



к договору (контракту) от 12.09.2022 г. № 22-48

**ГРАФИК ПЛАТЕЖЕЙ\***

Приложение № 8 к правилам казначейского исполнения бюджетов бюджетной системы Республики Узбекистан

между ООО "Starlab" и Беринария ва чорвачиликни ривожлантириш давлат кўмитаси на общую сумму 89 000 000,00

Глава

Казначейский лицевой счёт

401010860262947042131250001

250

\_\_\_\_\_

Наименование месяцев  
2022 г.

Наименование месяцев 2022 г.	Виды расходов** (соответствующий код бюджетной классификации)	4299990	Всего
Январь			
Февраль			
Март			
Апрель			
Май			
Июнь			
Июль			
Август			
Сентябрь		89 000 000,00	89 000 000,00
Октябрь			
Ноябрь			
Декабрь			
<b>Всего за год</b>		<b>89 000 000,00</b>	<b>89 000 000,00</b>

Всего 89000000,00 сум

Восемьдесят девять миллионов сум 00 тишин

сумма прописью

Из вышеуказанной суммы 2670000 сум или 30,00%\*\*\* от общей суммы договора подлежат оплате в \_\_\_\_\_ мес. 20 \_\_\_\_ г.

(\* — Бюджетные организации, получатели бюджетных средств и получатели средств ДЦФ, предоставляющих в казначейские органы в 2-х экземплярах;  
 (\*\* — Указывается раздел, глава, параграф и статья расхода;  
 (\*\*\*) — Месячный \_\_\_\_\_%, от указанной выше суммы которой необходимо оплатить до \_\_\_\_\_ числа текущего месяца. Данное поле заполняется со стороны бюджетных организаций, получателей бюджетных средств и получателей средств ДЦФ в случае осуществления оплаты в соответствии с порядком, установленным законодательством по договорам за оказание коммунальных услуг, услуг связи и предоставления в регулярном порядке товара (работ, услуг) указанных в правовых документах.)



Принял работник казначейского подразделения \_\_\_\_\_

(подпись)

20 \_\_\_\_ г.

Получил работник заказчика \_\_\_\_\_

(подпись)

20 \_\_\_\_ г.

Бохидов Л. Х.

Ф.И.О.

Бердикулов С. В.

Ф.И.О.



Компания ООО «Starlab», именуемая в дальнейшем «Лицензиар», в лице Генерального директора Умаров Х.Н. действующего на основании Устава с одной стороны, и Тошмухаммед Бермухамедов, именуемое в дальнейшем «Лицензиат», в лице Тошмухаммед Бермухамедов С. действующего на основании паспорта, с другой стороны, в дальнейшем именуемые по отдельности «Сторона», а вместе с «Сторонами», заключили настоящий договор (далее – Договор) о нижеследующем:

### 1. Предмет Договора

1.1. Лицензиар обязуется предоставить лицензиат право (простою) неисключительную лицензию (далее – ПО), согласно Спецификации, указанной в Приложении №1, а лицензиат обязуется выплачивать лицензиару в срок и в порядке, указанном в настоящем Договоре. ПО является объектом авторского права. Использование объектов авторского права регулируется Гражданским кодексом РУз, Законом РУз «Об авторском праве и смежных правах» и иными законодательными актами РУз. ПО может использоваться в соответствии с электронными лицензионными соглашениями, принимаемыми при использовании ПО.

### 2. Права и обязанности Сторон

2.1. Лицензиату предоставляется право на осуществление деятельности с использованием ПО.  
2.2. Лицензиар обязан:  
2.2.1. Передать ПО и электронно-цифровые ключи к нему в порядке и сроки, предусмотренным настоящим Договором;  
2.2.2. Одновременно с Актом сдачи-приёмки ПО и электронно-цифровых ключей передавать лицензиату счёт-фактуру, оформленную с соблюдением порядка и сроков, установленных законодательством Республики Узбекистан.  
2.3. Лицензиат обязан:  
2.3.1. Выплатить за право использования ПО в порядке, указанном в Разделе 5 настоящего Договора;  
2.3.2. Использовать ПО в строгом соответствии с настоящим Договором и действующим законодательством РУз.

### 3. ПОРЯДОК ПЕРЕДАЧИ, СДАЧИ-ПРИЁМКИ

3.1. Лицензиар обязуется осуществить передачу ПО и всех документов, предусмотренных пунктом 3.2 настоящего Договора в течение 20 (двадцати) календарных дней с момента вступления Договора в силу. Передача ПО осуществляется лицензиаром в номенклатуре, количестве и по ценам, указанным в Приложении №1 Договора. ПО может быть передано лицензиату средствами электронной почты (для электронных лицензий), на магнитных носителях или иным образом. Лицензиар передаёт лицензиату достаточную для использования объекта авторского права техническую и иную документацию, осуществляя оказание технической помощи и при необходимости поставку специального оборудования.



3.2. Лицензиаром предоставляется Лицензиату Акт сдачи - по завершении передачи ПО. Лицензиат в течение 10 (десяти) банковских дней с момента получения Акта сдачи ПО и электронно-цифровых ключей должен подписать его и передать один подписанный экземпляр Лицензиару. В случае если в указанный период Лицензиат обнаружит недостатки в переданном ПО или отсутствие документации, или принадлежности, необходимых для надлежащей эксплуатации ПО, Лицензиат направляет Лицензиару мотивированный отказ от подписания Акта. В этом случае Акт должен быть подписан в течение 5 (пяти) рабочих дней с момента исправления недостатков.

#### 4. ГАРАНТИИ И ЛЕГАЛЬНОСТЬ ПО

4.1. Лицензиар гарантирует легальность поставляемого ПО. Лицензиар гарантирует, что он обладает правом предоставлять права, указанные в пункте 1.1 настоящего Договора.

4.2. Гарантия на использование ПО обеспечивается компанией-производителем данного ПО в соответствии с принятого Лицензиатом во время установки ПО.

4.3. Лицензиар гарантирует отсутствие каких-либо претензий со стороны авторов ПО и иных третьих лиц по использованию ПО Лицензиатом. В случае возникновения подобных претензий Лицензиар обязуется принять на себя полную ответственность (в т.ч. материальную) за урегулирование споров и претензий.

#### 5. ПОРЯДОК ВЗАИМОРАСЧЕТОВ

5.1. За предоставленное неисключительное право, предусмотренное настоящим Договором, Лицензиат уплачивает Лицензиару. Общая сумма вознаграждения, согласно Приложению №1, составляет 89 000 000 (Восемьдесят девять миллионов) тиния, включая НДС

5.2. Сумма является твердой и не подлежит изменению в течение срока действия настоящего Договора.

5.3. Предоплата в размере 30% в течение 10 календарных дней с момента подписания договора, остальные 70% после получения акта выполненных работ в течение 5 рабочих.

5.4. Оплата по настоящему Договору производится Лицензиатом путем перечисления денежных средств на расчетный счет Лицензиара в банке.

5.5. Датой платежа считается дата списания денежных средств с расчетного счета Лицензиата.

5.6. Комиссии банка Лицензиата несет Лицензиат, все остальные комиссии банков, включая комиссии банка Лицензиара и банков корреспондентов, несет Лицензиар.

5.7. После истечения срока действия Договора, все условия Договора будут иметь силу до осуществления окончательных взаиморасчетов и исполнения всех обязательств сторонами возникших в период действия Договора.

#### 6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Договору Лицензиар и Лицензиат несут ответственность в соответствии с законодательством Республики Узбекистан.

6.2. В случае просрочки оплаты Лицензиатом, Лицензиар имеет право требовать от Лицензиата уплаты пени в размере 0,1% (ноль целых одна десятых процента) от



9.1. Ни одна из Сторон не несет ответственности в случае невыполнения, несвоевременного или ненадлежащего выполнения каких-либо обязательств по Договору, если указанные невыполнения, несвоевременное или ненадлежащее выполнение обусловлены обстоятельствами непреодолимой силы (форс-мажор), возникшими после заключения Договора в результате событий чрезвычайного характера, которые Стороны не могли предвидеть и предотвратить разумными мерами.

