

ПОКАНА ЗА УЧАСТИЕ В ПАЗАРНИ КОНСУЛТАЦИИ

На основание чл. 44 от Закона за обществените поръчки (ЗОП) „Булгартрансгаз“ ЕАД, провежда пазарни консултации с цел определяне на прогнозната стойност на доставките и дейностите, включени в предмета на обществена поръчка с наименование „Доставка, инсталиране и пускане в експлоатация на платформи и оборудване за информационна и киберсигурност“, съгласно чл. 21, ал. 2 от ЗОП.

УВАЖАЕМИ ДАМИ И ГОСПОДА,

„Булгартрансгаз“ ЕАД планира да проведе и възложи обществена поръчка с горепосоченото наименование и в тази връзка и в съответствие с разпоредбата на чл. 21, ал. 2 от ЗОП за определяне на прогнозната стойност на поръчката, „Булгартрансгаз“ ЕАД провежда по реда на чл. 44 от ЗОП настоящите пазарни консултации.

Във връзка с гореизложеното каним всички лица – независими експерти или органи, както и участници на пазара, които имат интерес, да представят оферта с предложени индикативни стойности за доставките и дейностите, свързани с изпълнение на предмета на поръчката, съгласно приложената към настоящата покана Техническа спецификация – Приложение № 1.

Всички предложени цени следва да бъдат посочени в евро, без ДДС, и да включват всички разходи, необходими за изпълнение на посочените в Приложение № 1 доставки дейности от предмета на поръчката.

Уведомявам Ви, че представените от Вас индикативни стойности не са обвързващи в случай на участие в процедурата за възлагане на обществената поръчка, като те имат единствено за цел да бъде извършено проучване на реалните пазарни цени, които да бъдат сравнени и анализирани за да бъде определена прогнозната стойност на обществената поръчка.

Цялата информация, разменена по повод пазарните консултации включително получените от възложителя предложени стойности, представени в резултат от пазарната консултация, ще бъдат публикувани в профила на купувача в ЦАИС ЕОП, както и в раздел „Профил на купувача“ на електронната страница на „Булгартрансгаз“ ЕАД.

Индикативните оферти с предложените стойности за изпълнение на доставките и дейностите предмет на обществената поръчка, следва да бъдат предоставени в срок до 23:59 ч. на 30.03.2026 г. на следния електронен адрес: stanislava.manolova@bulgartransgaz.bg, съгласно приложения образец - Приложение № 2.

Приложения:

1. Техническа спецификация, съдържаща описание на доставките и дейностите от предмета на поръчката, които следва да бъдат извършени – Приложение № 1.
2. Индикативна оферта Образец № 1 и Приложение към нея Образец № 1.1. за участие в пазарни консултации – Приложение № 2.

С уважение, Заличено по чл. 37 от ЗОП

НАДЯ СТОЙКОВА

и.д. Главен експерт - административно ръководство, директор дирекция „Обществени поръчки“ и пълномощник на изпълнителния директор на „Булгартрансгаз“ ЕАД, съгласно пълномощно с № БТГ 92-01-188 от 14.08.2025 г.

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

Наименование на поръчката:	„Доставка, инсталиране и пускане в експлоатация на платформи и оборудване за информационна и киберсигурност“
-----------------------------------	--

РАЗДЕЛ I: СЪЩЕСТВУВАЩО ПОЛОЖЕНИЕ

„Булгартрансгаз“ ЕАД е комбиниран оператор с предмет на дейност пренос и съхранение на природен газ и поддържане, експлоатация, управление и развитие на подземно газово хранилище. Обособени са Централно Управление в гр. София и регионални звена: Северозападен Експлоатационен Район „Ботевград“, Североизточен Експлоатационен Район „Вълчи Дол“, Югоизточен Експлоатационен Район „Стара Загора“, Югозападен Експлоатационен Район „Ихтиман“ и Подземно Газохранилище (ПГХ) „Чирен“.

В информационната инфраструктура на „Булгартрансгаз“ ЕАД са интегрирани системи и продукти на утвърдени производители, чрез които се постига високо ниво на защита на информационните активи.

РАЗДЕЛ II: ЦЕЛ, ПРЕДМЕТ, МЯСТО И СРОК НА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

1. ЦЕЛ НА ПОРЪЧКАТА

Целта на поръчката е да се доставят и имплементират съвременни хардуерни устройства и оборудване и софтуерни платформи, пакети и лицензи в сферата на киберсигурността за да се постигне високо ниво на устойчивост срещу злонамерени действия върху информационната инфраструктура.

Всички хардуерни устройства, софтуерни пакети и лицензи по т.т. 2.1., 2.2., 2.3., 2.4. и 2.5. следва да бъдат доставени за период на използване и обновяване от 5 години.

2. ПРЕДМЕТ НА ПОРЪЧКАТА

Предметът на поръчката е доставка и инсталиране в информационната система на „Булгартрансгаз“ ЕАД на съвременни хардуерни устройства и оборудване и софтуерни платформи, софтуерни пакети и лицензи за ползване, включващ следните основни дейности:

2.1. СИСТЕМА ЗА АНАЛИЗ И ОТКРИВАНЕ НА ЗАПЛАХИ НА БАЗА DNS ТРАФИК:

- 2.1.1. Доставка на системата окомплектована с необходимите софтуерни пакети и лицензи;
- 2.1.2. Инсталиране и активиране на системата.
- 2.1.3. Гаранционна поддръжка на системата.

2.2. РЕШЕНИЕ ЗА СКАНИРАНЕ НА УЯЗВИМОСТИ:

- 2.2.1. Доставка на решението окомплектовано с необходимите софтуерни пакети и лицензи;
- 2.2.2. Инсталиране и активиране на решението.
- 2.2.3. Гаранционна поддръжка на решението.

2.3. РЕШЕНИЕ ЗА МОНИТОРИРАНЕ И УПРАВЛЕНИЕ НА ПРИВИЛЕГИРОВАННИЯ ДОСТЪП (РАМ):

- 2.3.1. Доставка на решението окомплектовано с необходимите софтуерни пакети и лицензи;

- 2.3.2. Инсталиране и активиране на решението.
- 2.3.3. Гаранционна поддръжка на решението.
- 2.4. ПЛАТФОРМА ЗА ЦЕНТРАЛИЗИРАНО АВТЕНТИКИРАНЕ:**
 - 2.4.1. Доставка на платформата окомплектована с необходимите софтуерни пакети и лицензи;
 - 2.4.2. Инсталиране и активиране на платформата.
 - 2.4.3. Гаранционна поддръжка на платформата.
- 2.5. НАДГРАЖДАНЕ НА ЦЯЛОСТНА СИСТЕМА ОТ ЗАЩИТНИ СТЕНИ:**
 - 2.5.1. Доставка на допълнителни хардуерни устройства и лицензни абонаменти за използване на софтуерни функции на системата.
 - 2.5.2. Тестване на хардуерните устройства и активиране на лицензните абонаменти за използване на софтуерни функции.
 - 2.5.3. Осигуряване на валидна хардуерна и софтуерна поддръжка на надградената система от защитни стени, включваща доставените и наличните устройства.
- 2.6. Сървъри ТИП1**
- 2.7. ТИП1**
 - 2.7.1. Доставка на сървъри, окомплектовани с необходимите стойки и крепежи за монтаж в 19" сървърен шкаф;
 - 2.7.2. Гаранционно сервизно обслужване
- 2.8. Сървъри ТИП2**
 - 2.8.1. Доставка на сървъри, окомплектовани с необходимите стойки и крепежи за монтаж в 19" сървърен шкаф;
 - 2.8.2. Гаранционно сервизно обслужване
- 2.9. KVM комутатори**
 - 2.9.1. Доставка на KVM комутатори, окомплектовани с необходимите стойки и крепежи за монтаж в 19" сървърен шкаф;
 - 2.9.2. Гаранционно сервизно обслужване
- 2.10. Настолни компютри**
 - 2.10.1. Доставка на компютри, окомплектовани с необходимите кабели, клавиатури и мишки;
 - 2.10.2. Доставка на дисплеи, окомплектовани с необходимите кабели за връзка с компютрите;
 - 2.10.3. Инсталиране и активиране на съответните лицензии
 - 2.10.4. Гаранционно сервизно обслужване
- 2.11. Дисплеи**
 - 2.11.1. Доставка на дисплеи, окомплектовани с необходимите кабели за връзка с компютър;
 - 2.11.2. Гаранционно сервизно обслужване
- 2.12. Преносими компютри ТИП1**
 - 2.12.1. Доставка на преносими компютри, окомплектовани с необходимите кабели, мишки и раници;
 - 2.12.2. Инсталиране и активиране на съответните лицензии
 - 2.12.3. Гаранционно сервизно обслужване
- 2.13. Преносими компютри ТИП2**
 - 2.13.1. Доставка на преносими компютри, окомплектовани с необходимите кабели, мишки и раници;
 - 2.13.2. Инсталиране и активиране на съответните лицензии
 - 2.13.3. Гаранционно сервизно обслужване
- 2.14. LAN Комутатори**

- 2.14.1. Доставка на LAN комутатори, окомплектовани с необходимите кабели и стоки за монтаж в 19" шкаф;
- 2.14.2. Гаранционно сервизно обслужване
- 2.15. Непрекъсваеми токозахранващи устройства (UPS)**
- 2.15.1. Доставка на UPS, окомплектовани с необходимите кабели за захранване и комуникация;
- 2.15.2. Гаранционно сервизно обслужване

3. МЯСТО НА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

Мястото на изпълнение на поръчката е Централно управление на „Булгартрансгаз“ ЕАД – гр. София п.к. 1336, район „Люлин“, жк. Люлин 2, бул. Панчо Владигеров № 66.

РАЗДЕЛ III: ТЕХНИЧЕСКИ ИЗИСКВАНИЯ

Изпълнителят трябва да достави следните софтуерни платформи, пакети, лицензи и хардуерни устройства и оборудване:

Позиция	Наименование	Количество
1	СИСТЕМА ЗА АНАЛИЗ И ОТКРИВАНЕ НА ЗАПЛАХИ НА БАЗА DNS ТРАФИК	1 бр.
2	РЕШЕНИЕ ЗА СКАНИРАНЕ НА УЯЗВИМОСТИ	1 бр.
3	РЕШЕНИЕ ЗА МОНИТОРИРАНЕ И УПРАВЛЕНИЕ НА ПРИВИЛЕГИРОВАННИЯ ДОСТЪП (РАМ)	1 бр.
4	ПЛАТФОРМА ЗА ЦЕНТРАЛИЗИРАНО АВТЕНТИКИРАНЕ	1 бр.
5	НАДГРАЖДАНЕ НА ЦЯЛОСТНА СИСТЕМА ОТ ЗАЩИТНИ СТЕНИ	1 бр.
6	СЪРВЪРИ ТИП1	4 бр.
7	СЪРВЪРИ ТИП2	24 бр.
8	КVM КОМУТАТОРИ	18 бр.
9	НАСТОЛНИ КОМПЮТРИ	100 бр.
10	ДИСПЛЕИ	100 бр.
11	ПРЕНΟΣИМИ КОМПЮТРИ ТИП1	20 бр.
12	ПРЕНΟΣИМИ КОМПЮТРИ ТИП2	20 бр.
13	LAN КОМУТАТОРИ	60 бр.
14	НЕПРЕКЪСВАЕМИ ТОКОЗАХРАНВАЩИ УСТРОЙСТВА (UPS)	26 бр.

