ИНФОРМАЦИОННО ОБСЛУЖВАНЕ
Вх. №
30-00-10/17.01.2025
София

Приложение № 2
към рамков договор № ПО 16-3109/11.10.2024 г.

ЗАЯВКА по Рамков договор № ПО 16-3109 от 11.10.2024 г.		☑
ЗАЯВКА по Рамков договор № ПО 16-3109 от 11.10.2024 г. (актуализирана)		☐[1]
Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*2*
Описание на дейност/проект съгласно ПГ:	*Мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи*	
CPV код	*72220000-3*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: *(стойността следва да съответства на заложената в План-графика)* ***без ДДС****, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*	*234 000,00 лв., от които:* • *За 2025 г. – 78 000,00 лв.;* • *За 2026 г. – 78 000,00 лв.;* • *За 2027 г. – 78 000,00 лв.*	
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	***На части, както следва:*** ***<u>За 2025 г :</u>*** • *За периода от датата на подписване на заявката до 31.03.2025 г. след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи и издадена фактура на стойност 19 500 лв. без ДДС за съответния период* • *За периода от 01.04.2025 г. до 30.09.2025 г. на тримесечие след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи и издадена фактура на стойност 19 500 лв. без ДДС за съответния тримесечен период;* • *За периода от 01.10.2025 г. до 15.12.2025 г. след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето мониторинг*	

[1] *Отбелязва се в случай че заявката е актуализирана*

	*по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи и издадена фактура на стойност 19 500 лв. без ДДС.* ***<u>За 2026 г :</u>*** • *За периода от 01.01.2026 г. до 30.09.2026 г. на тримесечие след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи 19 500 лв. без ДДС за съответния тримесечен период;* • *За периода от 01.10.2026 г. до 15.12.2026 г. след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи и издадена фактура на стойност 19 500 лв. без ДДС.* ***<u>За 2027 г :</u>*** • *За периода от 01.01.2027 г. до 30.09.2027 г. на тримесечие след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето на мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи и издадена фактура на стойност 19 500 лв. без ДДС за съответния тримесечен период;* • *За периода от 01.10.2026 г. до 15.12.2026 г. след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето на мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи и издадена фактура на стойност 19 500 лв. без ДДС.*
Плащане с акредитив или авансово ДА/НЕ	*НЕ*
Документи за плащане с акредитив или авансово	*НЕ*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата****)***	*От датата на подписване на заявката до 31.12.2027 г.*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата****)***	*Неприложимо*
Отчитане: *(периодично – посочва се*	*На части, както следва:*

период, еднократно, срок за отчитане, отчетни документи)	***<u>За 2025 г.:</u>*** • *За периода от датата на подписване на заявката до 31.03.2025 г. с подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи* • *За периода 01.04.2025 г. 30.09.2025 г. с подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето на мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи и издадена фактура за съответния тримесечен период;* • *За периода от 01.10.2025 г. - 15.12.2025 г. с подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето на мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи. Дейностите за периода от 16.12.2025г. до 31.12.2025 г. се отчитат заедно със следващия тримесечен период през 2026 г, като за тях не се дължи заплащане.* ***<u>За 2026 г.:</u>*** • *За периода 01.01.2026 г. 30.09.2026 г. с подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето на мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи за съответния тримесечен период;* • *За периода от 01.10.2026 г. - 15.12.2026 г. с подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето на мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи.*

	Дейностите за периода от 16.12.2026 г. до 31.12.2026 г. се отчитат заедно със следващия тримесечен период през 2027 г, като за тях не се дължи заплащане. ***<u>За 2027 г.:</u>*** • *За периода 01.01.2027 г. 30.09.2027 г. с подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето на мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи за съответния тримесечен период;* • *За периода от 01.10.2027 г. - 15.12.2027 г. с подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ предоставянето на мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи. Дейностите за периода от 16.12.2027 г. до 31.12.2027 г. се отчитат с подписването на приемо-предавателен протокол до 10.01.2028 г, като за тях не се дължи заплащане.*
Приложения: *(напр: технически параметри, образци на отчетни документи)*	*Технически параметри*
Настоящата заявка да се изпълни при условията на приложените Технически параметри.	
ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:	
Координатор по заявката:	
Ръководител на проект/дейност по заявката *(напр: представител на дирекцията – Заявител):*	

ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:		
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Координатор от „Информационно обслужване“ АД по заявката		
Ръководител на проект/дейност по заявката		
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните - Регламент (ЕС) 2016/679

ТЕХНИЧЕСКИ ПАРАМЕТРИ

за

“Мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи ресурси за нуждите на Сметната палата на Република България“

София, 2025 г.