## 9. ФОРС-МАЖОР

8.3. В случае разглашения сведений, содержащихся в указанной документации и информации, Стороны, предприятия Стороны, его контрагентами или лицами из их персонала Сторона возместит понесенные в связи с этим убытки.

8.2. С указанной в приложении документации и информацией будут ознакомлены только те лица из персонала предприятий Сторон и его контрагентов, которые непосредственно связаны с использованием ПО по лицензии.

8.1. Информация, связанная с обязательством Сторон по настоящему Договору, является конфиденциальной. Стороны гарантируют сохранение конфиденциальности документации, информации, знаний и опыта, полученных Сторонами, предприятиями Сторон и его контрагентами. Стороны обязуются принять все необходимые меры для того, чтобы предотвратить полное или частичное разглашение документации и информации, или ознакомление с ними третьих лиц без письменного согласия Сторон.

## 8. КОНФИДЕНЦИАЛЬНОСТЬ

7.2. В течение срока действия настоящего Договора Лицензиар обязуется информировать Лицензиата о возможных усовершенствованиях и улучшениях ПО.

7.1. Лицензиат обязуется самостоятельно получать регулярные обновления ПО через встроенный адрес Интернета, указанный в ПО.

## 7. УСОВЕРШЕНСТВОВАНИЯ И УЛУЧШЕНИЯ

6.6. Ответственность, предусмотренная настоящим разделом Договора, применяется в случае направления заинтересованной Стороной соответствующего письменного требования противоположной Стороне и рассчитывается за период, определенный в таком письменном требовании.

6.5. Во всем остальном, что не предусмотрено настоящим Договором, Стороны руководствуются Гражданским кодексом РФ, Законом РФ «О договорно-правовой базе деятельности хозяйствующих субъектов» и иными законодательными актами РФ.

6.4. Сторона, нарушившая свои обязательства по Договору, уплачивает неустойку в течение 10 дней со дня предъявления соответствующего требования другой Стороной.

6.3. В случае если Лицензиар откажется от исполнения Договора в одностороннем порядке, или просрочит исполнение своих обязательств на срок более 30 (тридцати) календарных дней, Лицензиат вправе в одностороннем порядке отказаться от исполнения настоящего Договора и потребовать с Лицензиара уплаты штрафа в размере 10% (десять) от общей суммы, предусмотренного пунктом 5.1 настоящего Договора.

6.2. В случае если Лицензиар откажется от исполнения Договора в одностороннем порядке, или просрочит день просрочки, но не более 10% (десять) от суммы



9.2. Обязательствами не являются обязательства, которые стороны не могут оказывать влияние и за возникновение которых несут ответственности. К обязательствам не относятся: землетрясения, наводнения и другие стихийные явления природы, пожары, военные действия, блокады, катастрофы, препятствия со стороны Правительства, а также действия Правительства или законодательных положений, которые могут оказать негативное влияние на выполнение сторонами своих обязательств по настоящему Договору.

9.3. Сторона, для которой созданы вышеуказанные обязательства, приведшие к невозможности исполнения договорных обязательств, немедленно письменно известит другую Сторону об обстоятельствах, препятствующих исполнению обязательств, предполагаемом сроке действия и прекращении такого обязательства. Надлежащим показателем наличия обстоятельств непреодолимой силы является нормативный акт (документ) компетентного органа страны, в которой имело действие обязательства непреодолимой силы или его прямые последствия.

9.4. Срок исполнения обязательств по настоящему Договору Сторона, для которой возникли обязательства непреодолимой силы, переносится на время, в течение которого данные обстоятельства будут препятствовать исполнению Договора.

9.5. В случае если обязательства непреодолимой силы продолжатся более одного месяца, любая из Сторон вправе расторгнуть настоящий Договор, направив письменное уведомление второй Стороне. В этом случае вторая Сторона не будет иметь право требовать возмещения первой Стороной возможных убытков, вызванных такими обстоятельствами непреодолимой силы. В этом случае настоящий Договор считается расторгнутым в момент получения одной Стороной указанного уведомления другой Стороной об отказе от исполнения Договора.

## 10. РАЗРЕШЕНИЕ СПОРОВ И ПРИМЕНИМОЕ ПРАВО

10.1. Спорные вопросы, возникающие в ходе исполнения настоящего Договора, разрешаются Сторонами путем переговоров, и возникшие договоренности в обязательном порядке фиксируются дополнительным соглашением или протоколом настоящего Договора, становящееся с момента его подписания неотъемлемой частью настоящего Договора.

10.2. Все споры, разногласия или требования, возникающие из настоящего Договора или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или недействительности, которые Стороны не смогли урегулировать в разумные сроки в порядке, описанном в пункте 10.1 настоящего Договора, подлежат разрешению в Экономическом суде г.Ташкента, в соответствии с действующим законодательством Республики Узбекистан.

## 11. ИЗМЕНЕНИЯ, ДОПОЛНЕНИЯ И РАСТОРЖЕНИЕ

11.1. Все изменения и дополнения к настоящему Договору считаются действительными только в том случае, если они совершены в письменной форме и подписаны лицами, уполномоченными обеими договаривающимися Сторонами, а также одобрены компетентными органами, если такое одобрение необходимо.

11.2. Настоящий Договор может быть расторгнут по взаимному согласию Сторон.

11.3. Каждая из Сторон имеет право досрочно расторгнуть настоящий Договор путем направления письменного уведомления, если другая Сторона не выполнит какое-либо существенное условие настоящего Договора.

11.4. При не достижении согласия, неисполнении или ненадлежащем исполнении условий настоящего Договора одной из Сторон Договор может быть расторгнут в установленном порядке законодательством Республики Узбекистан.



## 12. СРОК ДЕЙСТВИЯ ДОГОВОРА

12.1. Договор вступает в законную силу после подписания обеими Сторонами. Договор действует до 31 декабря 2022 года.

## 13. ПРОЧИЕ УСЛОВИЯ

13.1. Настоящий Договор составлен в двух экземплярах, каждый экземпляр имеет

одинаковую юридическую силу.

13.2. Данный Договор является основанием для осуществления банковских операций.

13.3. К отношениям Сторон по тем вопросам, которые не урегулированы или не полностью урегулированы Договором, Стороны будут применять нормы

Гражданского кодекса РУз и других законов РУз.

13.4. Нижеследующие Приложение являются неотъемлемыми частями Договора:

Приложение № 1 – Спецификация;

13.5. Настоящий Договор составлен на Русском языке, в 2-х экземплярах одинаковой

юридической силы, по одному экземпляру для каждой из сторон.

## 14. РЕКВИЗИТЫ И ПОЧТОВЫЕ АДРЕСА СТОРОН

От Лицензиата

<b>VETERINARIYA VA CHORVACHILIKNI</b> <b>RIYOJLANTIRISH DAVLAT QO'MITASI</b> <b>TOSHKENT SH, KICHIK XALQA YO'LI, 21A</b> <b>SH/R: 401010860694917042131250001</b> <b>DNN: 200935112 OKONX: 97300 MV G'AZNACHILIGI</b> <b>XKKM MARKAZIY BANK BOSH BOSHQARMASI</b> <b>H/R: 2340 2000 3001 0000 1010 MFO: 00014</b> <b>DNN: 201122919 TEL: 71/ 276-91-50; 71/ 276-90-85</b>
---

ООО «Starlab»

От Лицензиара

г. Ташкент, Чиланзарский район,  
Каптал Е, дом 9.

<b>Банковские реквизиты: ОАК «Туронбанк»</b> <b>Чиланзарского филиала.</b> <b>МФО: 01084 ИНН: 304426154 ОКЗД: 62090</b> <b>Р/с: 2020 8000 3006 9161 5001</b> <b>Тел/факс: +998712001999</b> <b>Регистрационный код НДС: 326060121141</b>
---

Генеральный директор

Умаров Х.Н.

