2.2025 г. до 10.3.2025 г.
На база направеното задълбочено проучване на поставените в анкетата въпроси, свързани с киберсигурността в МСП в България са изведени следните значими за целевата група теми, които да се използват за програмата за финансова подкрепа на трети страни, а именно:

### НКЦ-БГ

***Националният координационен център – България (НКЦ-БГ) проведе задълбочен анализ на конкретните теми, свързани с киберсигурността. За целта беше разработено онлайн изследване/проучване, което се проведе с цел събиране на информация за киберсигурността от МСП, за***



***да се гарантира, че темите са съобразени с настоящия контекст и с най-новите развития в областта на киберсигурността.***

**Тема: Подобряване на съществуващи или внедряване на съвременни <u>облачно базирани</u> софтуерни решения за киберсигурност.**
**Възможни приложими решения за темата са:**

- *Реализиране на център за киберсигурност като услуга (SoCaaS)*
- *Изграждане или наемане на WAF*
- *Изграждане на решение за споделяне на файлове с криптирана връзка*
- *Наемане на инфраструктура като услуга (IaaS)*
- *Облачно базирано DLP решение*
- *EDR решения*
- *SIEM решения*
- *Надграждане/изграждане на 2FA за уеб приложение*
- *Наемане на платформа за разпознаване и превенция на киберзаплахи (CTI)*

**Тема: Подобряване на съществуващи или внедряване на съвременни <u>локално базирани</u> хардуерни или софтуерни решения за киберсигурност.**

**Възможни приложими решения за темата са:**

- *Внедряване на EDR, XDR решения за откриване и реагиране на заплахи*
- *Внедряване на SIEM решения за управление на уязвимостта*
- *Внедряване/надграждане на система за защита на информацията в локална мрежа. (напр. защитна стена; система за разпознаване на пробиви (IPS))*
- *Внедряване/надграждане на система за архивиране на информация (напр. автоматично архивиране на информация от сървъри/работни станции/мобилни устройства; вграждане на защита от атаки от типа "ransomware" и др.)*
- *Изграждане на защитени канали за предаване на данни между клиенти или офиси (VPN свързаност)*



- *Изграждане на система за управление на достъпа.*
- *Внедряване/надграждане на система за управление на съхранението и споделянето на информация (напр. централизирано управление на достъпа на служителите до информация и споделянето; наличие на журнален запис на действията на потребителите (audit log); DLP система; хардуерни елементи, включени в минималния обхват; сървър за съхранение и управление на информация и данни и др.)*
- *Развитие на професионалния капацитет и повишаване на квалификацията на персонала в областта на киберсигурността*
- *Покупка на лицензии (например антивирусни, база данни, NextGENFirewall, сървъри, сертификати и др.).*

**Тема: Подкрепа за съответствие с изискванията на Директива (ЕС) 2022/2555.**

**Възможни приложими решения за темата са:**

- *Одити по информационна сигурност*
- *Сертифициране по ISO 27001-2022*
- *Обучения*
- *Провеждане на тестове за уязвимости*

Киберсигурността остава динамична и предизвикателна област, която изисква непрекъснати усилия и инвестиции както на международно, така и на национално ниво. Важно е всички заинтересовани страни – правителства, бизнеси и граждани – да работят заедно за създаване на по-безопасна цифрова среда. Въпреки предизвикателствата, има положителни тенденции в развитието на киберсигурността за МСП в България.

С повишаване на осведомеността, достъпността на решенията и подкрепата от държавата, малките и средни предприятия могат да подобрят своята устойчивост срещу киберзаплахи. Важно е обаче да се продължат усилията за обучение и подкрепа, за да се гарантира, че МСП ще бъдат добре подготвени за бъдещите предизвикателства в областта на киберсигурността.








*Министерство на електронното управление*

*ул. „Ген. Гурко“ № 6*

*Гр. София 1000*

*Ел. поща: bnccc@egov.government.bg*

*Ел. адрес: https://ncc.egov.bg/*