Конкурстық құжаттамаға
2-қосымша

Конкурстық құжаттамаға сатып алынатын тауарлардың техникалық ерекшелігі

Сатып алудың нөмірі:	№ 17992139-1
Сатып алудың атауы:	Бағдарламалық-аппараттық кешенді сатып алу
Лоттың нөмірі:	№ 88705908-ЗЦП2
Лоттың атауы:	Бағдарламалық-аппараттық кешен
Лоттың сипаттауы:	желілік инфрақұрылымның қауіпсіздігі және қауіпсіздік оқиғалары, оқиғаларды талдау процесін автоматтандыру туралы ақпаратты басқару үшін
Лоттың қысқаша сипаттауы:	
Саны, көлемі:	1
Өлшем бірлігі:	Дана
Жеткізу орны:	591010000, Солтүстік Қазақстан облысы, Петропавл қ. Солтүстік Қазақстан облысы, Петропавл қ. Строительная көшесі, 23
Жеткізу мерзімі:	Шартқа қол қойылған күннен бастап 20 күнтізбелік күн
Функционалдық, техникалық, сапалық және пайдалану мінездемесін сипаттау:	Жеткізілімге FortiGate-51g Forticare premium and FortiGuard Unified Threat Protection (UTP) лицензиясын қоса алғанда, ngfw класты брандмауэрдің бағдарламалық – аппараттық кешені(бұдан әрі мәтін бойынша-ПАК) лицензия іске қосылған сәттен бастап кемінде 12 ай жарамдылық мерзімі бар жыл сайынғы жазылым түрінде енгізілуі тиіс. FortiGate-51g техникалық сипаттамалары: - Firewall Throughput (64-byte UDP): кем дегенде 4 Gbps; - SSL Inspection Throughput: кем дегенде 1.3 Gbps; - Ngfw өткізу қабілеті: кем дегенде 1.25 Gbps - Қауіптен қорғау өнімділігі: кемінде 1.1 Gbps - IPS өткізу қабілеті: кем дегенде 2.25 Gbps - Брандмауэр саясатының саны: кем дегенде 2000 - Бір мезгілде сессиялар саны (TCP): кем дегенде 720 000; - Жаңа қосылымдарды орнату жылдамдығы (TCP): секундына кемінде 85 000; - IPSec VPN өткізу қабілеті: кем дегенде 4.5 Gbps; - Базалық конфигурациядағы виртуалды қауіпсіздік контексттерінің саны: кемінде 5; - Интерфейстер саны: кем дегенде 5x GE RJ45; - USB порттарының саны: кемінде 1; - RJ-45 консоль порты: кемінде 1; - Жергілікті журналдарды сақтауға арналған кірістірілген дискінің болуыкемінде 1x 64 GB SSD. ПАК функционалдығына қойылатын талап: 1) лицензиялау пайдаланушылардың шектеусіз саны үшін жүзеге асырылуы тиіс. 2) FortiGate-51G қауіпсіздік модульдерінің қолтаңбаларының жаңартуларын және өндірушінің серверінен өзекті қауіптердің тізімін үнемі алып отыруы тиіс. 3) кластер түрін құру мүмкіндігі бар кемінде 4 құрылғыны кластерге біріктіруді қолдауы тиіс: суық резервпен(Active/passive), ыстық резервпен(active/active). 4) брандмауэр функционалдығы болуы тиіс, IP-мекенжайлар, порттар және қосымшалар негізінде желілік трафикті сүзу ережелерін жасау мүмкіндігін қамтамасыз етуі тиіс. 5) IPSec/L2TP vpn туннельдерін құру функционалдығы болуы керек. 6) жүктемені теңестіру функционалдығы болуы тиіс. 7) SD-WAN(Software-Defined Wide Area Network, бағдарламалықконфигурацияланатын желі) интеллектуалды трафикті басқару технологиясын қолдауы тиіс. 8) SD-WAN трафикті басқару контроллері қосымша бағдарламалық жасақтаманы орнатусыз және орналастырусыз кіріктірілген болуы керек және тұрақты ақысыз негізде лицензиялануы керек. 9) SD-WAN технологиясы әрбір пакеттің (per-packet Load Balancing) теңгерімдеу функционалдығын қолдауы тиіс. 10) қосымшаларға негізделген трафикті басқару функционалын қолдауы керек. 11) SD-WAN технологиясы пайдаланушыларды сәйкестендіру негізінде трафикті басқару функционалын қолдауы керек. 12) трафиктің өткізу қабілеттілігін басқару функционалдығы болуы керек (traffic shaping). 13) iCAP (Internet Content Adaptation Protocol) хаттамасы бойынша тексерілген