М.П. подпись (ИО)



М.П. подпись (ИО)



<b>O'ZBEKISTON RESPUBLIKASI</b> <b>VETERINARIYA VA CHORVACHILIKNI</b> <b>RIYOJLANTIRISH DAVLAT QO'MITASI</b> <b>YURIDIK BO'LIM</b> F.I.O. _____ IMZO _____ 20__ y.
--

Handwritten signature

Handwritten signature





# СВИДЕТЕЛЬСТВО

О государственной регистрации юридического лица

Юридическое лицо

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "СТАРЛАВ"

Полное наименование юридического лица - хозяйствующего субъекта с указанием организационно-правовой формы

ООО "СТАРЛАВ"

Сокращенное наименование юридического лица

304 426 154

Идентификационный номер налогоплательщика

Организация (реорганизация, иная регистрация, изменение сведений)

Дата

15.11.2016

Подтверждается

01253208

Организационно-правовая форма:

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

Место осуществления деятельности:

ГОРОД ТАШКЕНТ, ЧИЛАНЗАРСКИЙ РАЙОН, NULL

Свидетельство выдано:

CHILONZOR TUMANI DAVLAT XIZMATLARI MARKAZI

034649





**“ТАСДІКЛАЙМАН”**

Ўзбекистон Республикаси Ветеринария ва

чорвачиликни ривожлантириш давлат

қўмитаси раиси ўринбосари танлов

қўмитаси раиси ўринбосари танлов

2022 йил 12 сентябрь



Ўзбекистон Республикаси Ветеринария ва чорвачиликни  
ривожлантириш давлат қўмитаси танлов комиссияси йўналишининг

12-04-22/2-сон

**БАЁННОМА СИ**

2022 йил 12 сентябрь

**КАТНАШИЛАР:**

С.В. Бердиқулов

К.Х. Юнусов

Ф.С. Ахмедов

Л.Х. Воҳидов

А.А. Влащенко

Ж.С. Отаниёзов

Ветеринария ва чорвачиликни ривожлантириш давлат қўмитаси раиси ўринбосари, танлов комиссияси раиси.

Капитал қурилиш, таъминот ва маркетинг бўлими бош мутахассиси, танлов комиссияси қотиби.

Молия-иқтисодий таҳлил ва бухгалтерия хисоби бошқарма бошлиғи, танлов комиссияси аъзоси.

Ветеринария ва чорвачиликни ривожлантириш давлат қўмитаси Бош хисобчи, танлов комиссияси аъзоси.

Ахборот коммуникация ва технологияларни жорий қилиш бошқармаси Бош мутахассиси, танлов комиссияси аъзоси.

Хужалик ишлари мудири, танлов комиссияси аъзоси.

**ҚУН ТАРТИБИ:**

“Киберхавфсизлик тўғрисида”ги Ўзбекистон Республикасининг қонуни ҳамда Қўмита Раисининг 2022 йил 27 апрелдаги 52-и/ч-сон бўйруғининг қўмита Раисининг қўмитаси раиси ўринбосари, танлов комиссияси раиси С.Бердиқулов сузга чиқиб, “Киберхавфсизлик тўғрисида”ги Ўзбекистон Республикасининг қонуни ҳамда Қўмита Раисининг 2022 йил 27 апрелдаги 52-и/ч-сон бўйруғининг қўмитаси раиси ўринбосари, танлов комиссияси раиси ўринбосари, (Бердиқулов, Ахмедов, Влащенко, Отаниёзов, Воҳидов, Юнусов, Бердиқулов)

бўйруғини ижросини таъминлаш (ЛОТ 142534)

Қун тартибига қўйилган масала юзасидан Қўмита раиси ўринбосари, танлов комиссияси раиси С.Бердиқулов сузга чиқиб, “Киберхавфсизлик тўғрисида”ги Ўзбекистон Республикасининг қонуни ҳамда Қўмита Раисининг 2022 йил 27 апрелдаги 52-и/ч-сон бўйруғини ижросини таъминлаш мақсадида



berilganligini ma'lum kildi. 142534-sonli lot raqami orqali z'yon

Taklim etilgan 3 ta korxonada "ABB TECH SERVICE" MCHJ, "STARLAB" MCHJ va "NEW IT" MCHJ takliflari kelib tushganligi bilan

Tanlov komissiyasi kotibi K. Yunusov suzga chiqib, YPK-684-sonli "Davlat xaridlari tufarisida" ti konunni talaqlariga katiy riov kili sh buniyacha xamda budget va budgetdan tashkari ma'blaglar ni makadli tarzda foydalanishlari lozimligi tufarisida tushuntirish berib utdi xamda suzda davom etar ekan "NEW IT" MCHJ korxonasi tanlov talaqlaridaga xujжатlar tulik taklim kili nmatanligi sababli tanlovdan chetlatishilganligini, "ABB TECH SERVICE" MCHJ va "STARLAB" MCHJ korxonalari tanlov talaqlariga mos xujжатlar taklim kili nmatanligini bildirib utdi.

Tanlov komissiyasi a'zolarida mazkur 142534-son lot ish turokchilari bilan afxillan tanlik xususiyatiga era aloqalar mavjud emas. Uzbekiston Respublikasi "Davlat xaridlari tufarisida" ti Konunni (YPK-684-son, 22.04.2021 й.) 23-moddasiga kura, ish turokchi va uning afxillan tanlik kuyilgan masala yozasidan 2 (ikki) ish kuni davomida hech kanday takliflar kelib tushmadi va noroziliklar bildirilmadi. Maryulotlar stat.uz sahifasi orqali tekshirildi. Taklif etilgan narxlar kuyilgan belgilangan. 1. "ABB TECH SERVICE" MCHJ - 93 000 000,00 sum KKS bilan. 2. "STARLAB" MCHJ - 89 000 000,00 sum KKS bilan.

Komissiya qaror kildi: 1. Beterinariya va chorvachilikni rivojlantirish davlat kumitasi axborot tizimlari resurslarini kiberximov kili sh yu n sertifikatlatishilgan "Eset nod 32 smart security" antivirus dasturiy ta'minotini olish buyicha "STARLAB" MCHJ korxonasi ning taklif i bir ovozdan ma'kulangan. 2. "STARLAB" MCHJ tanlov fojib i deb topilgan va ushu korxonada bilan shartnoma imzolash makadli muvofik deb belgilangan. Ushu ba'innoma ijkrosi Molitva-iktisodiy taklim va buxgalteriya hisobi boshkarmasi bo shligi F. Axmedov zimmasiga otkatishin.

Tanlov komissiyasi a'zolari:

A. Vlasenko

F. Axmedov

L. Baxitov

J. Otanbayev







**Протокол закупочной комиссии по конкурсу лот № 142534 на приобретение Услуги по установке антивирусных программ**

Способ проведения электронный

Дата 07.09.2022

Время рассмотрения 03.09.2022 18:19

Конкурсная комиссия Узбекистон Республикаси Ветеринария ва Чорвачиликни ривожлантириш давлат кумитаси, (Далее – Комиссия) в составе:

**Председатель комиссии** BERDIKULOV SIKRIDDIN VALIKULOVICH  
Ветеринария ва чорвачиликни ривожлантириш давлат кумитаси Раис ўринбосари

**Секретарь комиссии** YUNUSOV KAMOLIDDIN XUSANOVICH  
Капитал қурлиши, таъминот ва маркетинг бўлими бош мутахассиси

**Член комиссии** OTANIYOZOV JAMSHID SAIDOVICH  
Хужалик мўдирли

**Член комиссии** VLASENKO ANDREY ANRIYEVICH  
Ахборот коммуникация ва технологияларни жорий қилиш бош мутахассиси

**Член комиссии** VOHIDOV LAZIZBEK HUSENOVICH  
Ветеринария ва чорвачиликни ривожлантириш давлат кумитаси Бош хисобчи

**Член комиссии** AXMEDOV FARID SAYFULLAYEVICH  
Молия-иқтисодий таҳлил ва бухгалтерия хисоби бошқармаси бошлиғи

**Член комиссии** Ветеринария ва чорвачиликни ривожлантириш давлат кумитаси

Наименование товара (работы, услуги)	Услуги по установке антивирусных программ
Подробное описание	Услуги по установке антивирусных
Количество товара	1.00
Единица измерения	
Цена товара (услуги) за единицу	95 000 000.00
Стартовая сумма	95 000 000.00
Валюта	UZS

Предмет закупки:

Мин. балл: 9

Расмотрев поступивших предложений со стороны участников по опубликованному объявлению на специальном информационном портале от 07.09.2022 года № лота 142534.

