

**Сатып алынатын тауарлардың техникалық ерекшелігі
(тапсырыс беруші толтырады)**

Тапсырыс берушінің атауы:	"Нұрсұлтан Назарбаев халықаралық әуежайы" акционерлік қоғамы
Ұйымдастырушының атауы:	"Нұрсұлтан Назарбаев халықаралық әуежайы" акционерлік қоғамы
Конкурстың №:	№ 17792618-1
Конкурстың атауы:	Бағдарламалық жасақтаманы сатып алу. Тел.: 8 (7172) 777-377, 777-177
Лоттың нөмірі:	№ 88075238-OK1
Лоттың атауы	Бағдарламалық қамтамасыз ету
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*:	620129.000.000000
Тауардың атауы*:	Бағдарламалық қамтамасыз ету
Өлшем бірлігі*:	Дана
Саны (көлемі)*:	1
Қосылған құн салығын есептегенде бірлік бағасы*:	14909482.75
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома*:	14909482.75
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс*:	

Жеткізу шарттары (сәйкес ИНКОТЕРМС 2010)*	DDP термині келу орнын көрсете отырып қолданылады. Бұл сатып алушының елінде көрсетілген жерге тауар жеткізілгеннен кейін сатушының жауапкершілігі аяқталатынын білдіреді. Жүктерді жеткізу бойынша барлық тәуекелдер, барлық шығыстар (салықтар, баждар және т.б.), импорт кезінде төленетін баждар мен басқа да төлемдерді қоса алғанда, тауардың бүлінуі мен жоғалуы үшін жауапкершілік осы уақытқа дейін сатушыға жүктеледі, сатушы сонымен қатар кедендік тазартуға жауап береді
Жеткізу мерзімі*	шартқа қол қойылған күннен бастап 15 күнтізбелік күн өткен соң, 30 күнтізбелік күн ішінде
Жеткізу орны*	711210000, Астана қ., Есіл ауданы Қабанбай батыр даңғылы 119, әуежай
Аванстық төлем мөлшері*:	0
Ұлттық стандарттардың атауы, ал олар болмаған жағдайда сатып алынатын тауарларға арналған мемлекетаралық стандарттар. Ұлттық және мемлекетаралық стандарттар болмаған кезде мемлекеттік сатып алуды нормалауды ескере отырып, сатып алынатын тауарлардың талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары көрсетіледі.	жоқ
Тұрғын емес мақсаттағы ғимараттарды, құрылыстарды, үй-жайларды, авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған шарт жасасу күніне дейін (үш жылға дейін) шығарылған жылы болуға тиіс	
Кепілдік мерзімі (айлармен)	24