	трафикті талдау және сыртқы жүйелерге беру мүмкіндіктерімен трафиктің SSL инспекциясын қамтамасыз етуге тиіс. 14) трафиктің SSH талдауын(SSH инспекциясы) қамтамасыз етуі керек. 15) IPv4, IPv6 динамикалық бағыттауды қамтамасыз етуі керек. 16) wccp протоколы бойынша жұмыс істей алуы тиіс (сервер режимінде де, клиент режимінде де). 17) WAN қосылымдарын оңтайландыруды қамтамасыз етуі керек. 18) аппараттық жеделдетумен антивирустық қорғауды қамтамасыз етуге тиіс. 19) аппараттық жеделдетілген IPS (Instruction Prevention System) басып кірудің алдын алу функционалдығы болуы керек. 20) танымал іздеу жүйелерінде қауіпсіз іздеу режимін мәжбүрлеп қосуды қамтамасыз етуі тиіс. 21) қосымшаларды бақылау функционалдығы болуы тиіс. 22) web proxy функционалдығы болуы керек. 23) әдепкі бойынша қол жетімді кемінде 5 виртуалды доменнің (бір құрылғының ішінде толық функционалды виртуалды МӘС) болуын қамтамасыз етуі тиіс. 24) трафиктің http(S), SMTP(S), POP3(S), IMAP(S), FTP(S) ішіндегі вирустарды тексере алуы керек. 25) кесте бойынша антивирустық базалардың жаңартуларын автоматты түрде ала алуы тиіс. 26) түріне қарай файлдарды жіберуді бұғаттау мүмкіндігі болуы тиіс. 27) көптеген WAN желілерінің қосылымдарын қолдауы керек. 28) PPPoE және L2TP протоколдарын қолдауы керек. 29) қолдауы керек DHCP "Клиент / Сервер" конфигурациясындағы хаттама. 30) саясатқа негізделген маршруттауды қолдауы керек. 31) rip, OSPF, is-IS, BGP хаттамаларына негізделген динамикалық маршруттауды қолдауы керек. 32) қауіпсіздік аймақтарын пайдалануды қолдауы тиіс. 33) аймақтар арасындағы маршруттауды қолдауы керек. 34) виртуалды желілер (VLAN) арасындағы маршруттауды қолдауы керек. 35) рөлдерге негізделген әкімшілендіруді қолдауы керек. 36) әкімшілер мен пайдаланушылардың бірнеше деңгейлерін қолдауы керек. 37) TFTP/FTP/SCP протоколы және веб-интерфейс арқылы ендірілген бағдарламалық жасақтаманы жаңартуды қолдауы керек. 38) ендірілген бағдарламалық жасақтаманың алдыңғы күйіне (нұсқасына) оралу мүмкіндігін қолдауы тиіс. 39) Ішкі деректер базасы арқылы пайдаланушылардың аутентификациясын қолдауы тиіс. 40) Kerberos протоколы арқылы пайдаланушылардың аутентификациясын қолдауы керек. 41) Windows Active Directory арқылы пайдаланушылардың аутентификациясын қолдауы керек, бұл ретте доменге қосылған Windows 7 және одан жоғары операциялық жүйелердің пайдаланушыларының аутентификациясы қосымша пароль сұрау рәсімдерінсіз автоматты түрде орындалуы тиіс. 42) IP/MAC мекенжайын байланыстыру арқылы пайдаланушылардың аутентификациясын қолдауы керек. 43) пайдаланушы топтары негізінде аутентификацияны қолдауы керек. 44) Nat, Pat, "мөлдір" (көпір) функцияларын қолдауы керек; саясатқа негізделген NAT функциялары; VLAN Tagging функциялары (802.1 Q); SIP/H. 323 NAT Traversal функциялары. 45) қауіпсіздік профильдерін орнатуды қолдауы керек. 46) URL/кілт сөз/сөз тіркесі бойынша бұғаттау мүмкіндігі болуы тиіс. 47) желілік шабуылдардың кем дегенде 10000 түрін болдырмауы керек. 48) шабуыл қолтаңбаларының тізімін теңшеу мүмкіндігі болуы тиіс. 49) IPS шабуылдар мен қолтаңбалар базасын автоматты түрде жаңартуды қолдауы керек. 50) қашықтағы syslog серверіне журналдарды жіберу мүмкіндігі болуы тиіс. 51) желілік трафикті, жүйенің жай-күйін және анықталған қауіптерді мониторингілеу үшін графикалық құралдары болуға тиіс. 52) вирустар мен желілік шабуылдар туралы электрондық пошта арқылы хабарлама жіберу мүмкіндігі болуы тиіс. 53) "0-day"класындағы белгісіз қауіптерді анықтау үшін sandbox бұлттық қызметіне талдау үшін файлдар мен URL мекенжайларын жіберуді қолдауы тиіс. 54) Cloud sandbox-та талдау үшін жеткізу жиынтығында күніне (24 сағат) кемінде 7200 нысанды (файлдарды және URL мекенжайларын) лицензиялау керек. 55) vrrp протоколын қолдауы керек. 56) SIEM интеграциясын қолдауы керек. 57) кепілдік берілген, ең жоғары немесе басым өткізу қабілетін белгілеу мүмкіндігіне ие болуға тиіс. 58) жедел хабар алмасу қызметтерін анықтауды және пайдалануды бақылауды қолдауы тиіс. 59) WEB интерфейсі арқылы басқаруды қолдауы керек.