1. СИСТЕМА ЗА АНАЛИЗ И ОТКРИВАНЕ НА ЗАПЛАХИ НА БАЗА DNS ТРАФИК

Обща информация	
T.1.1	Количество – 1 брой.
Спецификация – минимални изисквания	
T.1.2	DDI Системата (DNS, DHCP & IP Address Management) трябва да бъде доставена като готов за използване OVA образ с възможност за интегриране във VMware среда, която Възложителят вече притежава.
T.1.3	Системата трябва да е лицензирана за минимум 850 потребителя.
T.1.4	DDI Системата трябва да е оразмерена и лицензирана за безпроблемна работа на поне 3000 IP адреса.
T.1.5	Системата трябва да предоставя услуга за управление на IP адреси – IPAM (IP Address Management)

T.1.6	Системата трябва да разполага с механизми за контрол на въвежданите данни (коректност на IP адреси, маски и др.)
T.1.7	Системата трябва да позволява добавяне на описания и атрибути за мрежови обекти, IP адреси, домейни. Тези атрибути трябва да имат възможност за дефиниране на типа и размера им
T.1.8	Системата трябва да поддържа механизъм за сканиране на мрежи и хостове/IP адреси (т.нар. network discovery)
T.1.9	Системата трябва да поддържа функции като „намери 10 неизползвани адреса от мрежа X“ и „намери 10 неизползвани подмрежи с размер напр. /24 в подмрежа напр. abcd/16“. Функцията трябва да бъде налична за IPv4 и IPv6
T.1.10	Системата трябва да позволява импортиране на данни в CSV формат директно от графичния интерфейс и да разполага с подробна документация за формата на импортираните данни
T.1.11	Капацитетът на DNS/DHCP/IP базата данни трябва да бъде за минимум 100000 записа.
T.1.12	Системата трябва да позволява интеграция с VMware vCenter и OpenStack услуги, за да извършва процес на откриване на виртуални машини, работещи във VMware/OpenStack инфраструктура, и автоматично да създава DNS записи за тези машини
T.1.13	Системата трябва да поддържа внедряване на DHCP услуги за IPv4 и IPv6 с минимална производителност от 200 DHCP leases в секунда
T.1.14	Системата трябва да поддържа актуализиране на DDNS данни чрез DHCP услугата
T.1.15	Системата трябва да поддържа актуална информация за разпределените IP адреси и устройствата, на които е присвоен даден адрес (MAC адрес, време и дата на присвояване на адреса, IP)
T.1.16	Системата трябва да поддържа функционалност DHCP Failover с възможност за повторно договаряне на наличните адресни пространства
T.1.17	Трябва да бъде възможно проверката за наличност на IP адрес преди неговото разпределяне чрез ICMP
T.1.18	Системата трябва да разпознава типа на устройството/системата на станции, мобилни устройства и др. въз основа на анализа на DHCP заявката. Трябва да поддържа отчет за типа на устройството в историята на DHCP наемите и да предоставя възможност за филтриране/блокиране на разпределението на адреси за избрани типове устройства (напр. разпределяне на адрес за Windows станция, но не и за таблет или смартфон)
T.1.19	Системата трябва да предоставя авторитетни и рекурсивни услуги за разрешаване на домейн имена (DNS - Domain Name System)
T.1.20	Производителността на авторитетния DNS трябва да бъде поне 10 000 DNS заявки в секунда
T.1.21	Системата трябва да изпълнява автоматични DNS актуализации в съответствие с RFC 2136
T.1.22	Системата трябва да разполага с вграден механизъм за уведомяване при промени в зоните, в съответствие с RFC 1996
T.1.23	Системата трябва да поддържа DNS протоколи както за IPv4, така и за IPv6
T.1.24	Системата трябва да поддържа DNS Anycast услуга за IPv4 и IPv6 (използвайки BGP и OSPF протоколи)
T.1.25	Системата трябва да поддържа DNSSEC услуга с автоматично обновяване на

	подписите при промени в DNS зоните
T.1.26	Системата трябва да поддържа DDNS услуга
T.1.27	Системата трябва да поддържа защитено обновяване на DNS записи с поддръжка на GSS-TSIG протокол
T.1.28	Системата трябва да поддържа MultiMaster DNS функционалност
T.1.29	Системата трябва да поддържа механизъм за IDN (Internationalized Domain Names) и да разполага с вграден конвертор за punycode (поддръжка на кирилица)
T.1.30	Системата трябва да поддържа IDN за DNSKEY записи, DS записи, NSEC записи, NSEC3PARAM записи и RRSIG записи
T.1.31	Системата трябва да поддържа EDNS0 разширения съгласно стандарта RFC 6891
T.1.32	Системата трябва да поддържа следните алгоритми за публични ключове, използвани с DNSSEC: DSA, RSA/MD5, RSA/SHA1, RSA/SHA-256, RSA/SHA-512, ECDSAP/SHA-256, ECDSAP/SHA-384
T.1.33	Подписаните с DNSSEC зони трябва да поддържат динамични DNS актуализации
T.1.34	Системата трябва да поддържа автоматично подписване на DNS записи след промени
T.1.35	Системата трябва да функционира като платформа за разпространение на файлове чрез протоколите TFTP, FTP, HTTP и да предлага услуги за синхронизация на времето чрез NTP (Network Time Protocol)
T.1.36	Системата трябва да работи под контрола на специализирана операционна система. Използването на операционни системи с общо предназначение не е разрешено. Тя не трябва да зависи от или да изисква конкретни версии на операционни системи с общо предназначение или програмни библиотеки
T.1.37	Управлението на системата трябва да се осъществява чрез уеб браузър, без да е необходимо инсталирането на допълнителен софтуер като агент, клиент и др.
T.1.38	Системата трябва да предоставя възможност за управление от няколко системни администратори, вписани едновременно
T.1.39	Системата трябва да предоставя възможност за управление на IPv4 и IPv6 адреси, позволявайки графичен, конзолен и API интерфейси
T.1.40	Системата трябва да поддържа удостоверяване на потребители чрез: <ul style="list-style-type: none"> - Локална потребителска база - RADIUS протокол - TACACS+ протокол - LDAP - Microsoft Active Directory
T.1.41	Системата трябва да има вградена база данни за съхранение на DDI информация. Базата данни не трябва да изисква поддръжка, свързана с нейната конфигурация и управление
T.1.42	Системата трябва да може да бъде наблюдавана чрез SNMP (Simple Network Management Protocol)
T.1.43	Системата трябва да позволява планирани резервни копия (backups) към външен сървър, за да улесни възстановяването в случай на бедствие (минимум чрез един от следните протоколи TFTP, FTP или SCP)
T.1.44	Системата трябва да поддържа интеграция с всеки един от следните

	инструменти за управление на конфигурацията Ansible, Puppet и Chef
T.1.45	Системата трябва да поддържа възможност за импортиране и експортиране на данни в различни формати, включително CSV и JSON
T.1.46	Системата трябва да разполага с функционалност за разпознаване и блокиране на DNS тунелиране чрез аналитичен механизъм, базиран на машинно обучение, който разпознава неизвестни модели на тунелиране и извличане на данни чрез DNS. Системата трябва да анализира поне 10 атрибута на всяка DNS заявка, включително: ентропия на символите във FQDN, популярност на дву- и трибуквени комбинации, съотношение на гласни в FQDN, съотношение на цифри, размер на заявката, честота и промяна на честотата на DNS заявките
T.1.47	Системата трябва да разполага с функционалност за откриване на прониквания през DNS, по-специално трябва да разпознава техниката, използвана от зловредния софтуер Powersource/DNS Messenger, и да блокира опити за пренос на данни, кодирани в DNS отговори чрез TXT записи
T.1.48	Системата трябва да разполага с функционалност Response Policy Zones (RPZ) за работа като DNS защитна стена въз основа на списъци с опасни домейни
T.1.49	Системата трябва да регистрира и предоставя информация за всички промени, направени от администратори (кой, кога, какво е променил)
T.1.50	Системата трябва да може да изпраща логове към централен хранилищен сървър чрез Syslog механизъм (TCP и UDP)
T.1.51	Системата трябва да позволява администраторите да имат права, базирани на групи и роли, които ограничават достъпа им само до необходимите ресурси. Подробните разрешения трябва да позволяват конфигуриране на права за отделни обекти, като мрежи, DNS зони и конкретни DNS записи.
T.1.52	Системата трябва да поддържа криптирана комуникация между компонентите си чрез TLS (Transport Layer Security)
T.1.53	Достъпът до административния интерфейс трябва да бъде защитен чрез двуфакторна автентикация (2FA)
T.1.54	Системата трябва да предоставя механизъм за защита срещу неоторизиран достъп чрез прилагане на списъци за контрол на достъпа (ACL)
T.1.55	Системата трябва да поддържа защита от атаки тип DDoS срещу DNS и DHCP услуги
T.1.56	Системата трябва да поддържа механизъм за мониторинг и алармиране при откриване на аномалии в мрежовия трафик, свързан с конфигурираните услуги
T.1.57	Системата трябва да има възможност за запис и анализ на потребителските сесии в административния интерфейс за целите на одит и сигурност
T.1.58	Системата трябва да поддържа криптиране на чувствителни данни в конфигурационните файлове и базата данни
T.1.59	Системата трябва да позволява дефиниране на политики за автоматично деактивиране на потребителски акаунти при откриване на подозрителна активност
T.1.60	Системата трябва да има възможност да предприема действия по DNS заявки и отговори въз основа на дефинирани от клиента правила за защита. Възможните действия трябва да включват: разрешаване на заявка без регистриране, разрешаване на заявка с логиране, блокиране на заявка с NXDomain отговор (няма такъв домейн), пренасочване (отговор с дефиниран



	<p>IP адрес). Пренасочването трябва да е възможно към уеб страница, предоставена от доставчика. Системата трябва също така да позволява пренасочване към всеки IP адрес.</p> <ul style="list-style-type: none"> - Системата трябва да предприеме действия въз основа на името на домейна в заявката и въз основа на IP адреса в отговора. Действието върху името на домейн трябва да работи за всеки тип заявка – системата не трябва да позволява заобикаляне на блокирането чрез изпращане на специфични типове заявки като SOA или NS. Системата не трябва да позволява заобикаляне на блокирането на злонамерен домейн чрез изпращане на запитвания с главни или смесени FQDN (DNS протоколът е нечувствителен към малки и големи букви, а сигурната DNS система също трябва да е нечувствителна към малки и големи букви) - Системата трябва да позволява да се дефинира персонализиран списък с домейни/IP адреси, по които да се действа, и също така трябва да предоставя списък с домейни и IP адреси под формата на емисии за заплахи, дефинирани по-долу. За персонализирани списъци системата трябва да има възможност да дефинира нивото на заплаха и увереността на заплахата за всеки списък. - Системата трябва да позволява създаване и редактиране на персонализирани списъци от клиентския портал, както и чрез API, за да позволи лесно импортиране на персонализирани данни за заплахи. - Системата трябва да предоставя възможност за заобикаляне на блокове със специфични кодове, предоставени на избрани потребители
<p>T.1.61</p>	<p>Системата да има възможност за изпращането на DNS заявки към услуга предоставяща функции за категоризирането и филтрирането им</p> <ul style="list-style-type: none"> - от персонализирано дефинирана IP мрежа - от DMZ DNS сървъри - сървърите трябва да добавят вътрешен IP адрес на клиента вътре в заявките и да ги изпращат в криптирана форма към системата за проверка - от роуминг агент, предоставен от доставчика. Роуминг агентът трябва да бъде предоставен за Windows, Mac OS, Android и iOS <p>Данните за заплахите, предоставени от доставчика, трябва да включват:</p> <ul style="list-style-type: none"> - списък на интернет домейни, свързани с APT атаки - списък с домейни и IP адреси, свързани със злонамерен софтуер - списък с домейни, свързани с рансъмуер - списък с IP адреси, свързани с ботнет мрежи - списък на домейните, свързани със злонамерен софтуер, с помощта на алгоритми за генериране на домейни (DGA) - списък с IP адреси на изходните възли на TOR мрежата - списък с домейни, свързани с фишинг - списък на домейните, свързани с неоторизирано копаене на криптовалута - списък на домейните, регистрирани през последните три дни. Данните за новите регистрации трябва да идват от най-малко 500 различни домейна от първо ниво (домейни от първо ниво). - списък на домейни, които споделят подозрителни характеристики като примерни домейни са регистрирани по едно и също време от същия регистрант, който в миналото е регистрирал домейни, за които е доказано, че са свързани със злонамерена дейност
<p>T.1.62</p>	<p>Всички горепосочени списъци по T.1.61 за заплахи трябва да бъдат налични</p>