Метод оценки предложений – Метод наименьшей цены

По итогам рассмотрения поступивших предложений по технической части участником присвоены следующие



баллы:

Критерий №1 Услуги по установке антивирусных программ.

Тип: Текстовое значение

Описание: Наличие партнерского сертификата, предоставление авторизационного письма от производителя на имя ГОСУДАРСТВЕННЫЙ КОМИТЕТ ВЕТЕРИНАРИИ РЕСПУБЛИКИ УЗБЕКИСТАН подтверждающего факт того, что компания является официальным представителем продаваемой антивирусной программы.

Обязательность: Критично

Наименование	Макс	Значение	Балл	Значение	Балл	Тип	Примечание	Причина
АВВ ТЕCH SERVICE	10	10	10	10	10	Экспертная		
ООО STARLAB	10	авторизационное письмо № 18-08/22 от 18.08.2022 г., и партнёрский сертификат № RU220068, Партнёр ИД: 000013730 до 31.12.2022 г.	10	10	10	Экспертная		
ООО NEW IT	10	914330	0	0	0	Экспертная	Дисквалифицирован	Не представлено справка отсутствие задолженности по уплате налогов и других обязательных платежей, партнёрский сертификат и авторизационного письма.

Оценка участников финансовой части составила:

Наименование	Стартовая	Предлагаемая	Сумма с учетом конвертации (UZS)	Применение преференции	Общее значение (UZS)	Дата предложения	Оценка стоимости (балл)
АВВ ТЕCH SERVICE	95 000 000.00	93 000 000.00	93 000 000.00	00.00	93 000 000.00	31.08.2022 15:00:55	95.7
ООО STARLAB	95 000 000.00	89 000 000.00	89 000 000.00	00.00	89 000 000.00	31.08.2022 15:36:57	100

Итоговая оценка участников включая финансовую часть составила:

Наименование	Общий балл по технической части	Общий балл по финансовой части	Итоговый
АВВ ТЕCH SERVICE	Прошел	95.7	95.7
ООО NEW IT	Не прошел	Не прошел	Не прошел



Закупочная комиссия по конкурсу лот № 142534 от 07.09.2022 года на приобретение Услуги по установке антивирусных программ определила победителем:

ООО STARLAB  
304426154

и резервный исполнитель: АBB TECH SERVICE (301821568)

Проголосовали

100	100	Провел	100
-----	-----	--------	-----

Комиссия	Ф.И.О.	Голосование	Комментарии
Председатель комиссии	БЕРДИКУЛОВ СИРОИДИН ВАЛИКУЛОВИЧ	Согласен	
Член комиссии	ОТАНЙОЗОВ ЖАМШИД САИДОВИЧ	Согласен	
Член комиссии	ВЛАСЕНКО АНДРЕЙ АНРИЕВИЧ	Согласен	
Член комиссии	ВОИДОВ ЛАЗИЗБЕК ХУСЕНОВИЧ	Согласен	
Член комиссии	АХМЕДОВ ФАРИД САҒУЛЛАҒЕВИЧ	Согласен	

Протокол закупочной комиссии подписан посредством ЭЦП





УТВЕРЖДАЮ

Заместитель председателя  
 ГОСУДАРСТВЕННОГО КОМИТЕТА ВЕТЕРИНАРИИ  
 РЕСПУБЛИКИ УЗБЕКИСТАН  
 Бердикулов С.  
 «12» августа 2022 г.

Техническое задание на покупку антивирусного программного обеспечения на 200 пользователей (ИД № 1101/2022-01)

1	Наименование услуги	Покупка Антивирусного программного обеспечения на 200 пользователей сроком на 2 год.
2	Цель приобретения услуги	Служебная необходимость
3	Требования к поставщику (исполнителю)	Наличие партнерского сертификата, предоставление авторизационного письма от производителя на имя ГОСУДАРСТВЕННОГО КОМИТЕТА ВЕТЕРИНАРИИ РЕСПУБЛИКИ УЗБЕКИСТАН подтверждающего факт того, что компания является официальным представителем продаваемой антивирусной программы.
4	Требования к услуге	<p><b>Общие требования</b></p> <p>Антивирусная защита (АЗ) должна представлять собой масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети рабочих станций и серверов.</p> <p>В рамках всей организации должны использоваться единые антивирусные средства. Отдельно стоящие персональные компьютеры, то есть не подключенные к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированными программным продуктом, включающим в себя защиту от всех типов вредоносных программ (антивирус).</p> <p>Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке. Для организаций имеющих офисы за границей должна иметься возможность выбора языка интерфейса консоли управления для подключения к серверу администрирования, без переустановки консоли и сервера для ИТ персонала родной язык которого отличается от русского.</p> <p>Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке. Технические параметры программных средств антивирусной защиты должны соответствовать или превосходить следующие указанные параметры:</p> <p>Комплексная защита рабочих станций на ОС Windows и macOS с дополнительными функциями файрвола, аниспама и контроля доступа в интернет.</p>

	<p>Антивирусные средства и средства централизованного управления должны включать:</p> <ul style="list-style-type: none"> <li>• лицензионные файлы ключей для пакетов антивирусного программного обеспечения (АПО); при использовании схемы с несколькими серверами удаленного администрирования кластерная технология для организации связи между серверами не требуется дополнительных лицензий на связь между серверами.</li> <li>• программные средства антивирусной защиты рабочих станций, серверов и мобильных устройств (смартфонов, планшетов)</li> <li>• агент администрирования для выполнения связи между сервером администрирования и защищаемыми узлами</li> <li>• программные средства централизованного управления, мониторинга и обновления на ОС Windows, Linux/BSD, Mac OS, мобильные ОС Android;</li> <li>• программные средства централизованного управления должны иметь WEB консоль для управления и формирования отчетов;</li> <li>• централизованное управление может осуществляться с любого устройства через Web - браузер;</li> <li>• программные средства централизованного управления могут устанавливаться на Windows и Linux платформы</li> <li>• обновляемые антивирусные базы данных и компоненты ядра антивирусной системы;</li> <li>• Прокси-сервер - компонент для обеспечения высокой масштабируемости решения и уменьшения нагрузки на центральный сервер администрирования</li> <li>• наличие инструмента для обнаружения неизвестных компьютеров, осуществляющего автоматический поиск ПК в локальной сети, без необходимости осуществлять их ручной поиск и добавление;</li> <li>• наличие различных вариантов установки агентов администрирования клиентской части антивирусного программного обеспечения такие как:             <ul style="list-style-type: none"> <li>- Удаленно или локально;</li> <li>- Push установка;</li> <li>- Установка через e-mail;</li> <li>- Установка с применением съемного носителя, например USB;</li> <li>- Локальная установка;</li> </ul> </li> <li>• эксплуатационную документацию на русском языке.</li> <li>• Наличие выделенного программного инструмента для управления лицензиями. С его помощью можно отслеживать лицензии, активированные модули и связанные с лицензиями события, также как окончание срока действия, использование и авторизация.</li> <li>• Наличие выделенной утилиты для создания локального хранилища вирусных сигнатур, без использования сервера централизованного управления.</li> <li>• Наличие возможности организации двухфакторной аутентификации пользователей консоли сервера централизованного управления.</li> </ul>
--	---