	60) орталықтандырылған басқару және есептерді құру жүйелерімен ықпалдасу мүмкіндігіне ие болуға тиіс. 61) NetFlow, sflow протоколдарын қолдауы керек. 62) кері прокси-сервер режимін (reverse prosy) қамтамасыз етуі тиіс. 63) мөлдір прокси-сервер (transparent proxy) режимін қамтамасыз етуі тиіс. 64) командалық жолдан консольдік режимде қауіпсіздік саясатын басқару мүмкіндігін қамтамасыз етуге тиіс. 65) пайдаланушылар туралы ақпаратты, операциялық жүйенің пайдаланылған моделі мен нұсқасын, IP мекенжайын, VFC мекенжайын, анықталған осалдықтар туралы ақпаратты қамтитын телеметрия ақпаратын алу үшін сыртқы жүйелермен интеграцияны қолдауы тиіс. 66) сымсыз кіру нүктелерін басқару мүмкіндігін қамтамасыз етуі тиіс. 67) коммутаторларды басқару мүмкіндігін қамтамасыз етуге тиіс. 68) FortiGate-51G кемінде 12 ай бойы сервистерге жазылуға тиіс: қосымшаларды бақылау; IPS; Antivirus; Web Filtering; DNS Filtering; URL Filtering. 1) әлеуетті өнім беруші жеткізу шеңберінде Пак өндірушісінен Қазақстан Республикасының аумағында орнату, баптау және техникалық қолдау жөніндегі қызметтерді сатуға және көрсетуге құқықтардың болуы туралы ресми авторизациялық хат ұсынуға тиіс. 2) Әлеуетті өнім беруші өндірушіден техникалық қолдау лицензиясы іске қосылған сәттен бастап кемінде 12 ай ішінде істен шыққан жабдықты жөндеуді немесе ауыстыруды қамтамасыз ететін FortiGate-51G моделіне кепілдік қолдауды қамтамасыз етуі тиіс. 3) ПАК жоғары өнімділікті (high performance), қолданыстағы жабдықпен үйлесімділікті және Тапсырыс берушінің қолданыстағы инфрақұрылымымен интеграциялау мүмкіндігін қамтамасыз етуі тиіс. 4) ПАК жаңа, пайдаланылмаған болуы керек. 5) әлеуетті өнім беруші лицензия іске қосылған сәттен бастап кемінде 12 ай ішінде электрондық пошта (email) немесе телефон байланысы арқылы тапсырыс берушіден өтініштерді қабылдау жолымен жұмыс күндері (демалыс және мереке күндерін қоспағанда, дүйсенбіден жұмаға дейін) сағат 08:00-ден 18:00-ге дейін жергілікті техникалық қолдау көрсетуі тиіс, сатып алынған лицензияны іске қосуға көмек, орнату, конфигурациялау, басқару, ПАК ақауларын жою және ақаулықтарды жою мәселелері бойынша кеңес беру. FortiGate-51G бойынша техникалық қолдау мен сервистік қызмет көрсетуге қойылатын талаптар: 1) Жабдық мынадай шарттарда өндірушіден техникалық қолдауды қамтуы тиіс: кемінде 24 сағат, аптасына 7 күн, жылына 365 күн, сыни өтінімдерге жауап беру уақыты бір сағаттан аспайды және сыни емес өтінімдер бойынша келесі жұмыс күні. 2) техникалық қолдау телефон, электрондық пошта(email) және веб-портал арқылы жүзеге асырылуы тиіс. 3) өндірушіден жабдыққа кепілдік лицензия іске қосылған сәттен бастап кемінде 12 ай мерзімге (жазылудың барлық мерзіміне) берілуі тиіс. 4) бұзылған кезде жабдықты ауыстыру мүмкіндігін қамтуы тиіс. 5) жазылымның бүкіл қолданылу мерзімі ішінде ресми веб-портал немесе автоматты жаңарту жүйесі арқылы микробағдарламалардың өзекті нұсқаларын (қолтаңбалы, антивирустық және IPS\IDS-базаларын қоса алғанда) автоматты немесе қолмен жүктеу мүмкіндігі, сондай-ақ өндірушіні қолдау вебпорталы арқылы өтінімдерді жасау және қадағалау мүмкіндігі қамтамасыз етілуге тиіс. Жеткізілетін тауарға кепілдік мерзімі жеткізілген күннен бастап 12 айға белгіленеді.Тауарды дайындау күні 2025 жылдан ерте болмауы тиіс.

Приложение 2
к конкурсной документации

Техническая спецификация закупаемых товаров к конкурсной документации

Номер закупки:	№ 17992139-1