	за конфигуриране в политиката за защитени DNS услуги, както и във формат RPZ, за да бъдат изтеглени на DNS сървърите
T.1.63	Списъците по T.1.61 за заплахи от доставчика трябва да бъдат достъпни чрез API във формати CSV, STIX, XML, JSON и CEF за използване в други системи за сигурност като SIEM, защитни стени или защитени уеб шлюзове
T.1.64	Разузнаването на заплахите трябва да може да предоставя контекстуална информация за домейн/IP, поне трябва да включва данни, ако заплахата е свързана с експлорация на данни, влияе ли върху наличността на системите, необходимо ли е взаимодействие с потребителя за активиране на заплахата, какви техники са включени
T.1.65	Защитената DNS услуга трябва да има функционалността за откриване и блокиране на DNS тунелиране с помощта на аналитичен алгоритъм, базиран на машинно обучение и позволяващ откриване на неизвестни модели на тунелиране и експлорация на данни през DNS. Системата трябва да анализира поне 10 атрибута на всяка DNS заявка и това трябва да включва: ентропия на знаците в FQDN, оценяване на всеки набор от 2 и 3 знака за популярност в естествените езици, изчисляване на съотношението на гласните в FQDN, изчисляване на съотношението на цифрите в FQDN, анализиране на размера на заявката, анализиране на честотата на DNS заявките (стойност на честотата и промяна на честотата). Защитената DNS услуга трябва да открива DNS тунелиране, независимо от категорията на съдържанието на домейна, използван в DNS заявката
T.1.66	Защитената DNS услуга трябва да има функционалност за откриване на непознати DGA и DGA домейни в DNS заявки
T.1.67	Защитената DNS услуга трябва да има информация за категорията съдържание за домейни и трябва да може да действа по нея, например трябва да предоставя възможност за предприемане на действия за домейни, хостващи съдържание като порно, опасност, социални мрежи, анонимайзери и др.
T.1.68	Системата трябва да поддържа механизми за висока наличност (High Availability - HA) за всички основни услуги, включително DNS, DHCP и IPAM
T.1.69	Системата трябва да поддържа клъстеризация на компонентите си с цел осигуряване на надеждност и отказоустойчивост
T.1.70	Системата трябва да позволява автоматично превключване (failover) при отпадане на даден сървър или услуга
T.1.71	Системата трябва да поддържа географски разпределено внедряване с възможност за репликация на данни между различни локации
T.1.72	Системата трябва да има механизъм за автоматично балансиране на натоварването (load balancing) между DNS и DHCP сървърите
T.1.73	Системата трябва да осигурява непрекъсната работа при актуализации (Rolling Updates), без да се нарушава функционирането на критичните услуги
T.1.74	Системата трябва да позволява възстановяване след срив (Disaster Recovery) чрез механизъм за архивиране и репликация на данни
T.1.75	Системата трябва да поддържа синхронизация на конфигурацията и данните между главните и резервните инстанции в реално време
T.1.76	Системата да поддържа възстановяване на услугите в случай на срив, като времето за възстановяване не трябва да надвишава 10 минути.
T.1.77	Системата трябва да предоставя централизирана отчетност за всички DNS,

	DHCP и IPAM събития Системата трябва да поддържа механизъм за събиране и анализ на логове, включително възможност за интеграция с SIEM (Security Information and Event Management) решения
T.1.78	Системата трябва да поддържа механизъм за събиране и анализ на логове, включително възможност за интеграция с SIEM (Security Information and Event Management) решения
T.1.79	Системата трябва да позволява генериране на персонализирани отчети за използването на IP адреси, DHCP лизинги и DNS заявки
T.1.80	Системата трябва да осигурява механизъм за известяване на администраторите чрез имейл, SNMP трап (trap) или уеб интерфейс при откриване на критични събития
T.1.81	Системата трябва да предоставя детайлни статистики за производителността на DNS и DHCP услугите, включително натоварване, време за отговор и брой заявки
T.1.82	Системата трябва да позволява интеграция със системи за мрежов мониторинг чрез SNMP (v2c и v3)
T.1.83	Системата трябва да предоставя исторически данни за заетостта на IP адресите и тенденциите на използване
T.1.84	Системата трябва да поддържа механизъм за автоматично архивиране на логове и отчети за последващ анализ
T.1.85	Системата трябва да позволява конфигуриране на политики за съхранение и изтриване на исторически данни
T.1.86	Системата трябва да може да визуализира информацията чрез графики и диаграми в уеб интерфейса
T.1.87	Включените в системата защитени DNS услуги трябва да предоставя възможности за отчитане. Докладите трябва да включват: <ul style="list-style-type: none"> - Отчети за дейността, показващи DNS заявки, изпратени до услугата - Отчети за защитата, показващи DNS заявки, които засягат правилата за сигурност - Системата трябва да има възможност за изпращане на изходни данни (заявки, събития за защита) до локална SIEM система под формата на съобщения в системен дневник или директна интеграция
T.1.88	Достъпът до клиентския портал на системата трябва да се основава на потребителски данни за вход със специфични роли за достъп, като например достъп само за четене или административен достъп. Промените в конфигурацията на DNS услугата трябва да бъдат регистрирани в регистрационния файл за проверка.
T.1.89	Висока производителност с минимално време за отговор на DNS заявки (не по-високо от 50 милисекунди) при натоварване до 5 хиляди заявки на секунда.
T.1.90	Поддръжка на DHCP услуги с производителност минимум 200 заявки на секунда.
T.1.91	Надеждност при обработка на големи обеми данни и да не претоварва мрежовата инфраструктура при високи натоварвания.
T.1.92	Възможност за работа с разширени DNS записи и поддръжка функционалности като DNSSEC и Anycast без да се нарушава производителността.
T.1.93	Възможност за обработка на натоварвания, които включват обработка на над 30 милиона DNS заявки и DHCP лизинги месечно.
T.1.94	Възможност за динамично регулиране на ресурсите според натоварването, включително за работа в облачни среди и виртуализирани инфраструктури.
T.1.95	Възможност за интелигентно управление на натоварването и оптимизация на

	ресурсите чрез използване на технологии като load balancing и autoscaling.
T.1.96	Да бъде в състояние да обслужва нуждите на организацията при неограничено нарастващ обем от мрежови услуги и данни, като остава стабилна и ефективна.
T.1.97	Механизъм за известяване на администраторите за наличието на нови актуализации и критични поправки.
Гаранция и поддръжка:	
T.1.98	Поддръжка, включително получаване на нови версии на софтуера и 24/7 техническа помощ чрез телефон, имейл и портал за заявки за срок от 5 (пет) години, считано от дата на инсталиране и активиране на софтуера.
T.1.99	Поддръжката трябва да включва лицензни права за ползване на софтуерните пакети, получаване на софтуерни обновления, софтуер за корекции на грешки и помощ при отстраняване на несъвместимости с документираното поведение на софтуерното решение за целия срок на предоставеното право на ползване от 5 (пет) години, считано от дата на инсталиране и активиране на софтуера;

2. РЕШЕНИЕ ЗА СКАНИРАНЕ НА УЯЗВИМОСТИ

Обща информация	
T.2.1	Количество – 1 брой.
Спецификация – минимални изисквания	
T.2.2	Решението трябва да осигурява всички необходими лицензи с права за ползване на всички изисквани функционалности за минимум 1000 броя активи (асети), за период от 5 (пет) години;
T.2.3	<ul style="list-style-type: none"> • Решението трябва да се инсталира във виртуална/физическа 64-битова операционна система. • Решението трябва да предоставя възможност за използване на Security Console, Scan Engine и агенти. • Решението трябва да предлага вградени и персонализируеми шаблони за сканиране по тип система, регулация или критичност. • Уеб интерфейсът на решението трябва да е съвместим с всички основни браузъри (Chrome, Firefox, Edge и др.) • Уеб достъпът до решението трябва да е чрез HTTPS. • Позволява множество потребители да инициират сканирания. • Поддържа политика за достъп с потребителско име и парола. • Поддържа йерархична матрица от потребителски профили. • Централизирана администрация за управление на сканирания и отчети. • Локално внедряване (On-Premises Deployment): Решението трябва да се инсталира и функционира изцяло в инфраструктурата на Възложителя, без необходимост от използване на публичен облак. Да се поддържа пълна автономност при експлоатация, актуализация и съхранение на данни.
T.2.4	Решението трябва да обхваща всички активи: <ul style="list-style-type: none"> • Операционни системи: Windows, Unix AIX, Linux • Бази данни: SQL Server, Oracle, MySQL, PostgreSQL • Уеб сървъри: IIS, Apache, Tomcat, Nginx, и др. • Мрежово оборудване: Cisco, Palo Alto, Fortinet, Stonesoft и др. • Системи за сигурност: IDS/IPS, проксита, антивирусни • Приложения: Active Directory, SharePoint, уеб приложения и др.

T.2.5	Решението трябва: <ul style="list-style-type: none"> • да открива активи чрез IP адреси или диапазони. • точно да идентифицира ОС, име на хост, тип устройство (рутер, суич и др.), DNS, NetBIOS име, последна дата на анализ. • да поддържа категоризация на устройствата по различни критерии.
T.2.6	Решението трябва да открива уязвимости в: <ul style="list-style-type: none"> - Мрежово оборудване - Системи за сигурност - Бази данни - Операционни системи - Уеб приложения
T.2.7	Решението трябва да предлага и следните функции: <ul style="list-style-type: none"> • Вградена интеграция с инструменти за penetration testing. • Поддържа автентикация към системи за по-задълбочен анализ. • Включва механизъм за оценка на риска (освен CVSS, да включва и фактори като експлоатация, налични експлойти и др.) • Управление на SSL/TLS сертификати и известия. • Поддържа история на уязвимостите за конкретен хост.
T.2.8	Решението трябва да предоставя възможност за анализ и корелация чрез: <ul style="list-style-type: none"> • Честа актуализация на базата с уязвимости. • Приоритизиране на откритите уязвимости. • Свързване на уязвимост с наличен пач. • Поддръжка на ръчно и автоматично прилагане на корекции. • Предлагане на всички приложими мерки за корекция. • Системата трябва да използва глобална информация за заплахи, за да приоритизира уязвимостите според вероятността за експлоатация • Решението да предоставя възможност за анализ на Microsoft Active Directory с цел откриване на слабости, неправилни конфигурации и потенциални пътища за атака.
T.2.9	Решението трябва да предоставя следната отчетност: <ul style="list-style-type: none"> • Възможност за експорт на отчети в PDF, HTML, CSV, RTF, XML. • Проследяване на експозицията във времето. • Изпращане на отчети по имейл. • Готови шаблони и възможност за персонализиране. • Ограничаване на достъпа до отчети по потребителски профил. • Отчитане по критерии: ниво на критичност, CVE, групи активи, IP адреси, услуги, портове и др.
T.2.10	<ul style="list-style-type: none"> • Решението трябва да поддържа сканиране на активи както в локална среда, така и в облак.
Гаранция и поддръжка:	
T.2.11	Поддръжка, включително получаване на нови версии на софтуера и 24/7 техническа помощ чрез телефон, имейл и портал за заявки за срок от 5 (пет) години, считано от дата на инсталиране и активиране на софтуера.
T.2.12	Поддръжката трябва да включва лицензни права за ползване на софтуерните пакети, получаване на софтуерни обновления, софтуер за корекции на грешки и помощ при отстраняване на несъвместимости с документираното поведение на софтуерното решение за целия срок на предоставеното право на ползване от 5 (пет) години, считано от дата на инсталиране и активиране на софтуера;

3. РЕШЕНИЕ ЗА МОНИТОРИРАНЕ И УПРАВЛЕНИЕ НА ПРИВИЛЕГИРОВАННИЯ ДОСТЪП (РАМ)

Обща информация	
T.3.1	Количество – 1 брой.
Спецификация – минимални изисквания	
T.3.2	Предложеното решение трябва да включва лицензи за софтуер за мониториране и управление на привилегированния достъп (РАМ) за 20 привилегировани потребители с валидност и включена поддръжка за срок от 5 (пет) години.
T.3.3	Предложеното решение да не изисква директна интеграция с никой от елементите от мрежовата инфраструктура, както и да не изисква закупуването на допълнителни лицензи от трети страни.
T.3.4	Предложеното решение трябва да позволява мониторирането и управлението на привилегированния достъп чрез поддържаните от него протоколи до неограничен брой сървъри, като под сървър се разбира всеки уникален IP адрес с конкретен протокол за комуникация към него.
T.3.5	Предложеното решение трябва да се състои от минимално следните модули: - за мониториране и управление на отдалечени сесии с привилегирован достъп - за управление на пароли на акаунти на конкретни сървъри, минимално за Windows, Windows Server и Unix системи (Linux Red Hat, Linux Suse, Linux Debian, Linux Ubuntu, FreeBSD 10+), както и за Cisco мрежови устройства и MySQL бази от данни - за изготвяне на отчети за извършени активности и производителност на отдалечените сесии - за управление и разпределяне на пароли на приложения, чрез AAPM функционалност или чрез API.
T.3.6	Решението трябва да не изисква инсталирането на допълнителен софтуер (агенти) както на мониторираните сървъри, така и на работните станции, от които ще се извършват отдалечените сесии.
T.3.7	Решението трябва да разполага с функции за анализ на поведението, така че да може да засича автоматично аномалии по време на привилегированите сесии. Трябва да може да следи както потребителско поведение, така и съвпадение с поведение по зададен синтаксис.
T.3.8	Решението трябва да може да мониторира и управлява минимално следните протоколи: - Графични: RDP (включително сесии, използващи няколко монитора), VNC - Текстово-базирани: SSH (включително да се поддържа Proxy Jump функционалност), Telnet (да се позволява двойна автентикация) - За приложения: HTTP / HTTPS, MySQL, MS SQL и други базирани на TDS конектор - Други: за автоматизирани индустриални системи (SCADA), минимално MODBUS.
T.3.9	Решението трябва да поддържа минимално следните типове свързвания за RDP протокола: -TLS криптирани сесии -TLS сесии с NLA автентикация -некриптирани сесии -използвайки вграден клиент на ниво уеб-браузър.

