

**Сатып алынатын қызметтердің Техникалық ерекшелігі
(тапсырыс беруші толтырады)**

Тапсырыс берушінің атауы:	"Л.Н.Гумилев атындағы Еуразия ұлттық университеті" коммерциялық емес акционерлік қоғамы
Ұйымдастырушының атауы:	"Л.Н.Гумилев атындағы Еуразия ұлттық университеті" коммерциялық емес акционерлік қоғамы
Конкурстың №:	№ 17831612-1
Конкурстың атауы:	Веб-сайтты қорғау жүйесінің қызметі
Лоттың нөмірі:	№ 81556022-OK2
Лоттың атауы	Қолданбалы дайын бағдарламалық қамтамасыз етуді лицензиялау бойынша қызметтер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	582932.100.000000
Қызметтің атауы:	Қолданбалы дайын бағдарламалық қамтамасыз етуді лицензиялау бойынша қызметтер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептегенде бірлік бағасы:	53663793
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	53663793
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	шарт жасалған сәттен бастап 30 күнтізбелік күн ішінде
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	12
--------------------------------	----

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Техникалық ерекшелік Сайттарды веб-қорғау жүйесін орнату жөніндегі қызметтер (бұдан әрі – WAF). Саны: 1 данадан кем емес. Веб-қосымшаларды қорғау жүйесіне қойылатын функционалдық талаптар 1. WAF қауіпсіздіктің оң (позитивті), сондай-ақ теріс (негативті) модельдерін қолдауы тиіс. 2. Қауіпсіздіктің теріс моделі шабуылдардың белгілі сигнатураларын айқындауы тиіс: мазмұны шабуылдардың белгілі сигнатураларына сәйкес келетін транзакциялар бұғатталуы, ал қалғандарының барлығына рұқсат етілуі тиіс. 3. Қауіпсіздіктің теріс моделі алдын ала бапталған, жан-жақты әрі дәл шабуыл сигнатураларының тізімін қамтуы тиіс. 4. WAF сигнатураларды түрлендіруге немесе қосуға мүмкіндік беруі тиіс. 5. WAF сигнатуралар тізімінің автоматты түрде жаңартылуын қолдай отырып, ең жаңа қатерлерден толық қорғауды қамтамасыз етуі тиіс. 6. Қауіпсіздіктің теріс моделі белгілі шабуылдарды бірнеше деңгейде, оның ішінде желі, операциялық жүйе, веб-сервердің бағдарламалық қамтылымы және қосымшалар деңгейінде анықтауға мүмкіндік беруі тиіс. 7. Қауіпсіздіктің оң моделі белгілі нәрсенің бәріне рұқсат етілетінін, ал қалғанының бұғатталатынын көздеуі тиіс. 8. Қауіпсіздіктің оң моделі URL-мекенжайларды, каталогтарды, параметрлері бар форма өрістерін және HTTP әдістерін қамтуы тиіс. 9. Қауіпсіздіктің оң моделін баптаудың еңбек сыйымдылығын төмендету мақсатында WAF веб-қосымшаның құрылымын және оның элементтерін автоматты түрде зерделеу тетігіне ие болуы тиіс. 10. WAF веб-қосымшаның құрылымы мен деректеріндегі ықтимал жоспарланған өзгерістерді ескере отырып, оның қалыпты жұмыс үлгісін үздіксіз әрі автоматты түрде зерделеуді қамтамасыз етуі және сонымен қатар нормадан ауытқуларды белсенді түрде бұғаттауды қамтамасыз етуі тиіс. 11. Енгізу формалары өрістері параметрлерінің қолайлы мәндері профильге жазылуы тиіс; жазылған параметр мәндері қауіпсіздіктің оң моделінде сұраныстардың заңдылығын тексеру өлшемшарттары ретінде пайдаланылуы тиіс. 12. Оқыту режимі қосымшаның құрылымы мен элементтерінің (каталогтардың, URL-беттердің, параметрлердің) және пайдаланушының күтілетін мінез-құлқының (параметр мәндерінің өзгеру ауқымы, қолайлы таңбалар, параметрдің клиент тарапынан оқуға немесе өңдеуге арналуы, параметрдің міндеттілігі немесе міндетті еместігі) моделін құру үшін, яғни қауіпсіздіктің оң моделін баптауды автоматтандыру үшін қызмет етуі тиіс. 13. Әкімшінің профиль конфигурациясын қолмен өзгерту мүмкіндігі көзделуі тиіс. 14. Қосымша моделін автоматты түрде құру (оқыту) тетігі профильдегі осал тұстарды анықтап, оны оңтайландыру үшін тиісті шараларды (өзгерістерді) ұсынуы тиіс, мысалы динамикалық URL мекенжайларын үлгі үшін түсінікті URL мекенжайларына түрлендіру. 15. WAF қандай да бір бағдарламалау тілін қолдануды талап етпей, интуитивті түсінікті графикалық интерфейс арқылы күрделі қауіпсіздік саясаттарын құру мүмкіндігін қамтамасыз етуі тиіс. 16. WAF пайдаланушылардың сұраныстарын географиялық белгісі бойынша анықтап, оларға рұқсат беруі/бұғаттауы тиіс. 17. WAF қосымшалардың бағдарламалық
--	---

