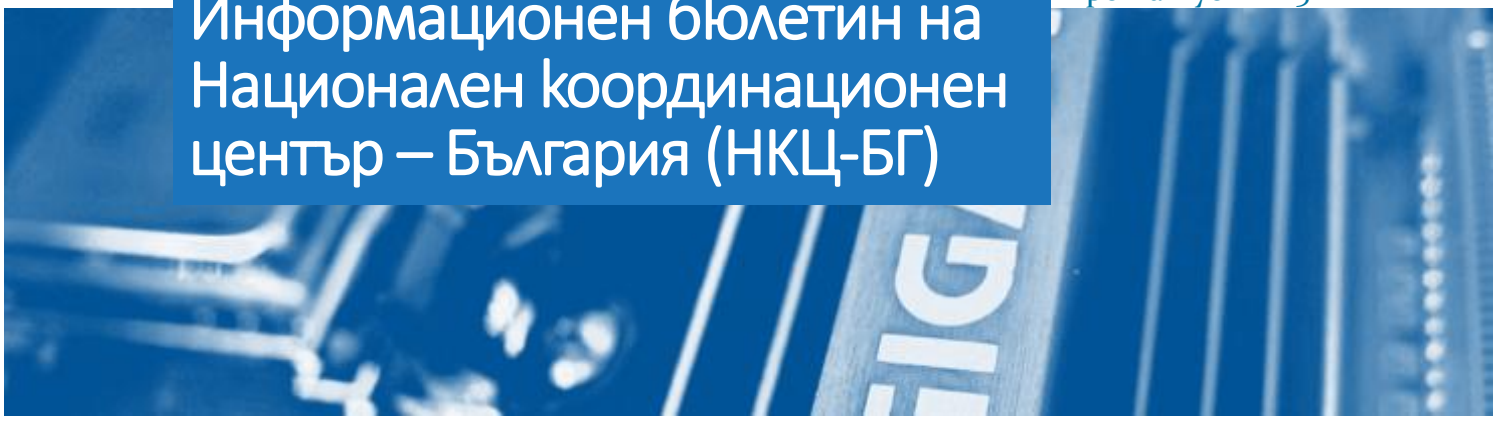
Министерство на електронното управление

Съфинансирано от Европейския съюз

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

Брой август 2025



ПУБЛИКУВАНА Е НОВАТА РАБОТНА ПРОГРАМА НА ПРОГРАМА „ЦИФРОВА ЕВРОПА“ ЗА КИБЕРСИГУРНОСТ С БЮДЖЕТ ОТ 390 МИЛИОНА ЕВРО ЗА ПЕРИОДА 2025-2027 Г.

Публикувана е новата работна програма на ПРОГРАМА „ЦИФРОВА ЕВРОПА“ за киберсигурност с бюджет от 390 милиона евро за периода 2025-2027 г., насочена към подкрепа за укрепването на нивата на киберсигурност на Съюза, като се фокусира върху няколко ключови области:

• нови технологии, изкуствен интелект и постквантов преход;

• прилагане на Закона за киберсолидарност;

• действия за укрепване на киберустойчивостта на ЕС, включително подкрепа за транспонирането на съответното законодателство на ЕС (Директива NIS2, Закон за киберустойчивост, CSA, DORA, GRPR и Закон за изкуствен интелект).

Програми за киберсигурност на ЕС

Европейският съюз (ЕС) предлага разнообразни възможности за финансиране на проекти за подобряване на киберсигурност по различни програми.

Специфични за тази сфера са директно управляваните от съюза програми Цифрова Европа (Digital Europe) и Хоризонт Европа (Horizon Europe), по които се



По-конкретно, откритите покани за представяне на предложения по ПРОГРАМА „ЦИФРОВА ЕВРОПА“ имат бюджет от 55 милиона евро и се фокусират върху три макрообласти:

• преход към постквантова инфраструктура с публичен ключ (15 милиона евро);

• укрепване на мрежата от национални координационни центрове (10 милиона евро);

• укрепване на киберсигурността на болниците и доставчиците на здравни услуги (30 милиона евро).

Предложенията трябва да бъдат подадени до 7 октомври 2025 г. в 17:00 ч. (централноевропейско време).

Допустими организации: всички национални организации, които отговарят на специфичните изисквания, посочени във всяка покана.

За повече информация относно конкретните покани, моля, посетете портала за финансиране и обществени поръчки на ЕС - https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/calls-for-proposals?isExactMatch=true&status=31094501,31094502&order=DESC&pageNumber=1&pageSize=50&sortBy=startDate .

РАБОТНА ПРОГРАМА НА „ХОРИЗОНТ ЕВРОПА“ 2025

Работна програма на „Хоризонт Европа“ 2025 описва подробно възможностите за финансиране в рамките на трите макрообласти на програмата:

• научни постижения (Стълб I);

• глобални предизвикателства и индустриална конкурентоспособност (Стълб II);

• иновации (Стълб III).

публикуват ежегодно директни покани за финансиране на проекти.

Програма „Цифрова Европа“ (2021-2027).