	<p>• сервис <b>Дополнительного уровня безопасности</b> продуктов включающий встроенную песочницу</p> <p><b>Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows</b></p> <p>Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows Vista;</li> <li>• Microsoft Windows Vista x64;</li> <li>• Microsoft Windows 7</li> <li>• Microsoft Windows 7 x64.</li> <li>• Microsoft Windows 8</li> <li>• Microsoft Windows 8.1</li> <li>• Microsoft Windows 10</li> </ul> <p>Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:</p> <ul style="list-style-type: none"> <li>• интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением;</li> <li>• резидентный антивирусный мониторинг;</li> <li>• возможность полностью скрыть интерфейс антивирусного ПО</li> <li>• антивирусное сканирование по команде пользователя или администратора;</li> <li>• антивирусное сканирование по расписанию;</li> <li>• антивирусное сканирование при определенных условиях: <ul style="list-style-type: none"> <li>- после обновления антивирусных баз данных;</li> <li>- каждый раз при запуске компьютера;</li> <li>- каждые сутки при первом запуске компьютера;</li> <li>- при успешном Интернет или VPN соединении;</li> <li>- вход пользователя;</li> <li>- при обнаружении подозрительной активности, в том числе и активным модулем «защита в режиме реального времени».</li> </ul> </li> <li>- состояние простоя, автоматически сканирует локальные диски, если компьютер находится в состоянии простоя, в одном из следующих трех режимов: заставка, блокировка компьютера, выход пользователя</li> </ul> <ul style="list-style-type: none"> <li>• наличие задачи на выключение ПК по завершению сканирования антивирусное сканирование трафика по следующим протоколам: FTP, HTTP и HTTPS, POP3 и POP3S, а так же IMAP и IMAPs трафика.</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>• наличие дополнительного модуля по защите документов Microsoft Office и сканировании проходящих через Internet Explorer файлов</li> <li>• защита от еще неизвестных вредоносных программ на основе эвристического анализа;</li> <li>• возможность добавлять в исключения только определенные угрозы, в независимости от их местонахождения на ПК;</li> <li>• обнаружение скрытых процессов;</li> <li>• возможность устанавливать только необходимые компоненты антивирусной защиты (модульная установка);</li> <li>• возможность отключения антивирусной защиты при необходимости;</li> <li>• антивирусная проверка и лечение файлов, упакованных программами типа PKLITE, LZEXE, DLET, EXERACK и пр.;</li> <li>• антивирусная проверка и лечение файлов в архивах форматов ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE;</li> <li>• содержать настраиваемую систему предотвращения вторжений Host Intrusion Prevention System (HIPS) для предотвращения попыток внешнего воздействия, изменения, а так же для мониторинга процессов, файлов и ключей реестра;</li> <li>• возможность работы HIPS по ряду заранее подготовленных режимов фильтрации;</li> <li>• обеспечивать защиту от хакерских атак, путем использования межетевого экрана с системой обнаружения и предотвращения вторжений (IDS/NIPS) при работе в вычислительных сетях любого типа, включая беспроводные;</li> <li>• персональный файрвол;</li> <li>• возможность настройки нескольких профилей файрвола, с автоматическим переключением данных профилей, при выполнении определенных условий;</li> <li>• управление всем сетевым трафиком компьютера в обоих направлениях;</li> <li>• низкоуровневое сканирование трафика;</li> <li>• поддержка протокола IPv6;</li> <li>• поддержка встроенной песочницы для защиты от угроз нулевого дня;</li> <li>• модуль сканирования CERT;</li> <li>• выделенный модуль защиты от вирусов шифраторов;</li> <li>• задачи по расписанию и/или сразу после загрузки операционной системы;</li> <li>• возможность управления доступом к веб-ресурсам, путем создания списка заблокированных либо разрешенных веб-сайтов, а также путем запрета всех веб-сайтов, кроме тех, которые внесены в список разрешенных.</li> </ul>
--	--



- активный режим фильтрации для приложений, а так же возможность отключения фильтрации или перевод в пассивный режим для исключенных приложений;
- настраиваемый веб-контроль по категориям сайтов, позволяющий задавать правила применения политики использования сети Интернет на уровне пользователей или групп пользователей;
- Наличие в модуле веб-контроля возможности кастомизации страницы предупреждения или блокирования
- фильтрации для доверенных приложений;
- сканирование из контекстного меню;
- отключение фильтрации для доверенных веб-адресов;
- отключение фильтрации для доверенных IP адресов;
- возможность исключить из проверки доверенные процессы, хэш суммы, файлы и папки
- настройка нескольких профилей обновлений (например, для мобильных пользователей) с возможностью обновления из сети Интернет.
- Наличие агента администрирования антивирусного программного обеспечения (АПО) для рабочих станций
- наличие планировщика в клиенте антивирусного ПО;
- возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы;
- ядро и все основные модули продукта не требуют перезагрузки и активны сразу после установки;
- наличие специализированной утилиты для сбора файлов журналов антивирусного пакета для ускорения решения проблем при возможных проблемах с антивирусным пакетом
- наличие модуля сканирования в состоянии простоя, автоматически сканирует локальные диски, если компьютер находится в состоянии простоя, в одном из следующих трех режимов: заставка, блокировка компьютера, выход пользователя
- возможность подключения уже установленных лицензий антивирусной защиты рабочих станций к серверу централизованного управления без необходимости удаления существующего пакета антивирусной защиты, путем установки агента администрирования
- запуск обновления антивирусных баз данных после установки модемного соединения или VPN;
- возможность создания задачи запуска приложения стороннего провайдера в планировщике антивируса при определенных условиях или по временному интервалу;

- защита на лету от вредоносных скриптов, загружаемых с Web-страниц
- блокирование нежелательных и рекламных сообщений
- самобуцаемый антивирус;
- защита почтовых клиентов: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail;
- черные и белые списки антиспама, списки исключений
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- наличие функциональности использования общего локального кэша для повышения скорости сканирования в виртуализированных средах;
- защита от фишинга: защищает от попыток получить пароли и другую конфиденциальную информацию, запрещая доступ к вредоносным веб-сайтам, которые принимают вид нормальных веб-сайтов;
- Защита от эксплойтов: блокировщик эксплойтов контролирует поведение процессов и выявляет подозрительную активность, которая является типичной для целевых атак и ранее неизвестных эксплойтов – угроз нулевого дня
- наличие модуля сканирования памяти, который отслеживает поведение процессов и сканирует зловерные процессы, когда они снимают маскировку в памяти;
- защита от ботнетов: помогает обнаруживать вредоносные программы, анализируя их схемы обмена данными и протоколы регуляции распределения ресурсов рабочей станции между антивирусом и другими приложениями в зависимости от приоритетности задач; возможность продолжать антивирусное сканирование в фоновом режиме;
- настройка лимитов сканирования по параметрам – глубина вложенности (архивов), размера объекта и времени сканирования объекта;
- наличие модуля, позволяющего проводить автоматическое сканирование содержания подключаемых внешних устройств хранения данных, а так же применять расширенный анализ запуска файлов с таких устройств;
- наличие модуля, позволяющего настроить отращивания доступа (нет доступа, только чтение, полный доступ, предупреждение) для каждого пользователя или для группы пользователей как по типу устройства (CD/DVD/Blu-Ray, USB хранения данных, USB принтеры, устройства обработки изображений, устройства FireWire, карты ридеров, модемов, LPT/SOM порты, Bluetooth устройства) так и по заданным атрибутам (производитель, модель, серийный номер) задавая одно правило на несколько устройств;
- интеграция с MS NAP и CISCO NAC;
- возможность формирования аварийных дампов памяти, на случай сбоя приложения
- возможность отката обновлений вирусных баз на предыдущие версии и приостановка их обновления с последующим