интерфейстерін (Application Programming Interfaces, API) қорғауды қамтамасыз етуі тиіс. 18. WAF Man-in-the-Browser түріндегі шабуылдарды орындау үшін пайдаланылатын алаяқтық бағдарламалардың жұмысын анықтауы тиіс. 19. WAF деректерді сол өндірушінің бұлттық құм жәшігіне талдауға жіберуді қолдауы тиіс, бұл ретте лицензияға кіретін көлем минутына кемінде 40 объектіні, бірақ тәулігіне 57 600-ден аспайтын көлемді құрауы тиіс. 20. WAF боттар мен заңды пайдаланушыларды ажыратуы тиіс. 21. WAF сұраныстардың IP-беделін анықтауы тиіс. 22. WAF HTTP RFC талаптарына сәйкестігін тексеруі тиіс. 23. WAF WebSocket қорғауын қамтамасыз етуі тиіс. 24. WAF заңды сұраныстарды зиянды сұраныстардан ажырату үшін қауіпсіздік оқиғаларын өзара байланыстыра (корреляциялай) білуі тиіс. 25. WAF жүйедегі қателер және кодты өңдеу қателері туралы өзінің жеке хабарламаларын қолдауы тиіс. 26. WAF операциялық жүйеге ену сигнатураларына ие болуы тиіс. 27. WAF HTTP-сығу функциясын қолдауы тиіс. 28. WAF CAPTCHA және Real Browser Enforcement аутентификациясы функцияларын қолдауы тиіс. 29. WAF пайдаланушылық қауіпсіздік ережелерін (саясаттарын) қолдауы тиіс: әкімшілерде қауіпсіздіктің оң моделі үшін де, теріс моделі үшін де саясаттар құруға, сондай-ақ бірнеше өлшемшарттан тұратын корреляциялық ережелер жасауға мүмкіндік болуы тиіс. 30. Прокси ретінде (мәлдір прокси немесе кері прокси) орналастырылған кезде WAF cookie-дің цифрлық қолтаңбасын, cookie-ді шифрлауды және URL-ді қайта жазуды қолдауы тиіс. 31. WAF виртуалды патчтар жасау мақсатында қосымшалардың осалдық сканерлерімен интеграциялау интерфейсіне ие болуы тиіс. 32. WAF OWASP Top 10 тізімінде көрсетілген веб-қосымшалардың осалдықтарын жоюы тиіс. 33. WAF-ты лицензиялау қорғалатын веб-қосымшалардың шектеусіз саны үшін жүзеге асырылуы тиіс. 34. Пайдаланушылардың қорғалатын веб-серверлерге жолдайтын сұраныстарының және қорғалатын веб-серверлер жауаптарының түрлі өлшемшарттары негізінде өз ережелерін айқындау мүмкіндігі қолдау табуы тиіс. 35. WAF веб-қосымшалардың осалдықтарын анықтайтын кірістірілген сканерге ие болуы тиіс. 36. WAF анықталған осалдықтарды жою үшін ережелерді автоматты түрде генерациялау мүмкіндігімен веб-қосымшалардың осалдықтарын анықтайтын үшінші тарап сканерлерімен интеграциялауды қолдауы тиіс. 37. WAF автоматты профильдеуді, яғни пайдаланушылардың қорғалатын веб-қосымшамен өзара әрекеттесу мәнмәтіні мен параметрлерін көрсететін профильді генерациялауды қолдауы тиіс. 38. WAF «brute force» түріндегі шабуылдардан (веб-қосымшаға кіру паролін іріктеу шабуылдарынан) қорғауды қамтамасыз етуі тиіс. 39. WAF «defacement» түріндегі шабуылдардан (веб-сайт контентін ауыстыруға бағытталған шабуылдардан) қорғауды қамтамасыз етуі тиіс. 40. WAF «қызмет көрсетуден бас тарту» түріндегі шабуылдардан қорғауды қамтамасыз етуі тиіс. 41. WAF HTTPS-қосылымдарды жүйенің терминациялауын қолдап, веб-қосымшаны SSL/TLS функцияларынан босатуы тиіс. 42. WAF HTTPS-қосылымдарды желіні пассивті мониторингтеу режимінде бақылауды қолдауы тиіс. 43. WAF

	клиенттік сұраныстағы SNI өрісінің мәніне байланысты бір қорғалатын мекенжайға бірнеше сертификат берілуін қолдауы тиіс. 44. WAF өндірушінің серверінен қауіпсіздік модульдері сигнатураларының жаңартуларын және өзекті қатерлердің тізбесін тұрақты түрде алып тұруы тиіс. 45. WAF жүктемені теңгерімдеу функционалына ие болуы тиіс. 46. WAF деректердің таралып кетуінен қорғау (DLP) функционалына ие болуы тиіс. 47. WAF веб-серверге жүктелетін файлдарды антивирустық сканерлеуді қолдауы тиіс. 48. WAF әдепкі қалпы бойынша қолжетімді әкімшілік домендердің (әкімшілер топтары бойынша қолжетімділігі бөлінген тәуелсіз саясаттар жиынтығының) болуын қолдауы тиіс. 49. WAF антивирустық базалардың жаңартуларын кесте бойынша автоматты түрде алу мүмкіндігіне ие болуы тиіс. 50. WAF рөлдерге негізделген әкімшілендіруді қолдауы тиіс. 51. WAF кірістірілген БҚ-ны TFTP хаттамасы және веб-интерфейс арқылы жаңартуды қолдауы тиіс. 52. WAF пайдаланушыларды ішкі деректер базасы арқылы аутентификациялауды қолдауы тиіс. 53. WAF пайдаланушыларды Windows Active Directory арқылы аутентификациялауды қолдауы тиіс. Бұл ретте доменге қосылған Windows 7 және одан жоғары операциялық жүйе пайдаланушыларының аутентификациясы қосымша пароль сұрау рәсімдерінсіз автоматты түрде орындалуы тиіс. 54. WAF веб-қосымша пайдаланушыларын RADIUS, LDAP, Kerberos хаттамалары бойынша аутентификациялауды қолдауы тиіс. 55. WAF пайдаланушылар топтары негізінде аутентификациялауды қолдауы тиіс. 56. WAF HTTP хаттамасы шеңберінде түрлі авторизация әдістерін, оның ішінде HTTP Basic әдісін қолдауы тиіс. 57. WAF VLAN Tagging (802.1Q) функцияларын қолдауы тиіс. 58. WAF «қара/ақ» IP-мекенжайлар тізімдері бойынша сүзгілеуді қолдауы тиіс. 59. WAF журнал жазбаларын қашықтағы syslog-серверге жіберу мүмкіндігіне ие болуы тиіс. 60. WAF желілік трафикті, жүйенің күйін және анықталған қатерлерді мониторингтеуге арналған графикалық құралдарға ие болуы тиіс. 61. WAF вирустар мен желілік шабуылдар туралы хабарламаларды электрондық пошта арқылы жіберу мүмкіндігіне ие болуы тиіс. 62. WAF қауіпсіздік оқиғаларын жинау және талдаудың сыртқы жүйелерімен интеграциялауды қолдауы тиіс. 63. WAF өткізу қабілетін және веб-ресурстарға қол жеткізу жылдамдығын оңтайландыру үшін веб-контентті жергілікті кэштеу мүмкіндігін қолдауы тиіс. 64. WAF графикалық басқару интерфейсінде талдау және диагностика жүргізу үшін трафик көшірмесін ұстап алу мүмкіндігін қолдауы тиіс. 65. WAF орталықтандырылған басқару және есептілік құру жүйелерімен интеграциялану мүмкіндігіне ие болуы тиіс. 66. WAF қауіпсіздік саясаттарын командалық жол интерфейсінде басқару мүмкіндігін қолдауы тиіс. 67. WAF мынадай веб-сервистерді қорғау мүмкіндігін қолдауы тиіс: Apache Tomcat, nginx, Microsoft IIS, JBoss, IBM Lotus Domino, Microsoft SharePoint, Microsoft Outlook Web App (OWA), RPC және ActiveSync – Microsoft Exchange Server үшін, Joomla, WordPress. 68. WAF жұмыстың пассивті және белсенді режимдерін қолдауы тиіс. Пассивті режимде WAF әкімшіге шабуылдар туралы, сервер
--	--