Наименование закупки:	Приобретение программно-аппаратного комплекса
Номер лота:	№ 88705908-ЗЦП2
Наименование лота:	Комплекс программно-аппаратный
Описание лота:	для управления информацией о безопасности и событиях безопасности, автоматизации процесса анализа событий сетевой инфраструктуры
Дополнительное описание лота:	FortiGate-51G Hardware plus 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP)
Количество:	1
Единица измерения:	Штука
Места поставки:	591010000, Северо-Казахстанская область, г.Петропавловск Северо-Казахстанская область, г.Петропавловск Строительная, 23
Срок поставки:	20 календарных дней с даты подписания договора
Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров:	В поставку должен быть включен программно-аппаратный комплекс межсетевого экрана класса NGFW (далее по тексту – ПАК) FortiGate-51G, включая лицензию FortiCare Premium and FortiGuard Unified Threat Protection(UTP) в виде ежегодной подписки со сроком действия не менее 12 месяцев с момента активации лицензии. Технические характеристики FortiGate-51G: - Firewall Throughput (64-byte UDP): не менее 4 Gbps; - SSL Inspection Throughput: не менее 1.3 Gbps; - Пропускная способность NGFW: не менее 1.25 Gbps - Производительность защиты от угроз: не менее 1.1 Gbps - Пропускная способность IPS: не менее 2.25 Gbps - Количество политик брандмауэра: не менее 2000 - Одновременное количество сессий (TCP): не менее 720 000; - Скорость установки новых соединений (TCP): не менее 85 000 в сек; - Пропускная способность IPsec VPN: не менее 4.5 Gbps; - Количество виртуальных контекстов безопасности в базовой комплектации: не менее 5; - Количество интерфейсов: не менее 5x GE RJ45; - Количество USB портов: не менее 1; - Консольный порт RJ-45: не менее 1; - Наличие встроенного диска для локального хранения логов – не менее 1x 64 GB SSD. Требование к функционалу ПАК: 1) Лицензирование должно осуществляться для неограниченного количества пользователей. 2) FortiGate-51G должен регулярно получать обновления сигнатур модулей безопасности и перечень акутальных угроз с сервера производителя. 3) Должен поддерживать объединение в кластер не менее 4 устройств с возможностью создания типа кластеров: с холодным резервом(active/passive), с горячим резервом(active/active). 4) Должен иметь функциональность межсетевого экранирования, обеспечивать возможность создания правил фильтрации сетевого трафика на основе IP-адресов, портов и приложения. 5) Должен иметь функциональность построения IPSec/L2TP VPN туннелей. 6) Должен иметь функциональность балансировки нагрузки. 7) Должен поддерживать технологию интеллектуального управления трафиком SD-WAN(Software-Defined Wide Area Network, программноконфигурируемая сеть). 8) Контроллер управления трафиком SD-WAN должен быть встроенным, без установки и развертывания дополнительного ПО, и лицензироваться на постоянной бесплатной основе. 9) Технология SD-WAN должна поддерживать функционал балансировки каждого пакета (Per-packet Load Balancing). 10) Должен поддерживать функционал управления трафиком на основе приложений. 11) Технология SD-WAN должна поддерживать функционал управления трафиком на основе идентификации пользователей. 12) Должен иметь функциональность управления полосой пропускания трафика (traffic shaping). 13) Должен обеспечивать инспекцию SSL трафика, с возможностями анализа и передачи проинспектированного трафика во внешние системы по протоколу