T.3.10	Решението трябва да поддържа минимално следните функции за работа с SSH протокола: -поддръжка на SFTP подсистема за преглед и сваляне на трансферирани файлове с протокола -поддръжка на X11 тунел -поддръжка на тунел с SSH агент за forwarding -свързване чрез използване на вграден клиент, на ниво уеб-браузър.
T.3.11	Решението трябва да поддържа минимално следните функции за HTTP / HTTPS сесии: - цялостно графично представяне на уеб сесията - регистриране на всички елементи на уебсайта с възможност за пресъздаване на сесията под формата на записано видео - пресъздаване на реалния уебсайт, без необходимост от използване на междинна крайна точка за трансфер на данни.
T.3.12	Решението трябва да позволява управление и мониториране на сесии с отдалечен достъп, стартирани директно от дадено приложение, както и да се предоставя потребителски интерфейс, достъпван чрез уеб-браузър, където всеки потребител да може да вижда позволените за него сесии и да може да ги стартира директно от уеб-браузъра, поне за RDP и SSH протоколи.
T.3.13	Функцията за стартиране на сесии през уеб-браузър на решението трябва да е достъпна само за одобрени и автентикирани потребители. Автентикацията да може да се извършва директно или чрез интеграция с външна директория, минимално Active Directory, LDAP и Radius.
T.3.14	Решението трябва да позволява да се гледат и да се управляват незавършени сесии (сесии на живо). Даден администратор трябва да може да се присъединява към активни сесии и да може да наблюдава случващото се в реално време, минимално за RDP, VNC, SSH и telnet протоколи.
T.3.15	Решението трябва да разполага с функция за разпознаване на кой е натиснал клавиш на клавиатурата или клик с мишката измежду наблюдаващия администратор и потребителя, стартирал отдалечената сесия.
T.3.16	Решението трябва да разполага с функция за преглед на всички въведени команди и натиснати клавиши по време на дадена отдалечена сесия, като тази функция трябва да изисква одобрение в интерфейса на решението от минимално двама администратори от зададен списък с такива с по-високо ниво на достъп.
T.3.17	Решението трябва да позволява на администраторите, които са свързани към активни сесии, да могат да ги прекъсват по всяко време и да могат да блокират дадения потребител, стартирал сесията, от повторен опит за свързване.
T.3.18	Решението трябва да позволява администрирането, мониторирането, верифицирането и прегледа на сесии с отдалечен достъп да се извършва изцяло през конзола за централизирано управление, достъпна чрез уеб-браузър.
T.3.19	Прегледът на мониторираните сесии, както записани в исторически план, така и сесии на живо, не трябва да изисква инсталирането на допълнителен софтуер (това важи и за добавки на ниво уеб-браузър, например Flash).
T.3.20	Решението трябва да може да анализира и записва сесии с отдалечен достъп директно, без да изисква междинни крайни точки за пренос на данни.
T.3.21	Решението трябва да може да известява (минимално чрез syslog или чрез

	email) администраторите за следните събития: - стартиране на сесия - прекратяване на сесия - присъединяване на администратор или на външно лице с покана към активна сесия - отписване на администратор или на външно лице с покана от активна сесия.
T.3.22	Решението трябва да разполага с функция за изискване на причина за установяване на сесия с отдалечен достъп. Причината трябва да може да се попълни от потребителите в поле преди установяването на сесията, като причината трябва да се съхранява в метаданните на дадената сесия. Тази функция трябва да се поддържа минимално за следните протоколи: RDP, VNC, SSH, telnet.
T.3.23	Решението трябва да позволява да се определят лимитации относно параметрите на извършваните сесии, минимално: - за RDP протокол: лимитиране на максималната резолюция на екрана и на цветовата гама (минимално 8 bpp и 16 bpp), възможност за блокиране на clipboard функцията - за SSH протокол: блокиране на пренасочване на портове, на X11 тунела, на пренасочване с SSH агент, на SFTP подсистемата и на файлов трансфер чрез SCP.
T.3.24	Решението трябва да поддържа методи за автентикация чрез външни сървъри, минимално Active Directory, Radius, LDAP (включително OpenLDAP).
T.3.25	Решението трябва да поддържа използването на цялостна синхронизация с Active Directory, включително: -конкретни групи от домейна на Active Directory -конкретна организация или OU -множество домейни на Active Directory, дори когато дадено потребителско име е дублирано в два или повече домейна -потребители и групи от потребители по предварително зададени филтри.
T.3.26	Решението трябва да може да записва целия мрежови трафик, свързан с дадена сесия (запис на „суров“ мрежови протокол).
T.3.27	Решението трябва да може да прави видео запис с всичките параметри на сесиите с отдалечен достъп, като да може да се селектира за кои сесии да се извършва запис.
T.3.28	Решението трябва да позволява на потребителите да могат да заменят техните данни за вписване с други, познати на таргетирания от тях сървър за отдалечена сесия.
T.3.29	Решението трябва да позволява при извършване на графични сесии с отдалечен достъп да се извиква персонализиран прозорец за въвеждане на данни за вписване към таргетираният сървър (система).
T.3.30	Решението трябва да позволява при извършване на графични и текстови сесии (минимално за SSH и telnet) с отдалечен достъп да може да се установи връзка, без да е необходимо потребителят да знае името на домейна (FQDN), нито IP адреса на таргетираният сървър (система), а само името, дефинирано от администратор на PAM решението.
T.3.31	Решението трябва да разполага с функция, при която да се изисква задължително одобрение от администратор преди установяване на сесия.
T.3.32	Решението трябва да може да се интегрира с SIEM технологии, минимално на ниво syslog протокол.

T.3.33	Решението трябва да може автоматично да категоризира събраните данни и да им поставя етикети директно според SIEM технологията, с която ще се интегрира решението, без да се налага ръчно да се маркират ключови думи от събраните логове.
T.3.34	Решението трябва да позволява да могат да се дефинират обхвати от IP адреси, до които ще се извършва достъп, включително събнети (например маска/24) - минимално за следните протоколи: RDP, VNC, SSH и telnet.
T.3.35	Решението трябва да позволява за RDP протокола да се извършва достъп до свързани подмрежи от VDI системи, използвайки Connection Broker, без да е необходимо да се дефинира всяка VDI система поотделно.
T.3.36	Решението трябва да позволява да се поставят коментари под прегледаните сесии, като това да важи за сесии в реално време и записани изминали сесии.
T.3.37	Решението трябва да може автоматично да терминира дадена сесия според зададена политика за съвпадение по време на сесията със зададен низ от символи, като да може да се изпраща автоматично аларма към даден администратор.
T.3.38	Решението трябва да разполага с функция за изпращане на изискване за допълнително одобрение на дадена сесия към трети страни (супервайзор), след като даден потребител успешно се е автентикирал с неговите данни.
T.3.39	Решението трябва да разполага и с опционално приложение за мобилни устройство за одобрение/отхвърляне от супервайзор на заявки за сесии.
T.3.40	Решението трябва да разполага минимално със следните функции за осигуряване на Just-in-Time (JIT) достъп: - лимит от стартирането на сесията до следващите 24 часа (например сесията да е валидна само за 1 час от стартирането ѝ) - по зададен график (зададени начална и крайна дата на дадена сесия).
T.3.41	Решението трябва да може автоматично да сканира за домейн контролери за акаунти с различни нива на привилегии и да може да ги интегрира за мониториране (auto-discovery).
T.3.42	Решението да разполага с Auto-discovery функцията, която трябва да може да сканира минимално Active Directory, използвайки само LDAP конектор и трябва да може да работи в два режима: - да може да присвоява на всички открити акаунти достъп до ресурси - да може да поставя под карантина всички недоверени акаунти и да може да блокира достъпа им до дадени сървъри.
T.3.43	Решението трябва да разполага с функция за търсене на сесии, като търсенето да е както на входящите данни (например въведени команди), така и на изходящите (например какво се показва на екрана). Конкретно за графични протоколи като RDP и VNC, да може да се търси в цялото съдържание, показано на екрана в даден момент.
T.3.44	Резултатите от търсенето в сесиите трябва да са мигновени, освен при използването на вградена OCR функция за разпознаване на графични елементи. OCR механизмът трябва да е имплементиран минимално за HTTP / HTTPS сесии (текстови и за графични), VNC сесии и RDP сесии, като да може да разпознава всички елементи и текст от дадена сесия и да може да ги запазва в база от данни на решението. Под текст се разбира както команди, въведени с клавиатурата, така и изписан текст, където и да е на екрана по време на графичната сесия (имена на прозорци на приложения, данни в документи, известия, имена на файлове и други).

T.3.45	Резултатите от търсенето в сесиите трябва да се изчисляват вградено, без да се налага да има износ на информация към облачни среди или други устройства.
T.3.46	Решението трябва да позволява функцията за търсене в сесиите да може да се изключва за определени потребители.
T.3.47	Решението трябва да позволява да се предоставя временен достъп до конкретна сесия, както за записани сесии, така и за сесии на живо. Ако сесията е на живо, да може да се определи дали достъпът е само за преглед, или и с функции за присъединяване и споделяне на сесията с външни лица. Трябва да има функция за премахване на временния достъп до споделена сесия по всяко време от администратор.
T.3.48	Решението трябва да може да мониторира и да разполага с отчети за потребителска активност и ефикасност по време на сесии с отдалечен достъп. Анализът на продуктивността на потребителите трябва да отразява как се е променяла във времето.
T.3.49	Решението трябва да позволява да се определя таргетирано поведение според тип активност (например брой действия с клавиатура или с мишка, при графични сесии) и да може лесно да се идентифицират всички потребители и сесии, които не са покрили изискванията за минимална активност. Активността да може да се измерва в процентно изражение и да може да се сравнява с нива на активност от различни периоди във времето.
T.3.50	Решението трябва да разполага с ролево-базиран контрол на достъпа, като определените роли да бъдат минимално: <ul style="list-style-type: none"> -обикновени потребителски акаунти -администраторски акаунти с достъп за преглед на сесии -администраторски акаунти с достъп за преглед на конфигурацията на решението -администраторски акаунти с достъп за промяна на конфигурацията на решението -администраторски акаунти с достъп за управление на решението (например за рестартиране на системата).
T.3.51	Достъпът на администраторите на решението трябва да може да се лимитира за преглед и управление до конкретни сървъри (системи) и конкретни потребителски акаунти.
T.3.52	Решението трябва да може да поставя маркери за дата и час на всяка сесия и действия в нея, като маркерите да могат да се синхронизират с квалифицирани системи за целта, минимално KIR и PWPW.
T.3.53	Решението трябва да позволява да се определя периода за съхранение на записаните сесии и събраните данни, като при изминаването му да могат да се изтриват автоматично от системата.
T.3.54	Решението трябва да може да се интегрира с външни решения за управление на пароли, минимално CyberArk, Thycotic, LAPS.
T.3.55	Решението трябва да разполага с check-in и check-out функции за работа с пароли на други потребители.
T.3.56	Решението трябва да позволява задаването на правила чрез използване на низ от изпълнени команди или въведени символи, които при наличие в сесия за отдалечен достъп да могат минимално да изпълняват следните действия автоматично: <ul style="list-style-type: none"> -да могат да изпращат информация за действието по syslog протокол

	<ul style="list-style-type: none"> -да могат да изпращат информация към SIEM ситеми -да могат да изпращат известия до дадени администратори чрез email -да могат незабавно да прекратят сесията, при която е възникнало даденото действие, с допълнителни опции да може да се блокира съмнителният потребител, независимо от статуса му.
T.3.57	Решението трябва да позволява използването на сложни регулярни изрази (regex) за изграждането на правилата му, използването на wildcards не се счита за еквивалентно.
T.3.58	Зададените правила в решението трябва да могат да работят минимално за следните протоколи: RDP, VNC, SSH, Telnet.
T.3.59	<p>Зададените правила в решението трябва да могат да функционират минимално в следните случаи:</p> <ul style="list-style-type: none"> -цялостно съвпадение във входящите данни и в данните от сесиите след индексирането им при приключване на сесията, поне за VNC и RDP протоколи. -за други поддържани протоколи, съвпадение във входящите данни и данните на екрана, минимално по време на изпълнение на сесията.
T.3.60	Решението трябва да позволява сесиите да могат да се записват като видео (линеен запис), използвайки формати, които позволяват възпроизвеждане с VLC 3.0 програма или по-нова версия. Подобно възпроизвеждане трябва да е налично минимално за VNC, RDP, SSH и telnet записани сесии.
T.3.61	<p>Решението трябва да разполага с добре описан API интерфейс в документацията на производителя, който да позволява изпълнението на скриптове минимално за:</p> <ul style="list-style-type: none"> -създаване, промяна и изтриване на потребителски акаунти в решението -създаване, промяна и изтриване на сървърни акаунти в решението -създаване, промяна и изтриване на права за достъп до сървъри и системи в решението -създаване, промяна и изтриване на информация за IP адреси и портове в решението, до които потребителите могат да се свързват -създаване, промяна и изтриване на връзки между акаунти, сървъри и права за достъп -сваляне на списък със сесии, с възможност за маркиране визуално кои сесии все още не са били приключили при изпълнението на скрипта -блокиране на потребители, независимо от статуса им.
T.3.62	Решението трябва да позволява връщането му към предходна работеща версия, директно от интерфейса на решението.
T.3.63	Решението трябва да разполага с функция за промяна на парола в Unix системи, използвайки привилегирован акаунт и достъп чрез SSH ключ.
T.3.64	Решението трябва да разполага с функция за изпълнение на низ от команди за промяна на парола на дадена система.
T.3.65	Решението трябва да разполага с механизъм за проверка, който да потвърждава, че промяна на дадена парола не е извършена по неоторизиран начин.
T.3.66	Решението трябва да може да съхранява историята на използваните пароли за даден акаунт и да позволява възстановяването на дадена парола като активна от списъка с използвани във времето.
T.3.67	Решението трябва да позволява да може да се конфигурира сложността на автоматично генерираните от него пароли.