	жұмысындағы қателер туралы және басқа да рұқсатсыз әрекеттер туралы хабарламаларды қарауға мүмкіндік беруі, сондай-ақ осы әрекет үшін таңдалған порт арқылы TCP RST пакетін жіберу жолымен зиянды сұраныстарды бұғаттауы тиіс. Белсенді режимде WAF шабуылдарды нақты уақыт режимінде бұғаттау мүмкіндігіне ие болуы тиіс. 69. Шабуыл немесе кез келген рұқсатсыз әрекеттер анықталған кезде WAF тиісті шаралар қабылдай алатындай күйде болуы тиіс: нақты сұраныстар мен жауаптарды тастау, тұтас TCP сессияларын, қосымшалардың нақты пайдаланушыларынан немесе белгілі бір IP-мекенжайлардан келетін сұраныстарды бұғаттау. Аса қауіпті шабуылдар үшін WAF белгілі бір пайдаланушыдан немесе нақты бір IP-мекенжайдан келетін барлық сұраныстарды берілген уақыт кезеңі ішінде бұғаттай білуі тиіс. 70. WAF in-line нұсқасында мөлдір көпір, кері немесе мөлдір прокси-сервер ретінде, сондай-ақ off-line режимінде сниффер (пассивті желілік монитор) ретінде орналастыру мүмкіндігіне ие болуы тиіс. 71. WAF веб-қосымшалардың өнімділігіне әсер етпеу үшін сызықтық өткізу қабілетіне және миллисекундтың үлестерімен өлшенетін кідіріске ие болуы тиіс. 72. WAF HTTP және HTTPS (SSL) веб-қосымшалар трафигімен жұмыс істей алуы тиіс. 73. SSL веб-қосымшаларын қорғау үшін веб-серверлердің сертификаттарын және жабық/ашық кілт жұптарын WAF жүйесіне импорттау мүмкіндігі көзделуі тиіс. 74. SSL веб-қосымшаларын қорғау үшін WAF клиенттік қосылымдарды терминациялап, олардың шифрын ашуы, трафиктің қауіпсіздік саясаттарына сәйкестігін тексеруі және режимге байланысты веб-серверлермен қосылу кезінде оны қайта шифрлауы тиіс. 75. Көпір және сниффер режимдерінде WAF тексеру үшін SSL-трафиктің шифрын HTTPS-қосылымды терминацияламай және өзгертпей аша білуі тиіс. 76. WAF XML-контенті бар веб-қосымшаларды қорғауға қабілетті болуы тиіс. XML қорғанысы автоматтандырылған оқыту (профильдеу) тетігін пайдалана отырып веб-қосымшаларды қорғауға баламалы болуы тиіс. 77. WAF жоғары қолжетімділік кластерінде (High Availability) жұмыс істеу мүмкіндігін қолдауы тиіс. 78. WAF әкімшілендіруге арналған веб-интерфейске ие болуы тиіс; конфигурация қарапайым әрі интуитивті түсінікті болуы тиіс. 79. WAF мынадай осалдық сканерлерімен интеграциялануы тиіс: Acunetix, HP WebInspect, IBM AppScan, Qualys, IBM QRadar және WhiteHat. 80. WAF қауіпсіздік оқиғаларын басқару жүйелерімен (SIEM) интеграциялануы тиіс: Micro Focus (HPE) ArcSight, IBM QRadar, Azure Event Hub. 81. WAF жаңа буын желіаралық экрандарымен және желілік құм жәшіктерімен интеграциялануы тиіс. 82. WAF жаңа буын желіаралық экранынан карантинге түсетін көздердің IP-мекенжайларын трафикті өңдеу ережелерін одан әрі қолдану үшін алу мүмкіндігіне ие болуы тиіс. 83. WAF жүктелген файлдарды бағалау үшін желілік құм жәшігіне TAR форматында жіберу мақсатында файлдарды жүктеуді шектеу саясатын пайдалану мүмкіндігіне ие болуы тиіс. 84. WAF желілік құм жәшігі файлды қатер деп айқындаған жағдайда, оны жүктеуді бұғаттау мүмкіндігіне ие болуы тиіс. 85. WAF HTTP-трафикті, оның ішінде
--	---