	<p>автоматическим включением обновления через указанный промежуток времени;</p> <ul style="list-style-type: none"> <li>наличие функциональности возобновлять прерванные загрузки без данных ситнаур вирусов и модули продуктов при обновлении;</li> <li>интеграция с центром безопасности Windows;</li> <li>интеграция с центром обновления Windows, для установки патчей закрывающих обнаруженные уязвимости, с выбором необходимых обновлений от «необязательных» обновлений до «критических»;</li> <li>настройка проверки исполняемых файлов и загрузочных областей компьютера в качестве отдельной задачи;</li> <li>технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или некавалифицированных пользователей;</li> <li>проверка наличия актуальных обновлений системы;</li> <li>наличие настраиваемой функции автоматического скрытия уведомлений при работе антивируса для приложений, работающих в фоновом режиме, т.е. при работе приложения в фоновом режиме на экран не выводятся информационные уведомления о работе антивирусного программного обеспечения;</li> <li>наличие множества путей уведомления администраторов о важных событиях, происходящих на рабочих станциях (почтовое сообщение, всплывающее окно, запись в журнал событий);</li> <li>обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на отужаемых носителях информации;</li> <li>экспорт логов и отчетов в форматы XML, TXT, DAT, OMR;</li> <li>наличие облачной технологии детектирования неизвестных угроз, контроль приложений на основе репутационного сервиса;</li> <li>наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную;</li> <li>возможность создания дисков аварийного восстановления;</li> <li>экономия электроэнергии в режиме автономного питания;</li> <li>системные требования не должны превышать: 300мб RAM, HDD 1тб, Processor Intel или AMD, одноканальный, x86 или x64 ППТ, размер дистрибутива антивирусного пакета не должен превышать – 165 Мб.</li> </ul> <p><b>Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows</b></p> <p>Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:</p> <ul style="list-style-type: none"> <li>Microsoft Windows Server 2008 (x86 и x64)</li> <li>Microsoft Windows Server 2008 R2</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>Microsoft Windows Server 2012</li> <li>Microsoft Windows Server 2012 R2</li> <li>Microsoft Windows Server 2016</li> <li>Microsoft Windows Server 2019</li> <li>Microsoft Windows Server 2008 x64 R2 SP1 / x64 R2 CORE</li> <li>Microsoft Windows Server 2008 x86 SP2 / x64 SP2 CORE</li> <li>Microsoft Windows Server 2012 x64 / x64 CORE</li> <li>Microsoft Windows Server 2012 x64 R2 / x64 R2 CORE</li> <li>Microsoft Windows Server 2012 R2</li> <li>Microsoft Windows Server 2008 R2</li> <li>Microsoft Windows Server 2012</li> <li>Microsoft Windows Server 2012 R2</li> <li>Серверы Storage, Small Business и MultiPoint:       <ul style="list-style-type: none"> <li>Microsoft Windows Storage Server 2008 R2 Essentials с пакетом обновления 1</li> <li>Microsoft Windows Storage Server 2012</li> <li>Microsoft Windows Storage Server 2012 R2</li> <li>Microsoft Windows Small Business Server 2008 (x64)</li> <li>Microsoft Windows Small Business Server 2011 (x64)</li> <li>Microsoft Windows Server 2012 Essentials</li> <li>Microsoft Windows Server 2012 R2 Essentials</li> <li>Microsoft Windows MultiPoint Server 2010</li> <li>Microsoft Windows MultiPoint Server 2011</li> <li>Microsoft Windows MultiPoint Server 2012</li> </ul> </li> </ul> <p>Программные средства антивирусной защиты файловых серверов под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:</p> <ul style="list-style-type: none"> <li>интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением;</li> <li>резидентный антивирусный мониторинг;</li> <li>антивирусное сканирование по команде пользователя или администратора;</li> <li>антивирусное сканирование по расписанию;</li> <li>антивирусное сканирование при определенных условиях:       <ul style="list-style-type: none"> <li>после обновлений антивирусных баз данных;</li> <li>каждый раз при запуске компьютера;</li> <li>каждые сутки при первом запуске компьютера;</li> <li>при успешном Интернет или VPN соединении;</li> <li>вход пользователя;</li> </ul> </li> <li>при обнаружении подозрительной активности, в том числе и активным модулем «защита в режиме реального времени»;</li> <li>антивирусное сканирование трафика по следующим протоколам: FTP, HTTP и HTTPS, а так же POP3 и POP3s трафика антивирусное сканирование Нурер-V на наличие вирусов на безагентной основе</li> </ul>
--	--



	<ul style="list-style-type: none"> <li>• защита от еще неизвестных вредоносных программ на основе эвристического анализа;</li> <li>• поддерживать настраиваемую систему предотвращения вторжений Host Intrusion Prevention System (HIPS) для предотвращения попыток внешнего воздействия, изменения, а так же для мониторинга процессов, файлов и ключей реестра;</li> <li>• возможность работы HIPS по ряду заранее подготовленных режимов фильтрации</li> <li>• возможность добавлять в исключения только определенные угрозы, в независимости от их местонахождения на ПК;</li> <li>• возможность исключить определенные процессы приложений, хэш суммы из сканирования на наличие вирусов;</li> <li>• обнаружение руткитов (скрытых файлов/системных аномалий);</li> <li>• антивирусная проверка и лечение файлов, улакованных программами типа РКЛТЕ, LZEK, DIET, EKERACK и пр.;</li> <li>• антивирусная проверка и лечение файлов в архивах форматов ARJ, BZZ, CAB, CHM, DVX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE;</li> <li>• запуск задач по расписанию и/или сразу после загрузки операционной системы;</li> <li>• возможность создания задачи запуска приложения стороннего производителя в планировщике антивируса;</li> <li>• защита на лету от вредоносных сценариев, загружаемых с Web-страниц;</li> <li>• возможность настройки параметров антивирусного пакета из интерфейса командной строки</li> <li>• функция автоматического обнаружения и исключения файлов на сервере, имеющих критическое значение для бесперебойной работы;</li> <li>• возможность задать количество модулей сканирования для увеличения скорости сканирования;</li> <li>• возможность управления доступом к веб-ресурсам, путем создания списка заблокированных либо разрешенных веб-сайтов, а также путем запрета всех веб-сайтов, кроме тех, которые внесены в список разрешенных;</li> <li>• активный режим фильтрации для приложений, а так же возможность отключения фильтрации или перевод в пассивный режим для исключенных приложений;</li> <li>• сканирование из контекстного меню;</li> <li>• отключение фильтрации для доверенных веб-адресов;</li> <li>• многооточное сканирование;</li> <li>• настройка нескольких профилей обновлений (например для мобильных пользователей) с возможностью обновления из интернета</li> <li>• наличие планировщика в антивирусном пакете.</li> <li>• наличие агента администрирования антивирусного программного обеспечения (АПО) для файловых серверов</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>• возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы;</li> <li>• ядро и все основные модули продукта не требуют перезагрузки и активны сразу после установки;</li> <li>• возможность подключения уже установленных лицензий антивирусной защиты рабочих станций к серверу централизованного управления без необходимости удаления существующего пакета антивирусной защиты, путем установки агента администрирования ;</li> <li>• наличие облачной технологии детектирования неизвестных угроз, контроль приложенный на основе репутационного сервиса;</li> <li>• запуск обновления антивирусных баз после установки модемного соединения или VPN;</li> <li>• ускорение процесса сканирования за счет пропуски объектов, состояние которых со времени прошлой проверки не изменилось;</li> <li>• наличие специализированной утилиты для сбора файлов журналов о конфигурации системы, установке и функционировании антивирусного пакета для ускорения решения проблем при возможных проблемах с антивирусным пакетом</li> <li>• наличие функциональности использования общего локального кэша для повышения скорости сканирования в виртуализированных средах;</li> <li>• защита от фишинга: защищает от попыток получить пароли и другую конфиденциальную информацию, запрещая доступ к вредоносным веб-сайтам, которые принимают вид нормальных веб-сайтов;</li> <li>• Защита от эксплойтов: блокировка эксплойтов контролирует поведение процессов и выявляет подозрительную активность, которая является типичной для целевых атак и ранее неизвестных эксплойтов – угроза нулевого дня</li> <li>• поддержка встроенной песочницы для защиты от угроз нулевого дня;</li> <li>• модуль сканирования UEFI;</li> <li>• выделенный модуль защиты от вирусов шифраторов;</li> <li>• модуль защиты от сетевых атак;</li> <li>• модуль защиты от ботнетов;</li> <li>• наличие модуля сканирования памяти, который отслеживает поведение процессов и сканирует зловердные процессы, когда они снимают маскировку в памяти;</li> <li>• регулировка распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;</li> </ul>
--	--