T.3.68	Решението трябва да може да работи със сървъри за управление на привилегированя достъп до тях с минимално следните операционни системи: -Windows Server 2012 или по-нови -Linux - Red Hat 6 или по-нови (както и еквивалентни дистрибуции, ако са по-нови) -FreeBSD 10 или по-нови.
T.3.69	Решението трябва да може да съхранява събраната информация в криптиран вид, минимално във формат AES 256.
T.3.70	Решението трябва да може да работи минимално в следните режими: -под формата на сървър, за трансмисия на данни (на слой 5+ от OSI модела) -под формата на приложение – да може да слуша зададени IP адреси или адреси с конкретни портове -под формата на рутер (слой 3 от OSI модела), изпращайки пакети/трафик само до посочени сървъри -под формата на мост (слой 2 от OSI модела), изпращайки целия мрежови трафик между две крайни точки с Ethernet връзка, но без да се намесва в мрежовите пакети, които не са част от дадена сесия.
T.3.71	Решението трябва да позволява използването на собствени сертификати/ключове за криптиране на комуникация (минимално за RDP и SSH протоколи), както и да позволява използването на текущи сертификати от управляваните сървъри или системи.
T.3.72	Решението трябва да позволява да се мониторира параметрите му чрез SNMP протокол, минимално версия 3.
T.3.73	Решението трябва да може да извършва базова мрежова диагностика от графичният интерфейс: -да може да прави проверка за свързаност чрез ping, използвайки ICMP сигнал -да може да прави проверка за свързаност чрез TCP връзка до портове и IP адреси.
T.3.74	Решението трябва да може да работи със следните мрежови услуги: -NTP -DNS
T.3.75	Решението трябва да може да се предоставя под формата на виртуално устройство, което да може да се поставя минимално на следните платформи: -VMware 5.x -VMware 6.x -KVM / OpenStack / Proxmox или други базирани на KVM или qemu хипервайзор.
Гаранция и поддръжка:	
T.3.76	Поддръжка, включително получаване на нови версии на софтуера и 24/7 техническа помощ чрез телефон, имейл и портал за заявки за срок от 5 (пет) години, считано от дата на инсталиране и активиране на софтуера.
T.3.77	Поддръжката трябва да включва лицензни права за ползване на софтуерните пакети, получаване на софтуерни обновления, софтуер за корекции на грешки и помощ при отстраняване на несъвместимости с документираното поведение на софтуерното решение за целия срок на предоставеното право на ползване от 5 (пет) години, считано от дата на инсталиране и активиране на софтуера;

4. ПЛАТФОРМА ЗА ЦЕНТРАЛИЗИРАНО АВТЕНТИКИРАНЕ

Обща информация	
T.4.1	Количество – 1 брой /състояща се от минимум 2 броя резервиран софтуер/.
Спецификация – минимални изисквания	
T.4.2	Платформата да поддържа инсталация върху виртуална машина с поддръжка на VMWare ESXi, Linux KVM и Microsoft Hyper-V.
T.4.3	Платформата да предоставя AAA услуги за потребители и устройства.
T.4.4	Платформата да предоставя вградени WEB/Captive портали за идентификация на потребителите.
T.4.5	Платформата да предоставя API интерфейс за интеграция с външни системи за отчетност и мрежови политики.
T.4.6	Платформата да предоставя възможност за интеграция с външни сървъри за идентификация - Microsoft Active Directory, LDAP, RADIUS, RSA системи за идентификация с еднократна парола.
T.4.7	Платформата да предоставя възможност за удостоверяване чрез потребителско име и парола, с X.509 сертификат и по MAC адрес.
T.4.8	Платформата да предоставя възможност профилиране на крайните устройства.
T.4.9	Платформата да предоставя BYOD функции.
T.4.10	Платформата да предоставя възможност за прилагане на различни политики за удостоверяване и оторизация на база: <ul style="list-style-type: none"> • Час и дата на идентификацията • Тип на връзката – 802.1x wired, 802.1x wireless, достъп през VPN , достъп през WEB портал за идентификация • Използван EAP тип • Потребителско име • RADIUS атрибути • Атрибути на X.509 потребителските сертификати • Вид/модел/OS на устройството
T.4.11	Платформата да има управление на мрежовия достъп: <ul style="list-style-type: none"> • Динамично зареждане на филтриращи листи (ACL) в мрежовите устройства на база политиките за управление на достъпа. • Динамично назначаване на VLAN мрежи към потребителите на база политиките за управление на достъпа. • URL пренасочвания на потребителите към вградени или външни WEB/Captive портали.
T.4.12	Платформата да има поддръжка на RADIUS и Radius CoA.
T.4.13	Платформата да има функция на RADIUS proxy.
T.4.14	Платформата да има възможност за TACACS+ за идентификация и управление нивото на достъп на администраторите към мрежови устройства.
T.4.15	Платформата да има възможност за проверка на състоянието (posture assessment) на крайните потребители.
T.4.16	Вграден Certificate Authority.
T.4.17	Платформата да поддържа: <ul style="list-style-type: none"> - Web GUI - HTTP и HTTPS - Ping - DNS

	<ul style="list-style-type: none"> - TFTP - FTP - NTP - SSHv2 - Интеграция с LDAP - Автоматичен backup на базата данни върху външни FTP и SFTP сървъри
T.4.18	За работа с платформата да бъдат предоставени лицензи за удостоверяване и оторизация на 650 крайни устройства едновременно.
Гаранция и поддръжка:	
T.4.19	Поддръжка, включително получаване на нови версии на софтуера и 24/7 техническа помощ чрез телефон, имейл и портал за заявки за срок от 5 (пет) години, считано от дата на инсталиране и активиране на софтуера.
T.4.20	Поддръжката трябва да включва лицензни права за ползване на софтуерните пакети, получаване на софтуерни обновления, софтуер за корекции на грешки и помощ при отстраняване на несъвместимости с документираното поведение на софтуерното решение за целия срок на предоставеното право на ползване от 5 (пет) години, считано от дата на инсталиране и активиране на софтуера;

5. НАДГРАЖДАНЕ НА ЦЯЛОСТНА СИСТЕМА ОТ ЗАЩИТНИ СЕНИ

5.1. Доставка на 6 броя защитни стени (NGFW) - хардуерни устройства, с еднакви параметри – модел, версия на Firmware, настройки и спецификация за осигуряване на непрекъсваемост на мрежовата услуга, както и необходимите лицензи за функциониране на цялата **надградена система**.

5.1.1. Минимални функционални изисквания за защитните стени:

Обща информация	
T.5.1.1.1	Количество – 6 броя хардуерни устройства и необходимите лицензи към тях за ползване на софтуерните пакети.
Спецификация – минимални изисквания	
T.5.1.1.2	Изграждане на сектори с различна степен на доверие, които да разделят мрежата на отделни сегменти и прилагане на политики на база потребителски имена от Активната Директория;
T.5.1.1.3	Защитната стена да анализира съдържанието за наличие на зловреден код като включва минимум AntiVirus, AntiSpyware, IPS;
T.5.1.1.4	AntiVirus инспекцията да може да задържа Zero day файл в защитната стена докато получи отговор за неговата репутация.
T.5.1.1.5	Защитната стена да анализира непознати заплахи (Zero Day зловреден код) в защитена среда като създава и дистрибутира сигнатури в реално време.
T.5.1.1.6	Защитната стена за IPS да използва машинно, задълбочено обучение да открива и блокира непознати Command and Control (C2), при преминаване на непознат HTTP, HTTP2, SSL, TCP и UDP трафика през защитната стена.
T.5.1.1.7	Защитната стена за анализ на Zero Day зловреден код трябва да използва минимум следните методи за анализ: Static Analysis, Machine Learning, Dynamic Analysis
T.5.1.1.8	Защитната стена да анализира PE, ELF файлове PowerShell скриптове в защитната стена и предоставя защита в реално време.
T.5.1.1.9	Защитната стена следва да инспектира за заплахи HTTPS протокола чрез

	декриптиране;
T.5.1.1.10	Защитната стена следва да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи;
T.5.1.1.11	Защитната стена да филтрира уеб сайтовете по категории и ограничаване на достъпа до опасно съдържание в Интернет, включително мултикатегоризация на URL съгласно тип на съдържанието и риск;
T.5.1.1.12	Защитната стена да анализира URL и тяхното съдържание в реално време. Всяка заявка за достъп да бъде анализирана чрез Machine Learning на база на HTTP Request.
T.5.1.1.13	Управлението на защитната стена трябва да се реализира чрез физически отделени процесор, памет и интерфейси отделени от ресурсите използвани за управление на трафика.
T.5.1.1.14	Операционната система на защитната стена да позволява на администратора да работи върху копие на работещата конфигурация и след като е готов с промените при потвърждение да се извърши валидация, резервно копие (backup) и прилагане на промените.
T.5.1.1.15	Защитната стена да може да дистрибутира входящите NAT сесии между няколко адреса като използва минимум следните методи: Round Robin, Source IP Hash, Least Sessions
T.5.1.1.16	Администратора трябва да може да изисква прекатегоризация на даден URL директно от графични интерфейс на защитната стена.
T.5.1.1.17	Защитната стена да анализира и открива phishing чрез ML анализ на изображения и домейни, CAPTCHA интегриран анализ, превенция на кражба на идентификационни данни (Username / password) в реално време.
T.5.1.1.18	Защитната стена да разполага с DLP (Data Loss Prevention) функционалност за ограничаване на движението на конфиденциални файлове.
T.5.1.1.19	Политиката за декриптиране трябва да има възможност да се настройва на база на URL или URL категория;
T.5.1.1.20	Защитната стена да притежава възможност да ограничава достъпа на потребителите до Web сървъри, които не поддържа минимални изисквания за валиден публичен сертификат и съответно високо ниво на сигурност (TLSv1.1, TLSv1.2, TLSv1.3);
T.5.1.1.21	Защитната стена трябва може да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина с Windows и MacOS .
T.5.1.1.22	Агента за VPN достъп трябва да поддържа (да може да бъде инсталиран) чрез добавяне на допълнителен лиценз на минимум следните операционни системи: Android, iOS, Raspbian, Ubuntu.
T.5.1.1.23	Възможност за QoS трафика според типа приложение потребител и/или URL категория.
T.5.1.1.24	Прозрачна идентификация на потребителите от Активната директория без изискване на крайната машина да се инсталира агент, настройки в browser или отваряне на Web Portal.
T.5.1.1.25	Защитната стена да предоставя възможност за надграждане с допълнителен лиценз за идентифициране на устройства (Device Fingerprint) в мрежата на база поведение, мета данни и логове, както и за карантина на заразени устройства независимо от техните IP адреси, локация и потребител.
T.5.1.1.26	Защитната стена да може при регистрирана атака (log) автоматично да поставя засегнатите потребители и IP в група с ограничен достъп до мрежата