Сатып алынатын тауардың талап етілетін функционалдық, техникалық, сапалық, пайдалану және өзге де сипаттамаларының сипаттамасы	Жеткізуші лицензияларды беруге міндетті БҚ осалдық сканері. Лицензияның қолданылу мерзімі-24 ай. Бағдарламалық жасақтама төмендегі сипаттамаларға сәйкес келуі керек: Бағдарламалық жасақтаманы басқару механизмі: қорғалған HTTPS қосылымын қолдана отырып, веб-интерфейсті қолдану. IP мекенжайларының саны: кемінде 500. Сканерлеу саясаты: өзіңіздің қажеттіліктеріңізге сәйкес сканерлеу саясатын орнату. Бір уақытта сканерлеу: лицензияланған хосттарды, атап айтқанда Windows / Linux / Mac ОЖ және желілік жабдықты басқаратын серверлер мен жұмыс станцияларын бір уақытта сканерлеу. Сканерлеу нәтижелерін сақтау орны: сканерлеу нәтижелері тек жергілікті компьютерде сақталады, нәтижелерді Интернет желісінде сақтауға жол берілмейді. Сканерленетін түйіндердің қызметтерін анықтау ерекшеліктері: тізбеден қосылу түрлері қолданылады: - Stealth scan (SYN); - Stealth scan (SYN+RST); - Stealth scan (SYN+FIN); - Stealth scan (SYN+ECE); - Full connect scan. Қызметтерді анықтауға арналған порттардың ауқымы: 1-65535. Дерекқор ақпаратына ерікті сұрауларды орындау: әкімшінің веб-интерфейсі арқылы сканерлеу нәтижелерімен ДБ-ға SQL сұрауларын орындау және сұрау бойынша деректерді CSV форматында экспорттау мүмкіндігі. Веб-ресурстарды сканерлеу: OWASPTop 10 құрамындағы осалдықтарды анықтау, SQLinjection, cross-sitescripting (CSS / XSS) қауіптерін, осал CGI сценарийлерін, әлсіз құпия сөздерді және конфигурация қателерін анықтау. Автоматты әрекеттер: ағымдағы оқиғаларға байланысты автоматты әрекеттерді орындау мүмкіндігі: * Жаңартуларды алу: - көрсетілген хосттарды жаңартуда түскен осалдықтардың бар-жоғын сканерлеңіз; * Жаңа хостты анықтау: - хостты сканерлеуге қосыңыз; - хостты сканерлеуге және сканерлеуге қосыңыз. Сканерлеуге жататын хосттарды анықтау мақсатында басқа бағдарламалық жасақтамамен интеграциялау: Microsoft Active Directory; Microsoft DHCP server; Microsoft Exchange; VMware ESX(i); VMware VSphere. Инфильтрациялық тестілеу шешімдерімен Интеграция: анықталған осалдықтарды тексеру және инфильтрацияның сәттілігіне қатысты ақпаратты басқару консоліне оралу мақсатында ену тестілеуін орындайтын шешімдермен екі жақты интеграциялау мүмкіндігі.осалдықтарды пайдалану. Есеп форматтары: PDF; - RTF; - HTML; - XML; - CSV; - TXT. Веб ресурстарға аутентификацияны қолдау: - Веб формаларды қолдану; - хедеров; - plain authentication. Сканерлеу нәтижелерін одан әрі өңдеу үшін сыртқы ДҚБЖ-ға экспорттау: - MS SQLServer; - Oracle; - MySQL; - PostgreSQL. ДҚБЖ сканерлеу: - MS SQLServer; - Oracle; - MySQL; - PostgreSQL; - Sybase Adaptive Server Enterprise (ASE); - DB2; - AS/400. Сканерлеу нәтижелерінің құрамы: Хост туралы толық техникалық мәліметтер (IP / MAC мекенжайлары, платформа түрі, ОЖ және т. б.) Динамикадағы хосттағы қауіп көрсеткіштері; The эксплуатациялар тізімі теориялық тұрғыдан осалдықтар тізіміне сәйкес хостқа шабуыл жасау үшін қолдануға болады; Cvss деректерін және осалдықтардың жарияланған / өзгертілген күнін қоса алғанда, хост осалдықтарының тізімі; Хост осалдықтарын
--	---

	пайдалана алатын зиянды бағдарламалардың тізімі; Хостта іске қосылған қызметтер; Хосттағы пайдаланушылар мен пайдаланушылар топтары; Хостта орнатылған; Деректер базасы; Файлдық ресурстар желіден қол жетімді. Хосттарды топтастыру және ұйымдастыру: Хосттарды динамикалық топтарға топтастыру мүмкіндігі (таңдалған критерийлерге байланысты хосттар тізімін автоматты түрде өзгерту мүмкіндігімен) келесі критерийлер мен олардың комбинациялары бойынша: - asset name; - CVE ID; - host type; - IP address range; - IP address type; - last scan date; - operating system name; - PCI compliance status; - service name; - open port numbers; - operating system name; - software name; - presence of validated vulnerabilities; - user-added criticality level; - user-added custom tag; - user-added tag (location); - user-added tag (owner); - vAsset cluster; - vAsset datacenter; - vAsset host; - vAsset power state; - vAsset resource pool path; - CVSS risk vectors; - vulnerability category; - vulnerability CVSS score; - vulnerability exposures; - vulnerability risk scores; - vulnerability title. Жеке есеп үлгілері негізінде ерікті есептер жасау: дайын үлгілерді пайдалану мүмкіндігімен жаңа есеп үлгілері негізінде есептер жасау мүмкіндігі. Бағдарламалық жасақтама элементтерін жаңарту: Интернет желісінен автоматты түрде жаңарту мүмкіндігі және міндетті түрде Интернет желісіне кірмей жаңарту мүмкіндігі. Сақтық көшірмеге қойылатын талаптар: Орындаушы енгізу қорытындысы бойынша конфигурацияланған жүйе конфигурациясының сақтық көшірмесін жасауға міндетті. Сақтық көшірмелер Тапсырыс берушіге берілуі және жедел қалпына келтіруге жарамды форматта сақталуы керек. Көрсетілген резервтік көшіру жөніндегі іс-шараларды Орындаушы аппараттық платформаның істен шығуына, сервистердің жұмысқа қабілеттілігін жедел қалпына келтіру мүмкіндігін қамтамасыз етуге және қажет болған жағдайда бастапқы немесе нысаналы конфигурацияға оралуға байланысты осы жоғалтуға байланысты тәуекелдерді азайту мақсатында орындауы тиіс. Сақтық көшірме жасау мен қалпына келтіруді Орындаушы өз қаражатынан қамтамасыз етуі тиіс. Сақтық көшірме жасау функциясы келесі талаптардың орындалуын қамтамасыз етуі керек: Масштабтау: компоненттерді көлденең масштабтау арқылы өнімділікті арттыру мүмкіндігі. Орталықтандырылған басқару: Windows немесе Linux жүйесінде басқару серверін орнату. Тасымалдау тиімділігі: тұрақсыз байланыс арналарында (Wi-Fi/4G) жұмыс істеу үшін тек өзгертілген блоктарды көшіру (қосымша көшіру). Сақтауды оңтайландыру: сақталған деректердің көлемін азайту үшін ғаламдық қайталану және бастапқы қысу. Автоматтандыру: кесте бойынша немесе файлдардағы өзгерістер анықталған кезде сақтық көшірме жасау. Өзіне-өзі қызмет көрсету: әкімшінің қатысуынсыз пайдаланушылардың файлдарды өз бетінше іздеуі және қалпына келтіруі үшін порталдың болуы. Файлдық жүйелерді қолдау: FAT, NTFS, ReFS, APFS (macOS), EXT, XFS және т.б. файлдық жүйелермен жұмыс. Қалпына келтіру: жеке файлдарды да, жүйенің немесе дискілердің бүкіл
--	---