	HTTP-тақырыптарды, форма өрістерін және берілетін деректерді тексеруді әрі бақылауды; HTTP-сұраныстар мен жауаптарды тексеруді; деректерді кейіннен тексеру мақсатында мәтіндік түрде ұсыну үшін декодтауды; URL, формаларды, cookie, сұраныс жолдарын, жасырын өрістер мен параметрлерді, HTTP әдістерін, XML-элементтерді тексеруді қолдауы тиіс. 86. WAF оқиғалар туралы есепті стандартты тетіктердің көмегімен, мысалы, жүйелік журналға немесе SNMP арқылы қалыптастыру мүмкіндігіне ие болуы тиіс. 87. Журнал жүргізу деңгейлері мен сүзгілерді әкімші белгілеуі тиіс. 88. WAF кестелік немесе алдын ала айқындалған графикалық есептерді қалыптастыра алуы тиіс. 89. WAF басқару интерфейсінде оның күйі және веб-белсенділігі туралы хабардар ететін графикалық панель болуы тиіс. 90. WAF мынадай орналастыру нұсқаларын қолдауы тиіс: кері прокси-сервер (Reverse Proxy), мөлдір көпір (Transparent Bridge), желіні пассивті мониторингтеу (Offline Sniffing), WCCP клиенті (контентті қайта бағыттау режимі). 91. Кері прокси-сервер режимінде WAF HTTP/HTTPS-қосылымдарды терминациялауы, веб-серверлер мен пайдаланушылардың арасында орналасуы және веб-сервердің ішкі мекенжайын пайдаланушылар оған жүгінетін сыртқы мекенжайға статикалық түрлендіруді жүзеге асыруы тиіс. 92. Мөлдір көпір режимінде WAF HTTP/HTTPS-қосылымдарды терминацияламауы тиіс: қорғалатын веб-серверлерге бағытталған барлық трафик WAF арқылы өтіп, тексерілуі тиіс, зиянды трафик бұғатталуы, қалған трафик мөлдір түрде өтуі тиіс. 93. Желіні пассивті мониторингтеу режимінде WAF коммутатордың SPAN-портына немесе Tap Ethernet құрылғысына қосылуы, қауіпсіздік оқиғаларын пассивті түрде қадағалауы және олар туралы хабардар етуі тиіс, ал қорғау ережелерінің бұзылуы анықталған кезде TCP-сессияны серверге TCP Reset командасын жіберу жолымен тастауы тиіс. 94. Контентті қайта бағыттау режимінде WAF веб-кэш деректерімен алмасу хаттамасының (WCCP) клиенті ретінде әрекет етуі тиіс, бұл WCCP сервері ретінде бапталған желіаралық экранға HTTP және HTTPS трафигін тексеру үшін WAF жүйесіне қайта бағыттауға мүмкіндік береді. Веб-қосымшаларды қорғау жүйесіне қойылатын техникалық талаптар – Орындалуы: виртуалды бағдарламалық өнім (Virtual Appliance), мынадай виртуалдандыру жүйелерінде орнату мүмкіндігімен: VMware, Microsoft Hyper-V, KVM, Citrix XenServer, Open Source Xen, VirtualBox. – Жария бұлттарда орнату мүмкіндігі: Oracle Cloud, Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure. – Жүйенің веб-трафик бойынша өнімділігі: кемінде 3 Гбит/с. – Көлемі 2 ТБ-қа дейінгі қатты дискіні қолдау. – Жедел жадты бөлу бойынша шектеулердің болмауы. – Қолдау көрсетілетін виртуалды ядролардың ең көп саны (vCPU): кемінде 8. – SSL/TLS өңдеу бағдарламалық құралдармен жүзеге асырылуы тиіс. Кепілдікке қойылатын талаптар – Веб-қосымшаларды қорғау кешенінің бағдарламалық қамтылымы өндірушінің 24x7 режиміндегі кеңейтілген кепілдігімен кемінде 12 ай мерзімге қамтамасыз етілуі тиіс. – Қызметтер көрсету кезінде жиынтықта қолданылу мерзімі кемінде 12
--	--

ай болатын сервистерге жазылымдар болуы тиіс: Антивирус, IP-мекенжайлардың беделі, Бұлттық құм жәшігі, Есептік деректерді қорғау сервисі. – Өндірушінің бағдарламалық қамтылымға беретін кепілдік мерзімі – кемінде 12 ай. – Өнім беруші бағдарламалық қамтылымға лицензияларды Тапсырыс берушінің атына беруі және растайтын құжаттарды ұсынуы тиіс. Кепілдік міндеттемелер бойынша жүйені баптауға қойылатын талаптар – Жүйе істен шыққан кезде Өнім беруші тарапынан жұмыс күндері сағат 09:00-ден 18:00-ге дейін (5х9 режимінде) кемінде 12 ай мерзімге баптау қамтамасыз етілуі тиіс. – Өнім беруші Тапсырыс берушінің жауапты маманымен келісе отырып, веб-қосымшаларды қорғау жүйесін баптауды орындауы тиіс, ол жұмыстардың мынадай түрлерін қамтуы тиіс: – Жүйенің ағымдағы конфигурациясының жұмыс істеуін (жұмысқа қабілеттілігін, өнімділігін және баптаулардың дұрыстығын) диагностикалау. – Тапсырыс берушінің қызметкерлеріне жүйенің ағымдағы конфигурациясы, оңтайландырылуы және компоненттерін баптау бойынша консультация беру. – Аталған компоненттермен проблемалар туындаған жағдайда WAF қауіпсіздік саясаттары мен ережелерін оңтайландыру бойынша консультация беру. – Жүйенің және қауіпсіздік компоненттерінің (сигнатуралардың, антивирустық базалардың) жаңа жаңартуларын орнату бойынша консультация беру. – Консультация беру электрондық пошта немесе телефон байланысы арқылы жүзеге асырылады. – Тапсырыс берушінің қызметкерлеріне консультацияны ұқсас жүйелерді сүйемелдеу және енгізу бойынша тиісті тәжірибесі бар Өнім берушінің мамандары жүзеге асырады. – Виртуалды платформаны және оған бөлінген ресурстарды (vCPU, жедел жад, дискілік кеңістік) диагностикалау. – Жүйенің барлық модульдерінің жұмыс істеуін диагностикалау. – Конфигурациялық файлдардың сақтық көшірмесін жасау. – Ақпараттық қауіпсіздіктің қандай оқиғалары ақпараттық қауіпсіздік оқиғалары мен ақпаратын мониторингтеу жүйесіне жіберілуі тиіс екенін Тапсырыс берушімен бірлесіп айқындау. – Тапсырыс берушінің өтінімдері бойынша Жүйе компоненттерін баптау. – Тапсырыс берушінің талабы бойынша Өнім беруші маманының Тапсырыс берушінің аумағына баруы: – Маманның баруы проблеманы шешу немесе жұмыстарды орындау электрондық пошта немесе телефон байланысы арқылы мүмкін болмаған жағдайларда жүзеге асырылады. – Маманның баруы Тапсырыс берушінің тиісті талабын алған сәттен бастап 2 (екі) жұмыс күнінен аспайтын мерзімде жүзеге асырылады. – Маманның баруы техникалық қолдау көрсету шеңберінде Тапсырыс беруші тарапынан қосымша ақы төлеусіз жүзеге асырылады. Қызмет көрсету мерзімі мен орнына қойылатын талаптар – Қызметтер көрсету кезінде Өнім беруші бағдарламалық қамтылымды жеткізуді жүзеге асыруға, сондай-ақ оны баптау жөніндегі қызметтерді толық көлемде Шартқа қол қойылған күннен бастап 30 (отыз) күнтізбелік күннен аспайтын мерзімде орындауға міндетті. – Қызметтер көрсету орны: Астана қ., Қаныш Сәтбаев көшесі, 2. – Қызметтер көрсету кезінде бағдарламалық қамтылымды жеткізу осы техникалық ерекшелікте көрсетілген толық көлемде және мерзімде