	(изолация или карантина).
T.5.1.1.27	Защитната стена да може да чете данните в X-Forwarded-For (XFF) за идентифициране на реалния източник на данни (IP Address), когато той се намира зад други мрежови устройства.
T.5.1.1.28	Защитната стена да има функционалност за защита на корпоративните потребителски имена и пароли, посредством блокиране или ограничаване на тяхното използване в външни за организацията системи и публично достъпни доставчици (Dropbox, Google, Facebook, LinkedIn).
T.5.1.1.29	Защитната стена да включва функционалност, позволяваща служебния достъп до публични облачни услуги като Office 365, Google, Dropbox и YouTube, и ограничаване достъпа до лични потребителски акаунти за същите приложения.
T.5.1.1.30	Защитната стена да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи. Анализа на логовете и репортинг да се извършва от самото устройство чрез неговия графичен интерфейс без да е необходима инсталация на допълнителен софтуер.
T.5.1.1.31	Генерираните отчети и логове следва да са обогатени с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и други).
T.5.1.1.32	Защитната стена да може автоматично да тегли IP, Domain или URL листи от Web Server собственост на Възложителя или външна организация с цел ограничаване / позволяване на достъпа до горе споменатите.
T.5.1.1.33	Защитната стена да открива в реално време атаки като инспектира DNS Response и DNS Request.
T.5.1.1.34	Защитната стена да разполага с функционалност за DNS защитата, която да може в реално време без допълнителни модули или платформи да прилага активна защита към специфични техники и категории като: "C&C domains", "DGA detection", "NXNSAttack", "DNS rebinding", "Malware domains", "Newly Registered Domains", "Phishing Domains", "Parked domains", "Proxy avoidance", "Ad tracking domains", "Hijacked Domains", "Misconfiguration Domains".
T.5.1.1.35	Защитната стена да може автоматично да открива какви приложения работят в организацията и да предлага лист от такива, които да бъдат добавени към нови или вече съществуващи правила за сигурност.
T.5.1.1.36	Защитната стена да притежава облачна услуга за събиране и анализ на служебни данни от устройството като чрез машинно обучение препоръчва добри практики и открива аномалии в нормалната работа.
T.5.1.1.37	Защитната стена да има възможност за надграждане чрез лиценз за услуга, която позволява на защитната стена да категоризира непознати приложения в облака на производителя, за които няма конкретни предварително дефинирани сигнатури.
T.5.1.1.38	Защитната стена да предоставя възможност за надграждане чрез лиценз за защита на крайно клиентските машини, позволяващ събиране и анализ на всички логове (от крайните точки и защитните стени) в защитена облачна среда на производителя.
T.5.1.1.39	Защитната стена да има възможност за надграждане с допълнителен лиценз, инсталиран на защитната стена, с който да открива и управлява IoT (Internet of Things) устройства като предоставя възможност за автоматично генериране на препоръчани правила за достъп и контрол.

T.5.1.1.40	Защитната стена да може да пропуска до три софтуерни версии при upgrade като дава възможност да се избере да пропусне две основни версии и една второстепенна, или една основна версия и две второстепенни.
Гаранция и поддръжка:	
T.5.1.1.41	Поддръжка, включително получаване на нови версии на софтуера и 24/7 техническа помощ чрез телефон, имейл и портал за заявки за срок от 5 (пет) години, считано от дата на инсталиране и активиране на софтуера.
T.5.1.1.42	Поддръжката трябва да включва лицензни права за ползване на софтуерните пакети, получаване на софтуерни обновления, софтуер за корекции на грешки и помощ при отстраняване на несъвместимости с документираното поведение на софтуерното решение за целия срок на предоставеното право на ползване от 5 (пет) години, считано от дата на инсталиране и активиране на софтуера;

5.1.2. Минимални технически изисквания на хардуерните устройства.

	Параметър	Минимално изискване
T.5.1.2.1	Минимална пропускателна способност с активирана функция за идентификация на приложенията (HTTP трафик)	2.5 Gbps
T.5.1.2.2	Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/ AntiSpyware / URL / Firewall / Application Control / Sandbox	1.1 Gbps
T.5.1.2.3	Минимална производителност за IPsec VPN	1.1 Gbps
T.5.1.2.4	Минимален брой TCP сесии	200 000
T.5.1.2.5	Минимален брой нови сесии в секунда	30 000
T.5.1.2.6	Разпознати и поддържани приложения (минимум)	5 000
T.5.1.2.7	Минимален брой мрежови интерфейси	Да разполага с 8x10/100/1000 Base-T ports
T.5.1.2.8	Режими на работа на интерфейсите	L2, L3, Tap, Transparent едновременно/микс да се използват върху едно устройство.
T.5.1.2.9	Машрутизираци протоколи	OSPFv2/v3, BGP with graceful restart, RIP, static routing Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE)
T.5.1.2.10	Минимални изисквания към IPSec имплементация	Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication) Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
T.5.1.2.11	Минимален брой конкурентни SSL VPN потребителя включени в	100 SSL VPN потребителя

	системата (постоянни лицензи)	
T.5.1.2.12	Минимален брой IPsec SD-WAN Site-to-Site VPN	30 отдалечени точки
T.5.1.2.13	Устройството да поддържа виртуални таблици за маршрутизация минимум	2 броя
T.5.1.2.14	IPv6 поддръжка	Всички конфигурации за интерфейсите модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
T.5.1.2.15	Инспекция на SSL криптиран трафик, без оглед на прилежащия протокол, като предоставя декриптирания трафик на всички свои функционални компоненти, за инспекция и налагане на политики над съдържанието	Системата следва да декриптира и инспектира SSL като поддържа : TLS v1.1, TLS v1.2, TLS v1.3
T.5.1.2.16	Управление на устройството	Всяко от устройствата в системата да има възможност да се управлява посредством имплементация на REST based API, извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
T.5.1.2.17	Режим на надеждност	Active-Passive, Active/Active
T.5.1.2.18	Минимален брой интерфейси за управление	1 x RJ45 (1GB) порт за управление 1 x RJ-45 конзолен порт 1 x USB port 1 x Micro USB port
T.5.1.2.19	Монтаж, размери, охлаждане	Предназначена за вграждане в 19"
T.5.1.2.20	Захранване и входно напрежение (Входяща честота)	Външно, с максимална консумирана мощност не повече от 35W

5.1.3. Изпълнителят следва да осигури валидна хардуерна и софтуерна поддръжка считано от датата на изтичане на наличната такава до 08.10.2031 г. за **наличните устройства** със следните серийни номера:

№	Партиден номер на устройството	Сериен номер на устройството	Дата на изтичане на поддръжката
T.5.1.3.1	PA-3410	24101017989	19.7.2027
T.5.1.3.2	PA-3410	24101017985	19.7.2027

T.5.1.3.3	PAN-PA-410	23109003739	02.4.2030
T.5.1.3.4	PAN-PA-440	21209049989	8.10.2028
T.5.1.3.5	PAN-PA-440	21209053335	8.10.2028
T.5.1.3.6	PAN-PA-440	21209053541	8.10.2028
T.5.1.3.7	PAN-PA-440	21209053559	8.10.2028
T.5.1.3.8	PAN-PA-440	21209053567	8.10.2028
T.5.1.3.9	PAN-PA-440	21209053570	8.10.2028
T.5.1.3.10	PAN-PA-440	21209053572	8.10.2028
T.5.1.3.11	PAN-PA-440	21209053573	8.10.2028
T.5.1.3.12	PAN-PA-440	21209053582	8.10.2028
T.5.1.3.13	PAN-PA-440	21209053633	8.10.2028
T.5.1.3.14	PAN-PA-440	21209053706	8.10.2028
T.5.1.3.15	PAN-PA-440	21209053742	8.10.2028
T.5.1.3.16	PAN-PA-440	21209053759	8.10.2028
T.5.1.3.17	PAN-PA-440	21209053774	8.10.2028
T.5.1.3.18	PAN-PA-440	21209053786	8.10.2028
T.5.1.3.19	PAN-PA-440	21209053788	8.10.2028
T.5.1.3.20	PAN-PA-440	21209053790	8.10.2028
T.5.1.3.21	PAN-PA-440	21209053797	8.10.2028
T.5.1.3.22	PAN-PA-440	21209053802	8.10.2028
T.5.1.3.23	PAN-PA-440	21209049989	8.10.2028
T.5.1.3.24	PAN-PA-440	21209053335	8.10.2028
T.5.1.3.25	PAN-PA-440	21209053541	8.10.2028
T.5.1.3.26	PAN-PA-440	21209053559	8.10.2028
T.5.1.3.27	PAN-PA-440	21209053567	8.10.2028
T.5.1.3.28	PAN-PA-440	21209053570	8.10.2028
T.5.1.3.29	PAN-PA-440	21209053572	8.10.2028
T.5.1.3.30	PAN-PA-440	21209053573	8.10.2028
T.5.1.3.31	PAN-PA-440	21209053582	8.10.2028
T.5.1.3.32	PAN-PA-440	21209053633	8.10.2028
T.5.1.3.33	PAN-PA-440	21209053706	8.10.2028
T.5.1.3.34	PAN-PA-440	21209053742	8.10.2028
T.5.1.3.35	PAN-PA-440	21209053759	8.10.2028
T.5.1.3.36	PAN-PA-440	21209053774	8.10.2028
T.5.1.3.37	PAN-PA-440	21209053786	8.10.2028
T.5.1.3.38	PAN-PA-440	21209053788	8.10.2028
T.5.1.3.39	PAN-PA-440	21209053790	8.10.2028
T.5.1.3.40	PAN-PA-440	21209053797	8.10.2028
T.5.1.3.41	PAN-PA-440	21209053802	8.10.2028
T.5.1.3.42	PAN-PRA-25	702077237	8.10.2028

5.1.4. Изпълнителят следва да осигури надграждане на налична централизирана система за управление по Т.5.1.3.42. като броят управлявани устройства следва да бъде 100 броя.

6. СЪРВЪРИ ТИП1

№	Параметър	Минимални технически изисквания
T.6.1	Процесор	Минимум 32 ядра, минимум 64 нишки, минимум 2.1GHz минимална честота, минимум 160MB Cache
T.6.2	Памет	Сървърите да бъдат доставени с минимум 16x 32GB DDR5 Registered. Паметта да е инсталирана
T.6.3	Дискове	Сървърите да бъдат доставени с 2 x 480GB SSD Drives и 4x 2.4TB SAS 12G Mission Critical 10K SFF HDD. Дисковете да са инсталирани
T.6.4	Свързаност	Сървърите да бъдат доставени с минимум: <ul style="list-style-type: none"> • Порт за отдалечено администриране – iLO или еквивалентен • 2 port x Ethernet 10Gb SFP+ • 2 port x 10 Gigabit Ethernet 10GBase-T
T.6.5	Захранване	Сървърите да бъдат доставени с 2x 1000W вградени захранвзци блока
T.6.6	Размери	2U
T.6.7	Вградено управление	Сървърите да бъдат доставени с възможности за вградено управление от типа на iLO 6 или еквивалент
T.6.8	Охлаждане	Вградени вентилатори - Минимум 6 бр.
T.6.9	Окомплектовка	Шини за монтаж в 19" сървърен шкаф
T.6.10	Гаранция	Не по-малко от 36 месеца

7. СЪРВЪРИ ТИП2

№	Параметър	Минимални технически изисквания
T.7.1	Процесор	Минимум 12 ядра, минимум 24 нишки, минимум 2.4GHz минимална честота, минимум 30MB Cache
T.7.2	Памет	Сървърите да бъдат доставени с минимум 8x 32GB DDR5 Registered. Паметта да е инсталирана
T.7.3	Дискове	Сървърите да бъдат доставени с 2x 480GB SSD Drives и 2x 2.4TB SAS 12G Mission Critical 10K SFF HDD. Дисковете да са инсталирани
T.7.4	Свързаност	Сървърите да бъдат доставени с минимум: <ul style="list-style-type: none"> • Порт за отдалечено администриране – iLO или еквивалентен • 2 port x Ethernet 10Gb SFP+ • 4 port x 1Gigabit Ethernet Base-T
T.7.5	Захранване	Сървърите да бъдат доставени с 2x 1000W вградени захранвзци блока
T.7.6	Размери	2U
T.7.7	Вградено управление	Сървърите да бъдат доставени с възможности за вградено управление от типа на iLO 6 или

		еквивалент
T.7.8	Охлаждане	Вградени вентилатори - Минимум 6 бр.
T.7.9	Окомплектовка	Шини за монтаж в 19" сървърен шкаф
T.7.10	Гаранция	Не по-малко от 36 месеца