	ICAP (Internet Content Adaptation Protocol). 14) Должен обеспечивать анализ SSH трафика(SSH inspection). 15) Должен обеспечивать динамическую маршрутизацию IPv4, IPv6. 16) Должен иметь возможность работы по протоколу WCCP (как в режиме сервера, так и в режиме клиента). 17) Должен обеспечивать оптимизацию WAN соединений. 18) Должен обеспечивать антивирусную защиту с аппаратным ускорением. 19) Должен иметь функциональность предотвращения вторжения IPS (Instruction Prevention System) с аппаратным ускорением. 20) Должен обеспечивать принудительное включение режима безопасного поиска в популярных поисковых системах. 21) Должен иметь функциональность контроля приложений. 22) Должен иметь функциональность WEB proxy. 23) Должен обеспечивать наличие не менее 5 виртуальных доменов (полнофункциональных виртуальных МСЭ внутри одного устройства), доступных по умолчанию 24) Должен иметь возможность проверки на наличие вирусов внутри HTTP(S), SMTP(S), POP3(S), IMAP(S), FTP(S) трафика. 25) Должен иметь возможность автоматически по расписанию получать обновления антивирусных баз. 26) Должен иметь возможность блокировки передачи файлов в зависимости от типа. 27) Должен поддерживать соединения множества WAN сетей. 28) Должен поддерживать протоколы PPPoE и L2TP. 29) Должен поддерживать DHCP протокол в конфигурации «Клиент/Сервер». 30) Должен поддерживать маршрутизацию на основе политик. 31) Должен поддерживать динамическую маршрутизацию на основе протоколов RIP, OSPF, IS-IS, BGP. 32) Должен поддерживать использование зон безопасности. 33) Должен поддерживать маршрутизацию между зонами. 34) Должен поддерживать маршрутизацию между виртуальными сетями (VLAN). 35) Должен поддерживать администрирование на основе ролей. 36) Должен поддерживать несколько уровней администраторов и пользователей. 37) Должен поддерживать обновление встроенного ПО через протокол TFTP/FTP/SCP и веб-интерфейс. 38) Должен поддерживать возможность возврата к предыдущему состоянию (версии) встроенного ПО. 39) Должен поддерживать аутентификацию пользователей посредством внутренней базы данных. 40) Должен поддерживать аутентификацию пользователей через протокол Kerberos. 41) Должен поддерживать аутентификацию пользователей посредством Windows Active Directory, при этом аутентификация пользователей операционных систем Windows 7 и выше, включенных в домен, должна выполняться автоматически без дополнительных процедур запроса паролей. 42) Должен поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу. 43) Должен поддерживать аутентификацию на основе групп пользователей. 44) Должен поддерживать функции NAT, PAT, «прозрачный» (мост); функции NAT на основе политик; функции VLAN Tagging (802.1Q); функции SIP/H.323 NAT Traversal. 45) Должен поддерживать настройку профилей безопасности. 46) Должен иметь возможность блокировки по URL/ключевому слову/фразе. 47) Должен уметь предотвращать не менее 10000 типов сетевых атак. 48) Должен иметь возможность настройки списка сигнатур атак. 49) Должен поддерживать автоматическое обновление базы атак и сигнатур IPS. 50) Должен иметь возможность отсылки логов на удаленный syslog сервер. 51) Должен иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угроз. 52) Должен иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках. 53) Должен поддерживать отправку файлов и URL на анализ в облачный сервис sandbox для обнаружения неизвестных угроз класса «0-day». 54) Должен иметь лицензирование в комплекте поставки для анализа в cloud sandbox не менее 7200 объектов (файлов и URL) в день (24 часа). 55) Должен поддерживать протокол VRRP. 56) Должен поддерживать интеграцию с SIEM. 57) Должен иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности. 58) Должен поддерживать обнаружение и контроль использования служб мгновенных сообщений. 59) Должен поддерживать управление через Web интерфейс.