	жүзеге асырылуы тиіс. Ұсынылған жабдықтың барлық сипаттамалары осы техникалық ерекшелікте көрсетілген ең төменгі техникалық сипаттамаларға сәйкес келуі немесе олардан асып түсуі тиіс. Өнім берушіге қойылатын қосымша талаптар: - жұмыстарды орындау басталғанға дейін Еңбекті қорғау және өндірістік бақылау қызметінде кіріспе нұсқамадан өту; - Еңбекті қорғау және өндірістік бақылау қызметінің рұқсатын алу; - Қазақстан Республикасы Еңбек кодексінің талаптарын, еңбекті қорғау, өрт қауіпсіздігі, электр қауіпсіздігі қағидаларын және санитариялық нормаларды сақтау; - мердігер ұйымның ұсынуы: - жұмыстарды орындауға тартылатын қызметкерлердің тізімдері; - қызметкерлердің мердігер ұйыммен еңбек қатынастарын растайтын құжаттардың болуы; - міндетті медициналық тексеруден өткені туралы құжаттардың болуы (заңнамада көзделген жағдайларда); - еңбекті қорғау, электр қауіпсіздігі және өзге де қауіпсіздік түрлері бойынша куәліктің, білімді тексеру хаттамаларының және рұқсаттардың болуы; - жұмыстарды қауіпсіз жүргізуге, өрт қауіпсіздігіне және электр қауіпсіздігіне жауапты адамдарды тағайындау туралы бұйрықтардың болуы; - мердігер ұйым қызметкерлерін жеке қорғаныс құралдарымен қамтамасыз ету.
Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	Қызметтер көрсетуге қойылатын талаптар – Әлеуетті өнім берушілер үшін, ол жеңімпаз деп айқындалған жағдайда: жеткізілетін бағдарламалық қамтылым немесе жабдық Қазақстан Республикасының аумағында өндірушінің ресми қолдауында тұрғанын, өндірушінің жүйелерінде тіркелгенін, сондай-ақ Қазақстан Республикасының аумағына өндірушінің немесе оның уәкілетті дистрибьюторларының ресми арналары арқылы әкелінгенін не әкелінетінін растайтын құжаттарды ұсыну міндеті көзделеді. Растама тапсырыс берушінің атауы мен конкурс нөмірі көрсетілген өндірушінің ресми құжаты түрінде ресімделуі тиіс, бұл ретте аталған құжаттар шарт жасалған сәттен бастап 15 күнтізбелік күні ішінде ұсынылуы тиіс – Өнім беруші Тапсырыс берушінің жауапты маманымен келісе отырып, веб-қосымшаларды қорғау кешенінің бағдарламалық қамтылымын толық көлемде орнатуды және баптауды, оның ішінде Тапсырыс берушінің инфрақұрылымында жұмысқа қабілеттілігін тексеруді жүргізуі тиіс. – Өнім беруші веб-қосымшаларды қорғау кешенінің бағдарламалық қамтылымын орналастыруды және баптауды жүргізуі тиіс (таңдалған орналастыру режимін, қауіпсіздік саясаттары мен профильдерін баптау, бағдарламалық қамтылым нұсқасын өзектендіру, Тапсырыс берушінің активтерімен интеграциялау). – Өнім беруші веб-қосымшаларды қорғау жүйесі лицензияларын орнатуды және белсендіруді жүргізуі тиіс. – Өнім беруші Тапсырыс берушіге жеткізілім жиынтығында көрсетілген барлық қауіпсіздік профильдері мен жазылымдардың белсендірілгенін көрсетуі тиіс.

