Съфинансирано от Европейския съюз

КРАТКА ИНФОРМАЦИЯ

Проект: BG65BVPR001-1.011-0005 **„Защита от инциденти в информационната сигурност за крайните потребители в мрежите на МВР“**

Финансиране: Инструмент за финансова подкрепа за управлението на границите и визовата политика 2021–2027.

Бенефициент: Дирекция „Комуникационни и информационни системи“ (ДКИС) – МВР

Изпълнение: 12.08.2026 г. – 12.12.2029 г.

Обща стойност на проекта: 398 813.08 евро

Съфинансиране от ЕС: 299 109.81 евро

Обхват на проекта: територията на страната

Основна цел на проекта:

Повишаване нивото на информационна сигурност в Министерството на вътрешните работи (МВР) чрез изграждане на проактивна, интегрирана и ефективна защита на крайно клиентските устройства, включително в среда с виртуални работни места и защитен достъп до интернет.

Конкрета цел на проекта:

* Защита от инциденти, свързани с информационната сигурност на крайните потребители в мрежите на МВР;

* Внедряване на съвременни технологични решения, които да осигурят надеждна и цялостна защита на ИТ инфраструктурата, както и възможности за откриване и анализ на киберзаплахи чрез поведенчески подход;

* Гарантиране на сигурен и контролиран достъп до интернет през защитената инфраструктура на МВР, подпомагащ ефективната работа с информационните системи и виртуалните работни места, използвани при граничния контрол;

* Намаляване на риска от киберинциденти, включително злоупотреби, неоторизиран достъп и изтичане на данни, както и ограничаване на тяхното въздействие върху дейностите на институцията.

Дейности:

Дейност 1. Защита от инциденти в информационната сигурност на крайните потребители в мрежите на МВР.

Очаквани резултати:

* Намаляване на риска от Изтичане на информация.
* Компрометиране на операции.

* Основните резултати от изпълнението на проекта, които следва да бъдат постигнати са:

- Осигуряване на надеждна, проактивна и цялостна защита за ИТ инфраструктурата на МВР чрез внедряване на съвременни технологии за киберсигурност;
- Значително намаляване на риска от злоупотреби, пробиви в сигурността, загуба на данни и други ИТ инциденти, както и на съпътстващите ги разходи;
- Проактивно идентифициране, автоматизирано реагиране и ефективно блокиране на познати и непознати киберзаплахи в реално време;
- Оптимизация на управлението на ИТ ресурси и създаване на условия за бърза и адекватна реакция при инцидент;
- Подобрено съответствие със стандартите за сигурност, надежден контрол и осигуряване на непрекъснатост на ключовите административни процеси.

Дейност 2. Управление и изпълнение на проекта**.**

Очаквани резултати:

* Постигане на заложените резултати и индикатори, изпълнение на дейностите по проекта и успешното му завършване.
* Информация за напредъка на проекта;
* Доклади за напредъка по проекта.

Дейност 3. Видимост, прозрачност и комуникация.

Очаквани резултати:

* Рубрика в интернет страница на ДКИС;
* Изработените документи, информационни и материали със съответната визуализация.