	конфигурациясын қалпына келтіру мүмкіндігі. Деректер қауіпсіздігі: қорғалған арналар арқылы сақтау және беру кезінде сақтық көшірмелерді міндетті түрде шифрлау. Интернет арқылы жұмыс істеу: орталық серверден 1000 км-ден астам қашықтықта бэкап пен қалпына келтірудің жұмыс қабілеттілігін қамтамасыз ету. Трафикті басқару: сығымдау механизмдері және өткізу қабілеттілігін шектеу (throttling), сондықтан сақтық көшірме пайдаланушының жұмысына кедергі келтірмейді. Синтетикалық сақтық көшірме: серверде синтездеу арқылы пайдаланушының құрылғысына жүктемесіз толық көшірмелерді жасауды қолдау. Әлеуетті өнім берушіге қойылатын талаптар: Әлеуетті өнім беруші Мемлекеттік сатып алуды жүзеге асыру қағидаларына 4-қосымшаның 2) тармақшасының 7) тармақшасының негізінде конкурсқа өтінім құрамында Қазақстан Республикасының аумағында БҚ жеткізу құқығына вендордан авторизациялық хат ұсынуға тиіс.
Ілеспе қызметтер (қажет болған жағдайда көрсетіледі) (тауарларды монтаждау, баптау, оқыту, тексеру және сынау)	
Әлеуетті өнім беруші оны жеңімпаз деп айқындаған және онымен мемлекеттік сатып алу туралы шарт жасасқан жағдайда (қажет болған жағдайда көрсетіледі) (Әлеуетті өнім берушінің көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін бас тартуына жол берілмейді)	

Ескертпе:

1. Функционалдық, техникалық, сапалық, пайдалану, өзге де сипаттамалар, ілеспе қызметтер және орындаушыға қосымша шарттар бойынша әрбір талап жеке жолда көрсетіледі.
 2. Осы техникалық ерекшелікте әлеуетті өнім берушіге қойылатын біліктілік талаптарын белгілеуге жол берілмейді.
 3. Өзге құжаттарда техникалық ерекшелік талаптарын белгілеуге жол берілмейді.
- *мәліметтер мемлекеттік сатып алу жоспарынан тартылады (автоматты түрде көрсетіледі).