**Техническая спецификация
закупаемых услуг
(заполняется заказчиком)**

Наименование заказчика	Некоммерческое акционерное общество "Евразийский национальный университет имени Л.Н.Гумилева"
Наименование организатора	Некоммерческое акционерное общество "Евразийский национальный университет имени Л.Н.Гумилева"
№ конкурса:	№ 17831612-1
Наименование конкурса:	Услуга системы веб-защиты сайтов
Номер лота:	№ 81556022-ОК2
Наименование лота:	Услуги по лицензированию готового программного обеспечения прикладного
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	582932.100.000000
Наименование услуги:	Услуги по лицензированию готового программного обеспечения прикладного
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	53663793
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	53663793
Срок оказания услуги:	с момента заключения договора в течение 30 календарных дней
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Техническая спецификация Услуг по установке системы веб-защиты сайтов (далее - WAF). Количество: не менее 1 шт. Функциональные требования к системе защиты веб-приложений 1. WAF должен поддерживать как положительную (позитивную), так и отрицательную (негативную) модели безопасности. 2. Отрицательная модель безопасности должна определять известные сигнатуры атак: транзакции, содержимое которых совпадает с известными сигнатурами атак, должны блокироваться, все остальные – разрешаться. 3. Отрицательная модель безопасности должна включать предварительно настроенный всеобъемлющий и точный список сигнатур атак. 4. WAF должен разрешать модификацию или добавление сигнатур. 5. WAF должен поддерживать автоматическое обновление списка сигнатур, обеспечивая полную защиту от новейших угроз. 6. Отрицательная модель безопасности должна позволять обнаруживать известные атаки на нескольких уровнях, в том числе на уровне сети, операционной системы, программного обеспечения веб-сервера и на уровне приложений. 7. Положительная модель безопасности должна предполагать, что разрешено всё известное, а остальное блокируется. 8. Положительная модель безопасности должна включать в себя URL-адреса, каталоги, поля форм с параметрами и методы HTTP. 9. С целью снижения трудоемкости настройки положительной модели безопасности WAF должен обладать механизмом автоматического изучения структуры веб-приложения и его элементов. 10. WAF должен обеспечивать непрерывное автоматическое изучение шаблона нормальной работы веб-приложения с учетом возможных запланированных изменений структуры и данных веб-приложения и в то же время обеспечивать активную блокировку отклонений от нормы. 11. Приемлемые значения параметров полей форм ввода должны записываться в профиль; записанные значения параметров должны использоваться в качестве критериев проверки легитимности запросов в положительной модели безопасности. 12. Режим обучения должен служить для создания модели структуры и элементов приложения (каталогов, URL-страниц, параметров) и ожидаемого поведения пользователя (диапазон изменения значений параметров, приемлемые символы, предназначение параметра для чтения или редактирования клиентом, обязательность или опциональность параметра) для автоматизации настройки положительной модели безопасности. 13. Должна быть предусмотрена возможность изменения конфигурации профиля вручную администратором. 14. Механизм автоматического построения модели приложения (обучения) должен выявлять узкие места в профиле и предлагать соответствующие меры (изменения) для его оптимизации, например преобразование динамических URL в понятные URL для шаблона. 15. WAF должен обеспечивать возможность создания сложных политик безопасности посредством интуитивно понятного графического интерфейса, не требуя применения какого-либо языка программирования. 16. WAF должен обнаруживать и разрешать/блокировать запросы пользователей по географическому признаку. 17. WAF должен обеспечивать защиту программных интерфейсов приложений
---	---

(Application Programming Interfaces, API). 18. WAF должен выявлять работу мошеннических программ, используемых для выполнения атак типа Man-in-the-Browser. 19. WAF должен поддерживать отправку данных на анализ в облачную песочницу от того же производителя, с входящим в лицензию объемом не менее 40 объектов в минуту, но не более 57 600 в день. 20. WAF должен различать ботов и легитимных пользователей. 21. WAF должен определять IP-репутацию запросов. 22. WAF должен проверять соответствие HTTP RFC. 23. WAF должен обеспечивать защиту WebSocket. 24. WAF должен уметь коррелировать события безопасности, чтобы отличать легитимные запросы от вредоносных. 25. WAF должен поддерживать собственные уведомления об ошибках в системе и об ошибках обработки кода. 26. WAF должен иметь сигнатуры вторжения в операционную систему. 27. WAF должен поддерживать функцию HTTP-сжатия. 28. WAF должен поддерживать функции CAPTCHA и Real Browser Enforcement аутентификации. 29. WAF должен поддерживать пользовательские правила (политики) безопасности: у администраторов должна быть возможность создавать политики как для положительной, так и для отрицательной модели безопасности, а также создавать корреляционные правила, содержащие несколько критериев. 30. При развертывании в качестве прокси (прозрачный прокси или обратный прокси) WAF должен поддерживать цифровую подпись cookie, шифрование cookie и перезапись URL. 31. WAF должен обладать интерфейсом интеграции со сканерами уязвимостей приложений с целью создания виртуальных патчей. 32. WAF должен устранять уязвимости веб-приложений, перечисленные в списке OWASP Top 10. 33. Лицензирование WAF должно осуществляться для неограниченного количества защищаемых веб-приложений. 34. Должна поддерживаться возможность определения собственных правил на основе различных критериев запросов пользователей к защищаемым веб-серверам и ответов защищаемых веб-серверов. 35. WAF должен обладать встроенным сканером уязвимостей веб-приложений. 36. WAF должен поддерживать интеграцию со сторонними сканерами уязвимостей веб-приложений с возможностью автоматической генерации правил для устранения выявленных уязвимостей. 37. WAF должен поддерживать автоматическое профилирование, то есть генерацию профиля, отражающего контекст и параметры взаимодействия пользователей с защищаемым веб-приложением. 38. WAF должен обеспечивать защиту от атак типа «brute force» (атак подбора пароля на вход в веб-приложение). 39. WAF должен обеспечивать защиту от атак типа «defacement» (атак, направленных на подмену контента веб-сайта). 40. WAF должен обеспечивать защиту от атак типа «отказ в обслуживании». 41. WAF должен поддерживать терминацию системой HTTPS-соединений с разгрузкой веб-приложения от функций SSL/TLS. 42. WAF должен поддерживать мониторинг HTTPS-соединений в режиме пассивного мониторинга сети. 43. WAF должен поддерживать предоставление нескольких сертификатов на один защищаемый адрес в зависимости от значения поля SNI в клиентском запросе. 44. WAF должен регулярно

	получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя. 45. WAF должен иметь функциональность балансировки нагрузки. 46. WAF должен иметь функционал защиты от утечек данных (DLP). 47. WAF должен поддерживать антивирусное сканирование выгружаемых на веб-сервер файлов. 48. WAF должен поддерживать наличие административных доменов (независимых наборов политик с разделением доступа по группам администраторов), доступных по умолчанию. 49. WAF должен иметь возможность автоматически по расписанию получать обновления антивирусных баз. 50. WAF должен поддерживать администрирование на основе ролей. 51. WAF должен поддерживать обновление встроенного ПО через протокол TFTP и веб-интерфейс. 52. WAF должен поддерживать аутентификацию пользователей посредством внутренней базы данных. 53. WAF 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. 54. WAF должен поддерживать аутентификацию пользователей веб-приложения по протоколам RADIUS, LDAP, Kerberos. 55. WAF должен поддерживать аутентификацию на основе групп пользователей. 56. WAF должен поддерживать различные методы авторизации в рамках протокола HTTP, в том числе HTTP Basic. 57. WAF должен поддерживать функции VLAN Tagging (802.1Q). 58. WAF должен поддерживать фильтрацию по «черным/белым» спискам IP-адресов. 59. WAF должен иметь возможность пересылки записей журналов на удаленный syslog-сервер. 60. WAF должен иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угроз. 61. WAF должен иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках. 62. WAF должен поддерживать интеграцию с внешними системами сбора и анализа событий безопасности. 63. WAF должен поддерживать возможность локального кэширования веб-контента для оптимизации полосы пропускания и скорости доступа к веб-ресурсам. 64. WAF должен поддерживать возможность захвата копии трафика для анализа и диагностики в графическом интерфейсе управления. 65. WAF должен иметь возможность интеграции с системами централизованного управления и построения отчетов. 66. WAF должен поддерживать возможность управления политиками безопасности в интерфейсе командной строки. 67. WAF должен поддерживать возможность защиты следующих веб-сервисов: Apache Tomcat, nginx, Microsoft IIS, JBoss, IBM Lotus Domino, Microsoft SharePoint, Microsoft Outlook Web App (OWA), RPC и ActiveSync для Microsoft Exchange Server, Joomla, WordPress. 68. WAF должен поддерживать пассивный и активный режимы работы. В пассивном режиме WAF должен позволять администратору просматривать уведомления об атаках, об ошибках работы сервера и о других несанкционированных действиях, а также блокировать вредоносные запросы путем отправки пакета TCP RST через выбранный для этого действия порт.
--	--

В активном режиме WAF должен обладать возможностью блокировки атак в режиме реального времени. 69. При обнаружении атаки или любых несанкционированных действий WAF должен быть в состоянии принять соответствующие меры: сбрасывать конкретные запросы и ответы, блокировать целые сессии TCP, запросы от конкретных пользователей приложений или с определенных IP-адресов. Для особо опасных атак WAF должен уметь блокировать все запросы от конкретного пользователя или с конкретного IP-адреса за заданный период времени. 70. WAF должен обладать возможностью развертывания в варианте in-line как прозрачный мост, обратный или прозрачный прокси-сервер, а также в режиме off-line как сниффер (пассивный сетевой монитор). 71. WAF должен обладать линейной пропускной способностью и латентностью в доли миллисекунд, чтобы не оказывать влияния на производительность веб-приложений. 72. WAF должен быть в состоянии работать с HTTP и HTTPS (SSL) трафиком веб-приложений. 73. Для защиты SSL веб-приложений должна быть предусмотрена возможность импорта в WAF сертификатов и пар закрытый/открытый ключ веб-серверов. 74. Для защиты SSL веб-приложений WAF должен терминировать и расшифровывать клиентские соединения, инспектировать трафик на предмет соответствия политикам безопасности и, в зависимости от режима, повторно зашифровывать его при соединениях с веб-серверами. 75. В режимах моста и сниффера WAF должен уметь расшифровывать SSL-трафик для проверки, не терминируя и не изменяя HTTPS-соединение. 76. WAF должен быть способен защищать веб-приложения, содержащие XML-контент. Защита XML должна быть эквивалентна защите веб-приложений с использованием механизма автоматизированного обучения (профилирования). 77. WAF должен поддерживать возможность работы в кластере высокой доступности (High Availability). 78. WAF должен иметь веб-интерфейс для администрирования; конфигурация должна быть простой и интуитивно понятной. 79. WAF должен интегрироваться со сканерами уязвимостей: Acunetix, HP WebInspect, IBM AppScan, Qualys, IBM QRadar и WhiteHat. 80. WAF должен интегрироваться с системами управления событиями безопасности (SIEM): Micro Focus (HPE) ArcSight, IBM QRadar, Azure Event Hub. 81. WAF должен интегрироваться с межсетевыми экранами нового поколения и сетевыми песочницами. 82. WAF должен иметь возможность получать от межсетевого экрана нового поколения IP-адреса источников, подпадающие под карантин, для дальнейшего применения правил обработки трафика. 83. WAF должен иметь возможность использовать политику ограничения загрузки файлов для отправки загруженных файлов в формате TAR в сетевую песочницу для оценки. 84. WAF должен иметь возможность блокировки загрузки файла, если сетевая песочница определяет этот файл как угрозу. 85. WAF должен поддерживать проверку и контроль HTTP-трафика, включая HTTP-заголовки, поля форм и передаваемые данные; проверку HTTP-запросов и ответов; декодирование данных для представления в текстовом виде с целью последующей проверки; проверку URL, форм, cookie,

	строк запроса, скрытых полей и параметров, методов HTTP, XML-элементов. 86. WAF должен обладать возможностью формирования отчета о событиях с помощью стандартных механизмов, например, в системный журнал или через SNMP. 87. Уровни ведения журнала и фильтры должны устанавливаться администратором. 88. WAF должен быть в состоянии формировать табличные или предопределенные графические отчеты. 89. Интерфейс управления WAF должен иметь графическую панель, информирующую о его состоянии и веб-активности. 90. WAF должен поддерживать следующие варианты развертывания: обратный прокси-сервер (Reverse Proxy), прозрачный мост (Transparent Bridge), пассивный мониторинг сети (Offline Sniffing), клиент WCCP (режим перенаправления контента). 91. В режиме обратного прокси-сервера WAF должен терминировать HTTP/HTTPS-соединения, располагаясь между веб-серверами и пользователями и осуществляя статическое преобразование внутреннего адреса веб-сервера во внешний, по которому пользователи обращаются к нему. 92. В режиме прозрачного моста WAF не должен терминировать HTTP/HTTPS-соединения: весь трафик к защищаемым веб-серверам должен проходить через WAF и проверяться, вредоносный трафик должен блокироваться, остальной трафик – проходить прозрачно. 93. В режиме пассивного мониторинга сети WAF должен подключаться к SPAN-порту коммутатора или к устройству Tap Ethernet, пассивно отслеживать и оповещать о событиях безопасности, а при обнаружении нарушений правил защиты – сбрасывать TCP-сессию путем отправки команды TCP Reset серверу. 94. В режиме перенаправления контента WAF должен выступать в качестве клиента протокола обмена данными веб-кэша (WCCP), что позволяет межсетевому экрану, настроенному как сервер WCCP, перенаправлять трафик HTTP и HTTPS в WAF для проверки. Технические требования к системе защиты веб-приложений – Исполнение: виртуальный программный продукт (Virtual Appliance) с возможностью установки в системах виртуализации VMware, Microsoft Hyper-V, KVM, Citrix XenServer, Open Source Xen, VirtualBox. – Возможность установки в публичных облаках: Oracle Cloud, Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure. – Производительность системы по веб-трафику: не менее 3 Гбит/с. – Поддержка жесткого диска размером до 2 ТБ. – Отсутствие ограничений по выделению оперативной памяти. – Максимальное количество поддерживаемых виртуальных ядер (vCPU): не менее 8. – Обработка SSL/TLS должна реализовываться программными средствами. Требования к гарантии – Программное обеспечение комплекса защиты веб-приложений должно обеспечиваться расширенной гарантией от производителя в режиме 24x7 сроком не менее 12 месяцев. – При оказании услуг в комплекте должны быть подписки на сервисы сроком действия не менее 12 месяцев: Антивирус, Репутация IP-адресов, Облачная песочница, Сервис защиты учетных данных. – Срок гарантии программного обеспечения производителем – не менее 12 месяцев. – Поставщик должен предоставить лицензии на программное обеспечение на имя Заказчика и
--	---