8. КVM КОМУТАТОРИ

№	Параметър	Минимални технически изисквания
T.8.1	Брой канали	8 бр. клавиатура, мишка и дисплей
T.8.2	Възможност за разширение на каналите	Последователно свързване на ≥ 16 устройства
T.8.3	Избор на канал	Бутон(и), Hotkey, GUI
T.8.4	Управление	<ul style="list-style-type: none"> През WEB
T.8.5	Отдалечено управление	10/100 Ethernet RJ45
T.8.6	Монтаж	Устройството да е окомплектовано със скоби за монтаж в 19" шкаф
T.8.7	Захранване	230VAC – през адаптер
T.8.8	Гаранция	Не по-малко от 36 месеца

9. НАСТОЛНИ КОМПЮТРИ

№	Параметър	Минимални технически изисквания
T.9.1	Тип система	Работна станция - Tower
T.9.2	Процесор	Двадесетядрен Intel Core Ultra 7 265K (3.3 - 5.5 GHz, 30 MB cache), еквивалентен или по-добър
T.9.3	Оперативна памет	2 x 16 GB DDR5 5600 с възможност за разширение до 256GB
T.9.4	Графика	Вградена
T.9.5	Дискова памет	1 TB SSD M.2 NVMe
T.9.6	Сигурност	TPM 2.0 модул за защита на данните
T.9.7	Аудио	Високоговорител 2 W
T.9.8	Комуникация	Мрежа: 10/100/1000 Mbps Безжична свързаност: Wi-Fi 7 802.11be, Bluetooth 5.4
T.9.9	Сертификати	Зелен сертификат ENERGY STAR
T.9.10	Захранване	230VAC 700W
T.9.11	Клавиатура	Кирилизирана по БДС (трайно гравирана) – включена в доставката
T.9.12	Мишка	Жична – включена в доставката
T.9.13	Интерфейси	1 x RJ-45 (вход за LAN кабел) 3 x USB 2.0 3.5 мм комбо аудио порт за слушалки и микрофон 1 x Line-out (изход за слушалки) 1 x M.2 2230 разширителен слот (Wi-Fi Card) 2 x DisplayPort 1.4 1 x PCI Express 4.0 x 16

		2 x USB 3.2 Gen 2 Type-C 1 x Line-in 1 x PCI Express 5.0 x 16 2 x M.2 2280 NVMe PCIe 4.0 x4 1 x M.2 2280 NVMe PCIe 5.0 x4 6 x USB 3.2 Gen 2 2 x PCI Express 4.0 x 4
T.9.14	Операционна система	MS Windows 11 Professional или по-висока версия, 64-bit, English, OEM, операционна система (ОС), предварително инсталирана с лиценз, позволяващ преинсталирането и/или надграждането ѝ.
T.9.15	Софтуер	MS Office 2021 или по-нова, с ключ за активиране.
T.9.16	Гаранция	Не по-малко от 36 месеца

10. ДИСПЛЕИ

№	Параметър	Минимални технически изисквания
T.10.1	Диagonal на дисплея	27" 16:9
T.10.2	Разделителна способност	2560 x 1440
T.10.3	Тип на матрицата	IPS
T.10.4	Ъгъл на видимост	• 178/178
T.10.5	Честота на опресняване	144 Hz -> HDMI, 165 Hz -> DisplayPort
T.10.6	Интерфейси	2 x HDMI 2.0, 1 x DisplayPort 1.4, 1 x Audio Out
T.10.7	Стойка	С възможност за позициониране на ъгъла на наклон напред, назад и регулиране по височина
T.10.8	Големина на пиксела	0.230 mm
T.10.9	Покритие на дисплея	Матово
T.10.10	Гаранция	Не по-малко от 36 месеца

11. ПРЕНОСИМИ КОМПЮТРИ ТИП1

№	Параметър	Минимални технически изисквания
T.11.1	Тип система	laptop
T.11.2	Процесор	Десетядрен Intel Core 7 150U (1.2 - 5.4 GHz, 12 MB cache), еквивалентен или по-добър
T.11.3	Оперативна памет	32 GB DDR5 5600
T.11.4	Графика	Допълнителна видео карта
T.11.5	Дискова памет	1 TB M.2 NVMe SSD
T.11.6	Сигурност	Четец на пръстови отпечатьци (Finger Print Reader) Kensington Lock
T.11.7	Аудио	Два вградени микрофона Poly Studio говорители Вградени стерео говорители
T.11.8	Комуникация	Мрежа: 10/100/1000 Mbps Безжична свързаност:

		Wi-Fi 6E 802.11ax Bluetooth 5.3
T.11.9	Сертификати	Зелен сертификат ENERGY STAR Зелен сертификат TCO
T.11.10	Захранване	230VAC
T.11.11	Клавиатура	Кирилизирана по БДС (трайно гравирана) Цифрова клавиатура Островен тип клавиатура Подсветка на клавиатурата Устойчива на разливане клавиатура Copilot бутон
T.11.12	Мишка	Bluetooth– включена в доставката
T.11.13	Интерфейси	2 x USB 3.2 Gen 1 захранващ порт 1 x HDMI 2.1 1 x M.2 2280 NVMe PCIe 4.0 2 x USB 3.2 Gen 2 Type C с DisplayPort функция (захранващ) 3.5 мм комбо жак за микрофон и слушалки 1 x RJ-45 (вход за LAN кабел)
T.11.14	Допълнителни функции	Multi-Touch Touchpad с поддръжка на жестове Технология за бързо зареждане на батерията
T.11.15	Камера	Full HD веб-камера Плъзгащ се протектор, покриващ камерата
T.11.16	Батерия	3-клетъчна, литиево-йонна батерия, 53 Wh
T.11.17	Мощност на захранващия адаптер	45 W
T.11.18	Тегло	1.75 кг
T.11.19	Операционна система	MS Windows 11 Professional или по-висока версия, 64-bit, English, OEM, операционна система (ОС), предварително инсталирана с лиценз, позволяващ преинсталирането и/или надграждането ѝ.
T.11.20	Софтуер	MS Office 2021 или по-нова, с ключ за активиране.
T.11.21	Окомплектовка	Раница, включена в доставката Раницата да е от същия производител като на лаптопа Раницата да е водозащитена Да има мин. 4 джоба с цип
T.11.22	Гаранция	Не по-малко от 36 месеца

12. ПРЕНОСИМИ КОМПЮТРИ ТИП2

№	Параметър	Минимални технически изисквания
T.12.1	Тип система	laptop
T.12.2	Процесор	Двадесетядрен Intel Core Ultra 7 265HX (2.30 - 5.30 GHz, 36 MB cache), еквивалентен или по-добър
T.12.3	Оперативна памет	32 GB DDR5 5600
T.12.4	Графика	Допълнителна видео карта 6GB GDDR7

T.12.5	Дискова памет	1 TB M.2 NVMe SSD
T.12.6	Сигурност	Kensington Nano Lock
T.12.7	Аудио	Два вградени микрофона Poly Studio говорители Вградени стерео говорители
T.12.8	Комуникация	Мрежа: 10/100/1000 Mbps Безжична свързаност: Wi-Fi 7 802.11be Bluetooth 5.4
T.12.9	Сертификати	Зелен сертификат ENERGY STAR Зелен сертификат TCO
T.12.10	Захранване	230VAC
T.12.11	Клавиатура	Кирилизирана по БДС (трайно гравирана) Цифрова клавиатура Островен тип клавиатура Подсветка на клавиатурата Устойчива на разливане клавиатура Copilot бутон
T.12.12	Мишка	Bluetooth– включена в доставката
T.12.13	Интерфейси	1 x USB 3.2 Gen 1 1 x USB 3.2 Gen 1 захранващ порт 1 x HDMI 2.1 2 x M.2 2280 NVMe PCIe 4.0 2 x USB 4 Type C / Thunderbolt 4 захранващ 3.5 мм комбо жак за микрофон и слушалки 1 x RJ-45 (вход за LAN кабел)
T.12.14	Допълнителни функции	Термичен IR сензор Сензор за светлина Сензор за цветово възприемане
T.12.15	Камера	5 MP уеб-камера IR уеб-камера за лицево разпознаване Плъзгащ се протектор, покриващ камерата
T.12.16	Батерия	6-клетъчна, литиево-полимерна батерия, 83 Wh
T.12.17	Мощност на захранващия адаптер	150 W
T.12.18	Тегло	<= 2.1 кг
T.12.19	Операционна система	MS Windows 11 Professional или по-висока версия, 64-bit, English, OEM, операционна система (ОС), предварително инсталирана с лиценз, позволяващ преинсталирането и/или надграждането ѝ.
T.12.20	Софтуер	MS Office 2021 или по-нова, с ключ за активиране.
T.12.21	Окомплектовка	Раница, включена в доставката Раницата да е от същия производител като на лаптопа Раницата да е водозащитена Да има мин. 4 джоба с цип
T.12.22	Гаранция	Не по-малко от 36 месеца
T.12.23		

13. LAN КОМУТАТОРИ

№	Параметър	Минимални технически изисквания
T.13.1	Процесор	ARM 64bit, 4 ядра/4 нишки, 2208MHz
T.13.2	Операционна система	RouterOS v7 или аналогична
T.13.3	RAM памет	≥ 1GB
T.13.4	Постоянна памет	≥ 128MB
T.13.5	Захранване	2 блока 100-240VAC
T.13.6	Охлаждане	4 вентилатора
T.13.7	Интерфейси	176p. 10/100/1000 Ethernet 2 бр. SFP+ Сериен порт RJ45 USB 3.0 type A
T.13.8	PoE out	8 порта с 802.3af/at
T.13.9	Безжични интерфейси	За 2.4 GHz: WiFi 6, 4 канала, Усилване на антената 5 dBi, поддържани стандарти: 802.11b/g/n/ax За 5 GHz: WiFi 6, 4 канала, Усилване на антената 6 dBi, поддържани стандарти: 802.11a/n/ac/ax
T.13.10	Работна температура	-20°C to 70°C
T.13.11	Вградени датчици	Следена на температурата на процесора, Следене на температурата на дънната платка, Следене на захранващото напрежение и ток
T.13.12	Поддържани логически интерфейси	Bridge, EoIP, Gre, Gre6, IPIP, L2TP, LTE, OVPN, PPP, PPPoE, PPTP, SSTP, VLAN, VPLS, VRRP, Virtual-ethernet или аналогични
T.13.13	Поддържани IP протоколи	ARP, Accounting, Address, Cloud, DHCP Client, DHCP Relay, DHCP Server, DNS, Fasttrack, Firewall, Address list, Connection tracking, Filter,L7, Mangle, NAT, Raw, Hotspot, Profile, User Walled Garden, IPsec, Neighbor discovery, Packing, Pools, Proxy, Route, SMB, SOCKS, SSH, Services Settings, TFTP, Traffic Flow, UPnP
T.13.14	Поддържани IPv6 протоколи	Address,DHCP Client, DHCP Server, Firewall, Address-list Filter, Mangle, ND, Neighbors, Pool, Route
T.13.15	Поддържани рутиращи протоколи	BFD,BGP,IGMP-Proxy,MME,Multicast,OSPF,Prefix list,RIP,Routing filters
T.13.16	Брой активни тунели	Неограничени (PPPoE, PPTP, L2TP, OVPN, EoIP или аналогичен)
T.13.17	RADIUS клиент	Да
T.13.18	Конфигуриране	WEB, TELNET, SSH, Winbox (или аналогичен)
T.13.19	Окомплектовка	кит за монтаж в 19" комуникационен шкаф, 2 бр. захранващи кабели
T.13.20	Гаранция	Не по-малко от 36 месеца

14. НЕПРЕКЪСВАЕМИ ТОКОЗАХРАНВАЩИ УСТРОЙСТВА (UPS)

№	Параметър	Минимални технически изисквания
T.14.1	Изходна мощност	6кVA
T.14.2	Начин на работа	Online double conversion
T.14.3	Входно напрежение	220/230/240V
T.14.4	Изходно напрежение	220V/230V/240V $\pm 2\%$, THDU < 3%
T.14.5	КПД	$\geq 93\%$ при Online mode, $\geq 97\%$ при ECO mode
T.14.6	Ток на късо	$\geq 82A$
T.14.7	Капацитет на претоварване	105%-110% : 5min, 110%-130% : 1min, 130%-150% : 10s, >150% : 100ms
T.14.8	Продължителност на работа на батерии	При товар 50%: ≥ 20 мин При товар 75%: ≥ 12 мин
T.14.9	Комуникация	1USB port + 1 RS232 Мрежова карта IP SNMP – ВКЛЮЧЕНА В ДОСТАВКАТА
T.14.10	Работна температура	0 до 40°C
T.14.11	Ново на шум	<55dB
T.14.12	Сигурност	IEC/EN 62040-1
T.14.13	ЕМС	IEC/EN 62040-2
T.14.14	Сертификати	CE, CB report (TUV)
T.14.15	Гаранция	Не по-малко от 36 месеца

РАЗДЕЛ IV: ИЗИСКВАНИЯ КЪМ ДОКУМЕНТИТЕ, КОИТО СЛЕДВА ДА БЪДАТ ПРЕДСТАВЕНИ КЪМ ТЕХНИЧЕСКОТО ПРЕДЛОЖЕНИЕ

1. Хардуерните компоненти на оборудването да отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа.