ТЕХНИЧЕСКИ ПАРАМЕТРИ
ЗА
ПРЕДОСТАВЯНЕ НА УСЛУГА ЗА МОНИТОРИНГ ПО СИГУРНОСТТА, НАБЛЮДЕНИЕ И ДОКЛАДВАНЕ НА КИБЕР-ИНЦИДЕНТИ В РЕЖИМ 24*7

1. Описание

1.1. Настоящите технически параметри представят описание на услуга за мониторинг по сигурността, наблюдение и докладване на кибер-инциденти в режим 24*7 за нуждите на Сметна палата на Република България (Сметна Палата). Услугата следва да осигури автоматично откриване на събития, които могат да повлияят на мрежовата и информационната сигурност на важните за дейността на Сметната палата информационни и комуникационни системи.

1.2. Чрез осигуряването на услугата ще се постигне:

1.2.1. Изпълнение на изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС).

1.2.2. Непрекъснато наблюдение на критичната информационна инфраструктура на Сметната палата.

1.3. Предприемане на своевременни мерки за намаляване на риска от заплахи чрез анализ на мрежовия трафик, логовете на критични ИТ активи - мрежови устройства, операционни системи, бази данни, приложен софтуер и др.

1.3.1. Своевременно подобряване на политики и правила, свързани с информационната сигурност в Сметната палата чрез предоставяното от Услугата интегрирано управление на данните от различни ИТ източници.

1.3.2. Своевременно идентифициране на подходящи мерки за актуализиране на специализирания приложен софтуер, използван от Сметната палата, с цел минимизиране на потенциални заплахи.

2. Съществуващо положение

2.1. В резултат на изпълнение на договор ПО-16-923/29.01.2024 *Предоставяне на услуги за мониторинг по сигурността, наблюдение и докладване на кибер-инциденти в режим 24*7 на информационните системи на Сметната палата на Република България*, сключен между Сметна палата на Република България и „Информационно обслужване“ АД (ИО АД) и в съответствие с изискванията на НМИМИС, на Сметната палата са предоставени и конфигурирани съвременни софтуерни средства IBM QRadar SIEM с вградени и настроени автоматични алгоритми за управление на сигурността на информацията и събитията, наричани за краткост „Системата“.

2.2. В инфраструктурата на Сметната палата е създадена виртуална машина (за Log Collector), с капацитет (1 000 eps (event per second), извършени са необходимите мрежови конфигурации, в инфраструктурата на Сметната палата са инсталирани Event Collector, които са интегрирани с аналогичните компоненти IBM QRadar SIEM системата в ИО АД с оглед непрекъснат мониторинг на събития и даване на своевременни препоръки за действия на ИТ екипа на Сметната палата в случай на идентифицирани заплахи.

2.3. Към Системата са присъединени източници на журнални (log) записи като: Microsoft Windows (домейн контролери, файлов сървър и др.); защитни стени; антивирусен софтуер и др.

3. Изисквания към мрежовата и информационната сигурност

3.1. Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове към тях.

4. Място на изпълнение

Предоставянето на услугата се извършва за управляваните от дирекция „Сигурност“ на Сметна палата ИТ активи, разположени в локация София 1000, ул. "Екзарх Йосиф" 37.

5. Изисквания към предоставянето на Услугата

5.1. За изпълнението на Услугата Изпълнителят следва да осигури компетентен и аналитичен екип, като се осигури 24/7 автоматизирано наблюдение.