	60) Должен иметь возможность интеграции с системами централизованного управления и построения отчетов. 61) Должен поддерживать протоколы NetFlow, sFlow. 62) Должен обеспечивать режим обратного прокси-сервера (reverse prosy). 63) Должен обеспечивать режим прозрачного прокси-сервера (transparent proxy). 64) Должен обеспечивать возможность управления политиками безопасности в консольном режиме из командной строки. 65) Должен поддерживать интеграцию с внешними системами для получения информации телеметрии, включающей информацию о пользователях, используемой модели и версии операционной системы, IP адрес, VFC адрес, информацию об обнаруженных уязвимостях. 66) Должен обеспечивать возможность управления беспроводными точками доступа. 67) Должен обеспечивать возможность управления коммутаторами. 68) FortiGate-51G должен иметь подписки на сервисы в течение не менее 12 месяцев: контроль приложений; IPS; Antivirus; Web Filtering; DNS Filtering; URL Filtering. 1) Потенциальный Поставщик в рамках поставки должен предоставить официальное авторизационное письмо от производителя ПАК о наличии прав на продажу и оказание услуг по установке, настройке и технической поддержке на территории Республики Казахстан. 2) Потенциальный Поставщик должен обеспечить гарантийную поддержку на модель FortiGate-51G, обеспечивающую ремонт или замену вышедшего из строя оборудования в течении не менее 12 месяцев с момента активации лицензии на техническую поддержку от Производителя. 3) ПАК должно обеспечивать высокую производительность (high performance), совместимость с существующим оборудованием и возможность интеграции с существующей инфраструктурой Заказчика. 4) ПАК должен быть новым, не бывшим в употреблении. 5) Потенциальный Поставщик должен оказывать локальную техническую поддержку с 08:00 ч. до 18:00 ч. в рабочие дни (с понедельника по пятницу, за исключением выходных и праздничных дней) путем принятия обращений от Заказчика по электронной почте (email) или телефонной связи в течении не менее 12 месяцев с момента активации лицензии, включающую помощь в активации приобретенной лицензии, консультирование по вопросам, касающимся установки, настройки, администрирования, устранения сбоев и отказов в работе ПАК. Требования к технической поддержке и сервисному обслуживанию по FortiGate-51G: 1) Оборудование должно включать техническую поддержку от производителя на следующих условиях: не менее 24 часа, 7 дней в неделю, 365 дней в году, время ответа не более часа на критичные заявки и на следующий рабочий день по не критичным заявкам. 2) Техническая поддержка должна осуществляться по телефону, по электронной почте(email) и через веб-портал. 3) Гарантия на оборудование от производителя должна быть предоставлена на срок не менее 12 месяцев с момента активации лицензии (на весь срок подписки). 4) Должна включать возможность замены оборудования при поломке. 5) Должна быть обеспечена возможность автоматического или ручного скачивания актуальных версий прошивок (включая сигнатурные, антивирусные и IPS\IDS-базы) через официальный веб-портал или систему автоматического обновления в течение всего срока действия подписки, также возможность создания и отслеживания заявок через веб-портал поддержки Производителя. Гарантийный срок на поставляемый товар устанавливается на 12 месяцев с даты поставки. Дата изготовления товара должна быть не ранее 2025г.