	предоставить подтверждающие документы. Требования к настройке системы по гарантийным обязательствам – При сбое системы должна быть обеспечена настройка от Поставщика с 09:00 до 18:00 в рабочие дни (в режиме 5х9) сроком на не менее 12 месяцев. – Поставщик при согласовании с ответственным специалистом Заказчика должен выполнить настройку системы защиты веб-приложений, которая должна включать следующие виды работ: – Диагностика функционирования (работоспособность, производительность и корректность настроек) текущей конфигурации системы. – Консультирование работников Заказчика по текущей конфигурации, оптимизации и настройке компонентов системы. – Консультирование по оптимизации политик и правил безопасности WAF в случае возникновения проблем с данными компонентами. – Консультирование по установке новых обновлений системы и компонентов безопасности (сигнатур, антивирусных баз). – Консультирование осуществляется посредством электронной почты либо телефонной связи. – Консультирование работников Заказчика осуществляется специалистами Поставщика, обладающими соответствующим опытом в сопровождении и внедрении подобных систем. – Диагностика виртуальной платформы и выделенных ей ресурсов (vCPU, оперативная память, дисковое пространство). – Диагностика функционирования всех модулей системы. – Резервное копирование конфигурационных файлов. – Определить совместно с Заказчиком, какие события информационной безопасности должны направляться в систему мониторинга событиями и информации об информационной безопасности. – Настройки компонентов Системы по заявкам Заказчика. – Выезд специалиста Поставщика на территорию Заказчика по требованию Заказчика: – Выезд специалиста осуществляется в случаях, когда решение проблемы или выполнение работ невозможно посредством электронной почты или телефонной связи. – Выезд специалиста осуществляется в срок не более 2 (двух) рабочих дней с момента получения соответствующего требования Заказчика. – Выезд специалиста осуществляется без дополнительной оплаты со стороны Заказчика в рамках оказания технической поддержки. Требования к сроку и месту оказания услуг – При оказании услуг Поставщик обязан осуществить поставку программного обеспечения, а также выполнить услуги по его настройке в полном объеме в срок не более 30 (тридцати) календарных дней со дня подписания Договора. – Место оказания услуг: г.Астана, ул. Каныша Сатпаева, 2. – При оказании услуг поставка программного обеспечения должна быть осуществлена в полном объеме и в сроки, указанные в данной технической спецификации. Все предложенные характеристики оборудования должны соответствовать или превосходить минимальные технические характеристики, указанные в данной технической спецификации. Дополнительные требования к Поставщику: - прохождение вводного инструктажа в Службе охраны труда и производственного контроля до начала выполнения работ; - получению допуска Службы охраны труда и производственного контроля; - соблюдение требований Трудового кодекса Республики Казахстан,
--	---

	правил охраны труда, пожарной безопасности, электробезопасности и санитарных норм; - предоставление подрядной организацией: - списки работников, привлекаемых к выполнению работ; - иметь документы, подтверждающих трудовые отношения работников с подрядной организацией; - иметь документы о прохождении обязательных медицинских осмотров (в предусмотренных законодательством случаях); - иметь удостоверение, протоколы проверки знаний и допусков по охране труда, электробезопасности и иным видам безопасности; - иметь приказы о назначении ответственных лиц за безопасное производство работ, пожарную безопасность и электробезопасность; - обеспечить работников подрядной организации средствами индивидуальной защиты.
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	Требования к оказанию услуг – Для потенциальных поставщиков, в случае определения его победителем: предусматривают обязанность предоставить документы, подтверждающие, что поставляемое программное обеспечение или оборудование находится на официальной поддержке производителя на территории Республики Казахстан, зарегистрировано в системах производителя, а также ввезено либо будет ввезено на территорию Республики Казахстан по официальным каналам производителя или его уполномоченных дистрибьюторов Подтверждение должно быть оформлено в виде официального документа от производителя с указанием наименования заказчика и номера конкурса, при этом указанные документы должны быть предоставлены в течение 15 календарных дней с момента заключения договора – Поставщик при согласовании с ответственным специалистом Заказчика должен произвести установку и настройку программного обеспечения комплекса защиты веб-приложений в полном объеме, включая проверку работоспособности в инфраструктуре Заказчика. – Поставщик должен произвести развертывание и настройку программного обеспечения комплекса защиты веб-приложений (настройку выбранного режима развертывания, политик и профилей безопасности, актуализацию версии программного обеспечения, интеграцию с активами Заказчика). – Поставщик должен произвести установку и активацию лицензий системы защиты веб-приложений. – Поставщик должен произвести демонстрацию Заказчику активированности всех профилей безопасности и подписок, указанных в комплекте поставки.