5.2. Услугата следва да осигури постоянен мониторинг на ИТ дейности, комуникационна и информационна инфраструктура, ИТ услуги и взаимодействия с външни фактори в съответствие с изискванията на НМИМИС като се:

5.2.1. Осигури наблюдение на крайните работни точки, присъединяване на други журнални файлове (log) към Системата, както и присъединяване на нови системи до достигане на предоставената от Системата възможност (1 000 eps (event per second), непрекъснат мониторинг и анализ, с оглед предприемане на ответни мерки в случай на инцидент. ИО АД следва да изпраща информация по e-mail за аларми, по които е нужна допълнителна проверка от системен администратор на Сметна палата до 4 часа след тяхното настъпване. При установяване на неуспешна атака или фалшиво-позитивна аларма, e-mail към Сметна палата не е необходимо да се изпраща. Сметната палата носи изцяло отговорност за управлението и диагностиката на аларми и инциденти с вектор на атака: електронна поща. При нужда от асистенция, екипът на ИО АД ще съдейства за отстраняването на заплахите и възстановяване на работоспособността на системите и услугите.

5.2.2. Извърши анализ на наличните уязвимости във вътрешната ИТ инфраструктура и предоставят препоръки и проследяване на изпълнението им, както и оказване на методическа помощ на дирекция „Сигурност“ при идентифициране на потенциални заплахи и набелязване на мерки в краткосрочен план.

5.2.3. Извърши анализ на базата на събраната информация поне за шестмесечен период и се предложат решения за извършване на промени в ИТ инфраструктурата в дългосрочен план.

5.2.4. Провеждат срещи със служители на дирекция „Сигурност“, на които се дискутират, анализират и планират действия и мерки срещу актуалните заплахи към ИТ инфраструктурата, както и се оценява ефективността на предприетите мерки, чрез повторен анализ и оценка на действията по отстраняване на заплахи за всеки отчетен период.

5.2.5. При поискване от страна на дирекция „Сигурност“ преглеждат, коригират и допълват изискванията за сигурност, включени в технически параметри или технически спецификации в областта на информационните и комуникационните системи.

5.3. Услугата следва да предостави и дейности по непрекъснато подобрение на сигурността чрез:

5.3.1. Мониторинг за наличността на ключови услуги и своевременно информиране на дирекция „Сигурност“ при наличие на атаки до 1 час от установяването им;

5.3.2. Установяване на кореновата причина за наличието на инцидент, извършване на корелационен анализ и препоръки за отстраняване;

5.3.3. Идентифициране на засегнатите от заплахите услуги/активи и даване на препоръки за действия от страна на дирекция „Сигурност“.

5.3.4. Управление на инциденти свързани със сигурността.

5.3.5. Извършване на последващ контрол, координирано с дирекция „Сигурност“ за отстранени инциденти.

5.3.6. Даване на препоръки за подходящи съвременни решения на дирекция „Сигурност“ за справяне с безфайлови (извършващи се в паметта) атаки - инжектиране на код, например чрез PowerShell и др. при необходимост;

5.3.7. Ежемесечна автоматизирана проверка за наличие на уязвимости в публично видимите услуги на клиента и вътрешна мрежа за управление.

5.3.8. Процес по отстраняване и проследяване на уязвимости.

6. Отчитане

6.1. Приемането на предоставената услуга се документира с приемо-предавателен протокол по чл. 6 от договора за всеки тримесечен период. Към него се предават и генерираните от Системата:

(1) Приложение № 1 - Доклад за открити уязвимости във вътрешната мрежа за управление на Сметната палата за всеки месец;

(2) Приложение № 2 - Доклад за открити уязвимости в публичните мрежи на Сметната палата, в който влизат публични услуги на Сметната палата за всеки месец;

(3) Приложение № 3 - Детайли за всички генерирани аларми и предприети действия за всеки месец;

(4) Други доклади или извадки, генерирани от Системата в случай на приложимост.

Приложенията, описани по-горе се предават на споделено пространство, до което се осигурява достъп на ръководителя на проект по заявката от страна на Възложителя.