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

Наименование заказчика	Акционерное общество "Международный аэропорт Нурсултан Назарбаев"
Наименование организатора	Акционерное общество "Международный аэропорт Нурсултан Назарбаев"
№ конкурса:	№ 17792618-1
Наименование конкурса:	Приобретение программного обеспечения. Тел.: 8 (7172) 777-377, 777-177
Номер лота:	№ 88075238-ОК1
Наименование лота:	Программное обеспечение
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*:	620129.000.000000
Наименование товара*:	Программное обеспечение
Единица измерения*:	Штука
Количество (объем)*:	1
Цена за единицу, без учета налога на добавленную стоимость*:	14909482.75
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*:	14909482.75
Условия поставки (в соответствии с ИНКОТЕРМС 2010)*:	DDP термин употребляется с указанием места прибытия. Он означает, что ответственность продавца заканчивается после того, как товар доставлен в указанное место в стране покупателя. Все риски, все расходы по доставке груза (налоги, пошлины и т. д.), ответственность за порчу и потерю товара, включая пошлины и прочие выплаты, выплачиваемые при импорте, до этого момента несёт продавец, также он несёт ответственность за таможенную очистку.
Срок поставки*:	по истечении 15 календарных дней со дня подписания договора, в течение 30 календарных дней

Место поставки товара*:	711210000, г.Астана, район Есиль проспект Кабанбай батыра 119, аэропорт
Размер авансового платежа* **:	0 %
Наименование национальных стандартов, а при их отсутствии межгосударственных стандартов на закупаемые товары. При отсутствии национальных и межгосударственных стандартов указываются требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров, с учетом нормирования государственных закупок.	отсутствуют
Товар должен быть новым, неиспользованным, год выпуска не ранее (до трех лет) до даты заключения договора за исключением приобретения здания, строения, сооружения, помещения, имеющих нежилое назначение, авиационной техники	
Гарантийный срок (в месяцах)	24

Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара	Поставщик обязан предоставить лицензии на ПО сканер уязвимостей. Срок действия лицензии – 24 месяца. Программное обеспечение должно соответствовать нижеуказанным характеристикам: Механизм управления программным комплексом: С помощью веб интерфейса с использованием защищенного HTTPS соединения. Количество IP адресов: не менее 500. Политика сканирования: Настройка политик сканирования согласно собственных потребностей. Одновременное сканирование: Одновременное сканирование пролицензированных хостов, а именно: серверов и рабочих станций под управлением ОС Windows / Linux / Mac и сетевого оборудования. Место хранения результатов сканирования: Результаты сканирования сохраняются только на локальном компьютере, хранения результатов в сети Интернет недопустимо. Особенности определения сервисов узлов, которые сканируются: Применяются типы соединения из перечня: - Stealth scan (SYN); - Stealth scan (SYN+RST); - Stealth scan (SYN+FIN); - Stealth scan (SYN+ECE); - Full connect scan. Диапазон портов для определения сервисов: 1-65535. Выполнение произвольных запросов к информации базы данных: Возможность с помощью веб интерфейса администратора выполнять SQL запросы к БД с результатами сканирования и экспортировать данные по запросу в формате CSV. Сканирование веб ресурсов: Выявление уязвимостей, содержащихся в OWASPTop 10, определять угрозы SQLinjection, cross-sitescripting (CSS / XSS), уязвимые CGI скрипты, слабые пароли и ошибки конфигурирования. Автоматические действия: Возможность выполнять автоматические действия в зависимости от текущих событий: - Получение обновлений: - просканировать указанные хосты на наличие уязвимостей, поступивших в обновлении; - Выявление нового хоста: - добавить хост в сканирования; - добавить хост в сканирования и просканировать. Интеграция с другим ПО с целью выявления хостов, подлежащих сканированию: Microsoft Active Directory; Microsoft DHCP server; Microsoft Exchange; VMware ESX(i); VMware VSphere. Интеграция с решениями для тестирования на проникновение: Возможность двусторонней интеграции с решениями, которые выполняют тестирование на проникновение с целью валидации выявленных уязвимостей и возвращения в консоль управления информации относительно успеха проникновения используя уязвимости. - Форматы отчетов: PDF; - RTF; - HTML; - XML; - CSV; - TXT. Поддержка аутентификации на веб ресурсы: - С помощью веб форм; - хедеров; - plain authentication. Экспорт результатов сканирования во внешнюю СУБД для дальнейшей обработки: - MS SQLServer; - Oracle; - MySQL; - PostgreSQL. Сканирование СУБД: - MS SQLServer; - Oracle; - MySQL; - PostgreSQL; - Sybase Adaptive Server Enterprise (ASE); - DB2; - AS/400. Состав результатов сканирования: - Подробные технические сведения о хосте (IP / MAC адреса, тип платформы, ОС и др.) - Показатели угроз на хосте в динамике; - Список эксплойтов которые, теоретически, можно применить для атаки на хост согласно списку уязвимостей; - Список уязвимостей хоста, включая данные CVSS и дату публикации /
--	--