Програмата „Цифрова Европа“ е инициатива на Европейския съюз за периода 2021-2027 г., която цели да подпомогне цифровата трансформация в целия ЕС. Бюджетът на програмата е 7,588 млрд. евро. Целта на програмата е да помогне страните от ЕС да подобрят своята цифрова инфраструктура и цифровите си възможности, така че да могат по-добре да се адаптират и да се възползват от възможностите на цифровата ера. Повече информация за програмата: https://digital-strategy.ec.europa.eu/ro/activities/work-programmes-digital



По-конкретно, отворените покани на „Хоризонт Европа“ имат бюджет от 90,55 милиона евро в Клъстер 3 и се фокусират върху шест теми:

• Генеративен изкуствен интелект, приложим за 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);

• Сигурно внедряване на PQC системи (6 милиона евро);

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

Предложенията за проекти трябва да бъдат подадени до 12 ноември 2025 г., 17:00 ч. (централноевропейско време).

За повече информация относно конкретните покани, моля, посетете портала за финансиране и обществени поръчки на ЕС - https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/calls-for-proposals?isExactMatch=true&status=31094501,31094502&order=DESC&pageNumber=1&pageSize=50&sortBy=startDate .

МЕНИДЖЪР НА ПАРОЛИ – НАЧИН ДА ИЗБЕГНЕМ ИЗПОЛЗВАНЕТО НА ЛЕСНИ ПАРОЛИ

В ерата на информационните технологии всеки един от нас има регистрация в безброй платформи. Най-добрият начин да избегнем ползването на лесни за хакване пароли или еднакви /подобни пароли, е използването на т.нар. password manager – мениджър на паролите. Много често хората използват една и съща парола навсякъде. Ако тази парола изтече, то всеки един от акаунтите бива компрометиран.

Програма Хоризонт Европа

Хоризонт Европа е програма за подкрепа на научните изследвания и иновации в Европа. Това е най-голямата програма, която осигурява финансова подкрепа за изследователски и иновационни проекти в различни области, включително за киберсигурност. Програмата Хоризонт Европа има за цел да подкрепи конкурентоспособността на Европа в глобален мащаб и да подобри жизнения стандарт на гражданите в ЕС. Бюджетът на програмата е 95,5 милиарда евро. Повече информация за програмата: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en



Когато използваме мениджър на паролите, главната ни парола не се съхранява никъде и тя е вид пазител на останалите пароли. Препоръчително е тази парола да е максимално сигурна с високо ниво на сложност и да не се съхранява на сървър, дори да не бъде записвана никъде, а запомнена.

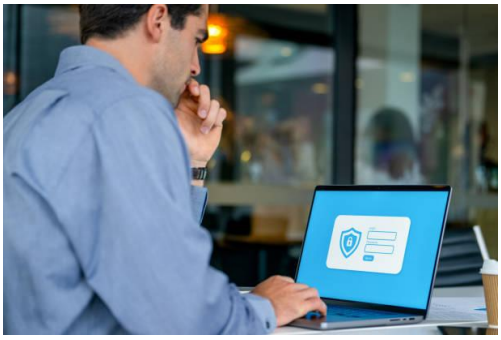
КАК РАБОТЯТ МЕНИДЖЪРИТЕ НА ПАРОЛИ?

Мениджърите на пароли не са просто една кутия за пароли, те обикновено използват сложни криптографски механизми.

Паролите се съхраняват в т.нар. „vault“ (хранилище). Шифроват се с главна парола (master password), която знае само потребителят. Повечето мениджъри я изискват при първоначално стартиране на браузъра, след което, ако искаме, може да попълват автоматично потребителят и паролата ни във всеки от сайтовете, за които тя е запаметена. - Главната парола никога не напуска нашето устройство – не се изпраща до сървъра (ако има такъв, защото има локални решения, които не са свързани -със сървър).

Всички -пароли се пазят в един шифрован файл или база данни. При локални решения като KeePass и Enpass той се съхранява е на компютъра, а при облачни решения е онлайн, синхронизиран между устройствата . Когато искаме той да бъде дефишрован, следва да въведем главната си (master) парола.

Друг позитив на мениджърите на пароли е, че всички те предлагат генерирането на сигурни пароли, като обикновено може да настроим сложността им - дължина и използване на специални символи (напр. удивителни знаци).





НАЙ-ЧЕСТО ИЗПОЛЗВАНИТЕ МЕНИДЖЪРИ НА ПАРОЛИ

Bitwarden – Най-популярното open-source облачно решение с много допълнителни функции, повечето от които са безплатни.

KeePass – Локално open-source решение.

KeePassXC – Съвременен кросплатформен клон на KeePass с подобрения

Google Password Manager – вграденият мениджър в браузърът на Гугъл – Google Chrome.

LastPass – Платено решение, един от най-старите мениджъри.

Keeper – Freemium решение, основно насочено към корпоративната сигурност.



Повечето мениджъри ни предупреждават при изтекли или слаби пароли.

Enpass – Локално решение, което може да се интегрира с Google Drive, Dropbox и др.





Министерство на електронното управление

ул. „Ген. Гурко“ № 6

Гр. София 1000

Ел. поща: bnccc@egov.government.bg

Ел. адрес: https://ncc.egov.bg/