	<p>возможность продолжать антивирусное сканирование в фоновом режиме;</p> <ul style="list-style-type: none"> <li>• настройка лимитов сканирования по параметрам – глубина вложенности (архивов), размера объекта и времени сканирования объекта;</li> <li>• блокировка сменных носителей информации и устройств (USB);</li> <li>• наличие модуля, позволяющего настроить ограничение доступа (нет доступа/только чтение/полный доступ/предупреждение) для каждого пользователя или для группы пользователей как по типу устройства (CD/DVD/Blu-Ray, USB хранилища данных, USB принтеры, устройства обработки изображений, устройства FireWire, карт ридеров, модемов, ЦРТ/СОМ порты, Bluetooth устройства) так и по заданным атрибутам (производитель, модель, серийный номер); задавать одно правило на несколько устройств;</li> <li>• интеграция с центром безопасности Windows;</li> <li>• интеграция с центром обновления Windows, для установки патчей закрывающих обнаруженные уязвимости, с выбором необходимых обновлений от «необязательных» обновлений до «критических»;</li> <li>• поддержка Windows Management Instrumentation</li> <li>• настройка проверки исполняемых файлов и загрузочных областей компьютера в качестве отдельной задачи;</li> <li>• поддержка кластерных систем с возможностью автоматического обновления антивирусного ПО (автоматическая синхронизация конфигурации ПО на кластерах)</li> <li>• технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неавторизованных пользователей;</li> <li>• проверка наличия актуальных обновлений операционной системы;</li> <li>• полноценная работа без графического интерфейса, администрирование и конфигурирование АПО через командную строку;</li> <li>• возможность автоматизации работы за счет выполнения сценариев, позволяющих конфигурировать АПО и выполнять какие-либо действия;</li> <li>• автоматическое скрытие уведомлений при работе антивируса в полноэкранном режиме;</li> <li>• наличие настраиваемой функции автоматического скрытия уведомлений при работе антивируса для приложений, работающих в полноэкранном режиме;</li> <li>• наличие множества путей уведомления администраторов о важных событиях, происходящих на серверах (почтовое сообщение, всплывающее окно, запись в журнал событий);</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>• обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на отуждаемых носителях информации;</li> <li>• наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную;</li> <li>• возможность создания дисков аварийного восстановления;</li> <li>• размер дистрибутива антивирусного пакета не должен превышать – 127 Мб.</li> </ul> <p><b>Требования к средствам антивирусной защиты мобильных устройств</b></p> <p>Программные средства для антивирусной защиты смартфонов и планшетов должны функционировать под управлением мобильных ОС:</p> <p>Android 5 (Lollipop) и выше</p> <p>Программные средства антивирусной защиты смартфонов должны обеспечивать следующие функциональные возможности:</p> <ul style="list-style-type: none"> <li>• возможность проведения аудита безопасности устройства с генерацией отчета;</li> <li>• постоянная защита файловой системы смартфона, планшета;</li> <li>• проверка всех приложений, файлов, папок и карты памяти в режиме реального времени;</li> <li>• проверка объектов файловой системы, находящихся на смартфоне или на подключенных картах расширения памяти, по требованию пользователя и по расписанию;</li> <li>• надежное изолирование зараженных объектов в карантинном хранилище;</li> <li>• обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов;</li> <li>• блокирование нежелательных SMS и MMS сообщений;</li> <li>• контроль приложений для отслеживания установленных приложений, блокировать доступ к определенным приложениям и снижать степень риска, предлагая пользователям удалять некоторые программы;</li> <li>• задание минимальных уровней безопасности и сложность кодов разблокировки экрана;</li> <li>• указание максимального количества неудачных попыток разблокировки экрана;</li> <li>• указание максимального срока действия для кода разблокировки экрана;</li> <li>• настройка таймера блокировки экрана;</li> <li>• ограничить использование камеры;</li> <li>• защита от фишинга: защита пользователей от попыток получить пароли, банковские данные и прочую конфиденциальную информацию незаконными веб-сайтами, выдающими себя за законные</li> <li>• центр уведомлений: предоставляет сведения о разных событиях, о причинах их несоответствия корпоративным политикам и о том как эту несоответствие устранить</li> </ul>
--	---



- защита от кражи и утери смартфона. Обеспечить возможность удаленной блокировки мобильного устройства;
- возможность дистанционно удалить информацию со смартфона;
- возможность определить доверенную SIM-карту;
- возможность скрывать отправку уведомлений посредством SMS-сообщения, с предупреждением об использовании не доверенной SIM-карты. Так же сообщение должно включать информацию, необходимую для идентификации злоумышленника: телефонный номер текущей SIM-карты, номер IMEI и номер IMEI телефона;
- расширенный сбор до заводских установок: все доступные на устройстве данные будут удалены (заголовки файлов будут уничтожены). Кроме того, на телефоне будут восстановлены заводские настройки по умолчанию
- возможность включить сирену: Потерянное устройство блокируется и начинает издавать очень громкий звук, даже если звук на устройстве отключен
- Наличие встроенного агента администрирования антивирусного программного обеспечения (АПО)
- Системные требования: Операционная система: Android 5 (Lollipop) и более поздние версии. Разрешение сенсорного экрана: 480 x 800 пкс. Процессор: ARM с набором инструкций ARMv7 или x86 Intel Atom. Свободное место для хранения данных: 20MB.

**Требования к системе управления антивирусной защитой**

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:

- Масштабируемое решение: масштабирование производится за счет использования прокси серверов
- интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением;
- Прокси- сервер - компонент для обеспечения высокой масштабируемости решения и уменьшения нагрузки на центральный сервер администрирования
- наличие инструмента для обнаружения неизвестных компьютеров, осуществляющий автоматический поиск ПК в локальной сети, без необходимости осуществлять их ручной поиск и добавление;
- централизованная установка/обновление/удаление программных средств антивирусной защиты, настройки, администрирование;
- централизованный сбор информации и создание отчетов о состоянии антивирусной защиты;
- защищенное соединение между сервером и клиентом;
- программные средства централизованного управления должны иметь WEB консоль для управления и формирования отчетов;
- централизованное управление может осуществляться с любого устройства через Web - браузер;
- создание отчетов в наглядном графическом виде;
- экспорт логов и отчетов в форматы HTML, TXT, CSV, PDF;
- наличие модуля поддержки SIEM;

- предварительная настройка политики для групп или клиентов (профили обновлений, запрещенные сайты, расписание планировщика и т.д.);
- возможность отправки сообщений, как на мобильные устройства, так и на персональные компьютеры;
- возможность удаленного создания журнала аудита безопасности с мобильного устройства
- возможность установки пользовательских приложений;
- наличие различных вариантов установки агентов администрирования клиентской части антивирусного программного обеспечения также как:
- удаленно или локально :
  - Push установка,
  - Установка через e-mail,
  - Установка с применением съемного носителя , например USB.
  - Локальная установка;
- наличие возможности автоматически выбирать соответствующий установочный пакет агента для операционных систем или в ручном режиме.
- настройка политики безопасности для клиентов;
- возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы;
- возможность удаленного запуска определенного сценария на конечных клиентах. Предназначенного для удаления/изменения критических объектов системы.
- отсутствие необходимости перезагрузки ПК после установки системы управления антивирусной защитой;
- автоматизированное обновление программных средств антивирусной защиты и антивирусных баз;
- возможность прокинуть быстрый отчет обновлений сигнатурных баз для отдельных компьютеров или групп;
- доставка обновлений на рабочие места пользователей сразу после их получения;
- централизованный карантин;
- возможность создания групп управляемых компьютеров как вручную, так и автоматически на основе структуры Active Directory;
- возможность синхронизации с Active Directory как по расписанию, так и вручную;
- автоматический поиск незащищенных рабочих станций с учетом топологии сети;
- аудит изменений в настройках сервера по четным записям;
- построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;