	модификации уязвимостей; - Список вредоносного ПО, которое может использовать уязвимости хоста; - Запущенные на хосте сервисы; - Пользователи и группы пользователей на хосте; - Установленное на хосте ПО; - Базы данных; - Файловые ресурсы доступны из сети. Группировка и организация хостов: Возможность группировать хосты в динамические группы (с возможностью автоматически изменять список хостов, что в них входят, в зависимости от выбранных критериев) по следующим критериям и их комбинациям: - asset name; - CVE ID; - host type; - IP address range; - IP address type; - last scan date; - operating system name; - PCI compliance status; - service name; - open port numbers; - operating system name; - software name; - presence of validated vulnerabilities; - user-added criticality level; - user-added custom tag; - user-added tag (location); - user-added tag (owner); - vAsset cluster; - vAsset datacenter; - vAsset host; - vAsset power state; - vAsset resource pool path; - CVSS risk vectors; - vulnerability category; - vulnerability CVSS score; - vulnerability exposures; - vulnerability risk scores; - vulnerability title. Создание произвольных отчетов на основе собственных шаблонов отчетов: Возможность создания отчетов на основе новых шаблонов отчетов с возможностью использования готовых шаблонов. Обновление элементов программного обеспечения: Возможность автоматического обновления из сети Интернет и, обязательно, возможность обновления без доступа к сети Интернет. Требования к резервному копированию: Исполнитель обязан осуществить резервное копирование настроенной по итогам внедрения конфигурации системы. Резервные копии должны быть переданы Заказчику и храниться в формате, пригодном для оперативного восстановления. Указанные мероприятия по резервному копированию должны быть выполнены Исполнителем в целях минимизации рисков, связанных с потерей данных ввиду выхода из строя аппаратной платформы, обеспечения возможности оперативного восстановления работоспособности сервисов и возврата к исходной либо целевой конфигурации при необходимости. Резервное копирование и восстановление должны быть обеспечены Исполнителем из собственных средств. Функционал резервного копирования должен обеспечивать соблюдение следующих требований: Масштабируемость: Возможность увеличения производительности путем горизонтального масштабирования компонентов. Централизованное управление: Установка сервера управления на Windows или Linux. Эффективность передачи: Копирование только изменившихся блоков (инкрементальное копирование) для работы на нестабильных каналах связи (Wi-Fi/4G). Оптимизацию хранения: Глобальная дедупликация и сжатие на стороне источника для минимизации объема хранимых данных. Автоматизация: Резервное копирование по расписанию или при обнаружении изменений в файлах. Самообслуживание: Наличие портала для самостоятельного поиска и восстановления файлов пользователями без участия администратора. Поддержка файловых систем: Работа с файловыми системами FAT, NTFS, ReFS,
--	---

	APFS (macOS), EXT, XFS и другими. Восстановление: Возможность восстановления как отдельных файлов, так и всей конфигурации системы или дисков. Безопасность данных: Обязательное шифрование бэкапов при хранении и передаче по защищенным каналам. Работа через интернет: Обеспечение работоспособности бэкапа и восстановления на удалении более 1000 км от центрального сервера. Управление трафиком: Механизмы сжатия и ограничения полосы пропускания (throttling), чтобы бэкап не мешал работе пользователя. Синтетический бэкап: Поддержка создания полных копий без нагрузки на устройство пользователя за счет синтеза на сервере. Требования к потенциальному поставщику: Потенциальный поставщик на основании пп. 7) п. 2) Приложения 4 к Правилам осуществления государственных закупок, в составе заявки на конкурс должен предоставить авторизационное письмо от вендора на право поставки ПО на территории Республики Казахстан.
Сопутствующие услуги (указываются при необходимости) (монтаж, наладка, обучение, проверки и испытания товаров)	
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)	

Примечание

1. Каждое требование по функциональным, техническим, качественным, эксплуатационным, иным характеристикам, сопутствующим услугам и дополнительным условиям к исполнителю указывается отдельной строкой.
 2. Установление в настоящей технической спецификации квалификационных требований, предъявляемых к потенциальному поставщику, не допускается.
 3. Установление требований технической спецификации в иных документах не допускается.
- * сведения подтягиваются из плана государственных закупок (отображаются автоматически).