2. Оборудването да бъде ново и неупотребявано, доставено в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, където се изискват, както и с необходимата техническа документация (на електронен носител или чрез линкове, от които може да бъде свалена).

РАЗДЕЛ V: ГАРАНЦИОНЕН СРОК И ОБХВАТ НА ТЕХНИЧЕСКАТА ПОДДРЪЖКА

1. ГАРАНЦИОНЕН СРОК

Гаранционният срок на всички хардуерни устройства по Т.5 следва да бъде не по-малко от 5 (пет) години, считано от датата на инсталиране и активиране на устройството.

Участникът да предложи гаранционен срок и гаранционно сервизно обслужване в рамките на гаранционния срок на доставеното оборудване по Т.6 до Т.14, не по-малко от 36 месеца,

считано от датата на приемане на съответното оборудване с подписване на приемо-предавателен протокол за доставка на оборудването.

2. ОБХВАТ НА ТЕХНИЧЕСКАТА ПОДДРЪЖКА ПРЕЗ ГАРАНЦИОННИЯ СРОК

По отношение на системите и решенията по Т.1 до Т.5 изпълнителят трябва да осигури техническа поддръжка в рамките на гаранционния срок в режим 5 /пет/ дни x 8 /осем/ часа седмично в рамките на работното време - от 8:30 до 17:00 часа.

В обхвата на техническата поддръжка се включва:

- При необходимост - Извършване на миграция към по-висока версия на софтуерното оборудване;
- Оказване на техническа помощ и консултации при използване и администриране на предложеното решение при срокове, от подаване на заявка от Възложителя (чрез e-mail или телефон, посочен от ИЗПЪЛНИТЕЛЯ), както следва:

Категория проблем	Срок за реакция	Срок за отстраняване на проблема
Urgent – Критични проблеми, водещи до прекъсване работата на системата/ неработоспособност на системата	1 час	24 часа
High priority – Проблеми с висок приоритет с критично въздействие върху работоспособността и функционалностите на системата	1 час	48 часа
Medium priority – Некритични проблеми, затрудняващи работата на системата, но не водещи до спиране на работата ѝ	4 часа	5 работни дни
Low priority - Маловажни проблеми с несъществено влияние върху работата на системата	1 работен ден	12 работни дни
Отговор на заявки за методическа помощ, техническа помощ, консултации за използване и поддръжка на софтуерното и хардуерно оборудване	1 час	1 работен ден

По отношение на оборудването по Т.5.1.2.1 до Т.5.1.2.20 и Т.6.1 до Т.14.15 изпълнителят се задължава да отстранява за своя сметка и в договорените срокове всички несъответствия и повреди на доставеното оборудване, проявени и/или открити в рамките на гаранционния срок, констатирани и предявени по реда на сключения Договор и съгласно гаранционните условия. Изпълнителят е длъжен при отстраняване на Несъответствия да влага само оригинални или одобрени от производителя резервни части и материали.

В рамките на гаранционния срок Изпълнителят отстранява със свои сили и средства всички повреди и/или Несъответствия на оборудването, съответно подменя дефектирани части, модули или устройства с нови, съгласно гаранционните условия.

Изпълнителят се задължава да отстрани настъпила повреда и/или Несъответствието и възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява на място при Възложителя в ЦУ на „Булгартрансгаз“ ЕАД или сервиз.

Изпълнителят следва да възстановява в работоспособно състояние оборудването в срок до 5 работни дни от получаването на рекламацията за повреда.

При невъзможност за отстраняване на настъпила повреда и/или Несъответствие на оборудване, когато отстраняването на проблема изисква повече от 5 работни дни, Изпълнителят заменя оборудването с ново и прехвърля неговата собственост на възложителя в срок до 5 работни дни след изтичане на срока за отстраняване на повредата.

ИНДИКАТИВНА ОФЕРТА

ОТ

(посочва се наименованието на дружеството, правно организационна форма и ЕИК)

ЗА УЧАСТИЕ В ПАЗАРНИ КОНСУЛТАЦИИ С ЦЕЛ ОПРЕДЕЛЯНЕ ИНДИКАТИВНА СТОЙНОСТ НА ДОСТАВКИТЕ И ДЕЙНОСТИТЕ , ПРЕДМЕТ НА ОБЩЕСТВЕНА ПОРЪЧКА С НАИМЕНОВАНИЕ „ДОСТАВКА, ИНСТАЛИРАНЕ И ПУСКАНЕ В ЕКСПЛОАТАЦИЯ НА ПЛАТФОРМИ И ОБОРУДВАНЕ ЗА ИНФОРМАЦИОННА И КИБЕРСИГУРНОСТ“

УВАЖАЕМИ ДАМИ И ГОСПОДА,

С настоящото представяме нашата индикативна оферта за горепосочените пазарни консултации съобразно изискванията и условията на възложителя, посочени в техническата спецификация към поканата за участие.

1. Предметът на дейност на дружеството е, както следва:

.....

.....

.....

(описва се от участника)

2. Представяме предлаганите от нас индикативни стойности за изпълнение на доставките и дейностите от предмета на горепосочените пазарни консултации в Приложение, изготвено по Образец № 1.1. към настоящата индикативна оферта.

Запознати сме и даваме своето съгласие нашето предложение, представено в резултат от пазарната консултация, да бъде публикувано в профила на купувача в ЦАИС ЕОП, както и в раздел „Профил на купувача“ на електронната страница на „Булгартрансгаз“ ЕАД, съгласно разпоредбите на Закона за обществените поръчки и Правилника за прилагане на Закона за обществените поръчки.

Приложение: Образец № 1.1.

С уважение,

.....

(име, длъжност и подпис)

гр.,2026 г.

Образец № 1.1 и Приложение към Образец № 1

Позиция №	Наименование на позицията с описание на доставките и дейностите	количество	единична цена в евро без ДДС	обща цена в евро без ДДС
1	СИСТЕМА ЗА АНАЛИЗ И ОТКРИВАНЕ НА ЗАПЛАХИ НА БАЗА DNS ТРАФИК (вкл. доставка на системата окомплектована с необходимите софтуерни пакети и лицензи; Инсталиране и активиране на системата; Гаранционна поддръжка на системата), съгласно изискванията на т.1 от раздел III: Технически изисквания от техническата спецификация.	1 бр.		
2	РЕШЕНИЕ ЗА СКАНИРАНЕ НА УЯЗВИМОСТИ (вкл. доставка на решението окомплектовано с необходимите софтуерни пакети и лицензи; инсталиране и активиране на решението; гаранционна поддръжка на решението.), съгласно изискванията на т.2 от раздел III: Технически изисквания от техническата спецификация.	1 бр.		
3	РЕШЕНИЕ ЗА МОНИТОРИРАНЕ И УПРАВЛЕНИЕ НА ПРИВИЛЕГИРОВАННИЯ ДОСТЪП (РАМ) (вкл. доставка на решението окомплектовано с необходимите софтуерни пакети и лицензи; инсталиране и активиране на решението; гаранционна поддръжка на решението), съгласно изискванията на т.3 от раздел III: Технически изисквания от техническата спецификация.	1 бр.		
4	ПЛАТФОРМА ЗА ЦЕНТРАЛИЗИРАНО АВТЕНТИКИРАНЕ (вкл.Доставка на платформата окомплектована с необходимите софтуерни пакети и лицензи; инсталиране и активиране на платформата; гаранционна поддръжка на платформата.), съгласно изискванията на т. 4 от раздел III: Технически изисквания от техническата спецификация.	1 бр.		
5	НАДГРАЖДАНЕ НА ЦЯЛОСТНА СИСТЕМА ОТ ЗАЩИТНИ СТЕНИ	1 бр.		
5.1.	Доставка на защитни стени (NGFW) - хардуерни устройства, с еднакви параметри – модел, версия на Firmware, настройки и спецификация за осигуряване на непрекъсваемост на мрежовата услуга, както и необходимите лицензи за функциониране на цялата надградена система вкл. изискванията и дейностите по т. 5.1.1. и т. 5.1.2. от раздел III: Технически изисквания от техническата спецификация.	6 бр.		

Образец № 1.1 и Приложение към Образец № 1

5.2.	Осигуряване валидна хардуерна и софтуерна поддръжка считано от датата на изтичане на наличната такава до 08.10.2031 г. за наличните устройства, съгласно изискванията на т. 5.1.3.от раздел III: Технически изисквания от техническата спецификация.	42 бр.		
5.3.	техническата спецификация като броят управлявани устройства следва да бъде 100 броя, съгласно изискванията на т. 5.1.4. от раздел III: Технически изисквания от техническата спецификация.	1 бр.		
6	СЪРВЪРИ ТИП1 (вкл. доставка на сървъри, окомплектовани с необходимите стойки и крепежи за монтаж в 19" сървърен шкаф; гаранционно сервизно обслужване), съгласно изискванията на т. 6 от техническата спецификация	4 бр.		
7	СЪРВЪРИ ТИП2 (вкл. доставка на сървъри, окомплектовани с необходимите стойки и крепежи за монтаж в 19" сървърен шкаф; гаранционно сервизно обслужване), съгласно изискванията на т.7 от раздел III: Технически изисквания от техническата спецификация.	24 бр.		
8	KVM КОМУТАТОРИ (вк. доставка на KVM комутатори, окомплектовани с необходимите стойки и крепежи за монтаж в 19" сървърен шкаф; гаранционно сервизно обслужване), съгласно изискванията на т. 8 от раздел III: Технически изисквания от техническата спецификация.	18 бр.		
9	НАСТОЛНИ КОМПЮТРИ (вкл. доставка на компютри, окомплектовани с необходимите кабели, клавиатури и мишки; доставка на дисплеи, окомплектовани с необходимите кабели за връзка с компютрите; инсталиране и активиране на съответните лицензии; гаранционно сервизно обслужване), съгласно изискванията на т. 9 от раздел III: Технически изисквания от техническата спецификация.	100 бр.		
10	ДИСПЛЕИ (вкл. доставка на дисплеи, окомплектовани с необходимите кабели за връзка с компютър; гаранционно сервизно обслужване), съгласно изискванията на т.10 от раздел III: Технически изисквания от техническата спецификация.	100 бр.		

Образец № 1.1 и Приложение към Образец № 1

11	ПРЕНОСИМИ КОМПЮТРИ ТИП1 (вкл. доставка на преносими компютри, окомплектовани с необходимите кабели, мишки и раници; инсталиране и активиране на съответните лицензии; гаранционно сервизно обслужване), съгласно изискванията на т. 11 от раздел III: Технически изисквания от техническата спецификация.	20 бр.		
12	ПРЕНОСИМИ КОМПЮТРИ ТИП2 (вкл. доставка на преносими компютри, окомплектовани с необходимите кабели, мишки и раници; инсталиране и активиране на съответните лицензии; гаранционно сервизно обслужване), съгласно изискванията на т. 12 от раздел III: Технически изисквания от техническата спецификация.	20 бр.		
13	LAN КОМУТАТОРИ (вкл. доставка на LAN комутатори, окомплектовани с необходимите кабели и стоки за монтаж в 19" шкаф; гаранционно сервизно обслужване), съгласно изискванията на т.13 от раздел III: Технически изисквания от техническата спецификация.	60 бр.		
14	НЕПРЕКЪСВАЕМИ ТОКОЗАХРАНВАЩИ УСТРОЙСТВА (UPS) (вкл. доставка на UPS, окомплектовани с необходимите кабели за хранване и комуникация; гаранционно сервизно обслужване), съгласно изискванията на т. 14 от раздел III: Технически изисквания от техническата спецификация.	26 бр.		
15	Обща цена на поръчката (т.1 + т. 2 + т.3 + т.4 + т.5 + т.6 + т.7 + т.8 + т.9 + т. 10 + т. 11 + т.12 + т. 13 + т.14)			

Забележка № 1: Гаранционните срокове, гаранционната поддръжката и гаранционно сервизно обслужване са съобразени с изискванията на техническата спецификация

Забележка № 2: Забележка: В единичната цена за всяка позиция са включени всички относими доставки и дейности, описани в техническата спецификация по съответната позиция, включително доставка, инсталиране, активиране, лицензиране, гаранционна поддръжка, гаранционно сервизно обслужване и всички съпътстващи дейности и окомплектовка.