	<ul style="list-style-type: none"> <li>• обновление программных средств и антивирусных баз из различных источников, как по каналам связи, так и на носителях информации;</li> <li>• механизм оповещения о событиях в работе установленных приложений антивирусной защиты и возможность настройки рассылки почтовых уведомлений о них;</li> <li>• наличие системы передачи образов вредоносного кода вирусным экспертам автоматически или вручную;</li> <li>• возможность создания динамических групп, в которые динамически будут включаться клиентские станции при соответствии условиям данных групп;</li> <li>• работа со статическими и динамическими группами</li> <li>• различные варианты уведомлений администратора сети ( по e-mail, использование SNMP-ловушки);</li> <li>• возможность создания резервных копий содержимого базы данных и настроек сервера;</li> <li>• возможность подключения к консоли сервера удаленного администрирования с использованием доменных имени пользователя и пароля;</li> <li>• администрирование серверов и рабочих станций Windows, Linux/BSD, а так же решений для защиты мобильных ОС (Android);</li> <li>• наличие функции пробуждения по локальной сети Wake on LAN</li> <li>• возможность автоматического определения «клонированных машин» с помощью сложной логики обнаружения отпечатков оборудования;</li> <li>• наличие протокола для репликации, с использованием «DNS» (Push Notification Service) и поддержкой многоадресных вызовов для WOL.</li> <li>• функционал для инвентаризации оборудования;</li> <li>• наличие функции быстрого отключения или включения уведомлений на выбранных компьютерах для прерывания или возобновления обмена данными с сервером администрирования</li> <li>• поддержка баз данных MS SQL, MySQL;</li> <li>• программные средства централизованного управления могут устанавливаться на Windows и Linux платформы</li> <li>• программные средства должны поддерживать установку на отказоустойчивые кластеры Windows и Linux платформ сервер удаленного администрирования может быть установлен и должен поддерживать операционные системы Windows Server: <ul style="list-style-type: none"> <li>o Windows Server 2003 x86 SP2 /x64 SP2</li> <li>o Windows Server 2003 x86 R2 SP2 /x64 R2 SP2</li> <li>o Windows Server 2008 x64 R2 SP1 / x64 R2 CORE</li> <li>o Windows Server 2008 x86 SP2 / x64 SP2</li> <li>o Windows Server 2012 x64 /x64 CORE</li> <li>o Windows Server 2012 x64 R2 / x64 R2 CORE</li> <li>o Windows Server 2016 x64</li> <li>o Windows Server 2019 x64</li> <li>o Microsoft SBS 2003 x86 SP2 / x86 R2</li> <li>o Microsoft SBS 2008 x64 SP2</li> <li>o Microsoft SBS 2011 x64 Standard / x64 Essential</li> </ul> </li> <li>Linux: <ul style="list-style-type: none"> <li>o Ubuntu 12.04 LTS x86 Desktop / Server</li> <li>o Ubuntu 12.04 LTS x64 Desktop / Server</li> <li>o Ubuntu 14.04 LTS x86 Desktop / Server</li> <li>o Ubuntu 14.04 LTS x64 Desktop / Server</li> <li>o RHEL Server 6 x86 / x64</li> </ul> </li> </ul>
--	---

	<ul style="list-style-type: none"> <li>o RHEL Server 7 x86 / x64</li> <li>o CentOS 6 x86 / x64</li> <li>o CentOS 7 x86 / x64</li> <li>o SLED 11 x86 / x64</li> <li>o SLES 11 x86 /x64</li> <li>o SLES 11 x86 /x64</li> <li>o OpenSUSE 13 x86 / x64</li> <li>o Debian 7 x86 / x64</li> <li>o Fedora 19 x86 / x64</li> </ul> <ul style="list-style-type: none"> <li>• Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий: <ul style="list-style-type: none"> <li>o VMware vSphere/ESXi (версии 5.0 и новее)</li> <li>o VMware Workstation (версии 9 и новее)</li> <li>o VMware Player (версии 7 и новее)</li> <li>o Microsoft Hyper-V (Server 2012 и 2012 R2)</li> <li>o Oracle VirtualBox (версии 4.3.24 и новее)</li> </ul> </li> </ul> <p>Наличие выделенного программного инструмента для управления лицензиями. С его помощью можно отслеживать лицензии, активированные модули и связанные с лицензиями события, такие как окончание срока действия, использование и авторизация. Работа с инструментом под разными ролями как владелец лицензии или как администратор безопасности.</p> <p>Возможность выполнять следующие действия:</p> <ul style="list-style-type: none"> <li>• просматривать состояние лицензий в реальном времени;</li> <li>• отслеживать отдельные устройства (и при этом их отключать);</li> <li>• настраивать уведомления, связанные с событиями лицензий;</li> <li>• хранить лицензии одновременно в старой и новой формах в смешанных средах;</li> <li>• обменивать ключи лицензий на сообщения электронной почты и пароли, с помощью которых также можно активировать программы;</li> <li>• назначать несколько лицензий на одну учетную запись;</li> <li>• разрешать другим лицам использовать лицензии (активировать их);</li> <li>• настраивать уведомления для более удобного отслеживания состояния лицензий;</li> <li>• наличие функции синхронизации с сервером централизованного управления.</li> <li>• наличие выделенной утилиты для мигрирования с более ранних версий антивирусного программного обеспечения с сохранением настроек политик и информационной базы журналов событий.</li> </ul>
--	--



	<ul style="list-style-type: none"> <li>• наличие выделенной утилиты для создания локального хранилища вирусных сигнатур, без использования сервера централизованного управления.</li> <li>• наличие возможности организации двухфакторной аутентификации пользователей консоли сервера централизованного управления. Поддержка двухфакторной аутентификации для 10 пользователей консоли сервера централизованного управления. При использовании данной функциональности должно быть использовано решение двухфакторной аутентификации того же производителя, что и сам пакет антивирусного программного обеспечения.</li> <li>• наличие возможности деактивации лицензий на узлах через создание заданий на сервере управления.</li> </ul> <p><b>Сервис дополнительного уровня безопасности продуктов</b> для защиты рабочих станций, файловых и почтовых серверов с помощью встроенной песочницы на основе технологий машинного обучения для обнаружения новых, ранее неизвестных угроз.</p> <p>В сервисе должна быть реализована следующая функциональность:</p> <ul style="list-style-type: none"> <li>• Детектирование на основе анализа поведения</li> <li>• Машинное обучение</li> <li>• Обнаружение угроз нулевого дня</li> <li>• Встроенная песочница</li> </ul> <p>Сервис на основе технологий машинного обучения для обнаружения новых, ранее неизвестных угроз поставляется в составе решения по антивирусной защите рабочих станций, файловых серверов локальной сети заказчика.</p> <ul style="list-style-type: none"> <li>• Наличие поддержки антивирусными продуктами дополнительной функциональности, активируемой отдельной лицензией. Сервис предназначен для продуктов того же производителя антивирусного обеспечения, что и сам сервис. Сервис должен активироваться и управляться из центра обеспечения безопасности системы.</li> <li>• Сервис должен поддерживать работу с антивирусными решениями по защите рабочих станций, файловых серверов и почтовых серверов.</li> <li>• Для работы с сервисом необходим только доступ в сеть интернет, никаких аппаратных средств в сети заказчика не требуется.</li> </ul> <p>Сервис должен обеспечивать:</p> <ul style="list-style-type: none"> <li>• Многоуровневую защиту - иметь не менее 3 моделей машинного обучения. Система выполняет работу с образцами в виртуальной среде или в песочнице. Система моделирует поведение пользователей, чтобы обмануть образцы вредоносных программ и использует модели нейронных сетей Deep Learning для сравнения поведения образцов с поведением всех известных образцов вредоносных программ.</li> </ul>
--	--

	<ul style="list-style-type: none"> <li>• Детальный обзор - Каждый изучаемый образец отображается в консоли центра безопасности, где наглядно и удобно представлена детальная информация о его характеристиках и происхождении.</li> <li>• Высокую скорость анализа – предоставлять анализ 90% неизвестных образцов в течение 5 минут</li> <li>• Мобильность – наличие возможности анализа файлов вне зависимости от местонахождения пользователей в корпоративной сети или за ее пределами.</li> <li>• Наличие возможности отправки подзорительных файлов вручную или автоматически на основе конфигурации политики.</li> <li>• Возможность отправки файлов вручную из веб-консоли Центра обеспечения безопасности или с клиентских компьютеров с активированным сервисом.</li> <li>• Возможность управлять действиями сервиса через API Центра обеспечения безопасности</li> <li>• Наличие возможности отправки больших файлов объемом до 64 Мб</li> <li>• Поддерживаемые типы файлов для отправки на проверку: <ul style="list-style-type: none"> <li>• Документы (.docx, .xlsx, .lft и др.)</li> <li>• Исполняемые файлы (файлы .exe, .dll, .sys и др.)</li> <li>• JAR, LNK, REG, MSI, SWF и др</li> <li>• Сценарии (.bat, .cmd, .js, .vbs, .ps и др.)</li> <li>• Ole2 - при использовании с продуктами по защите почтовых серверов</li> <li>• .hta</li> </ul> </li> <li>• Наличие функциональности предоставления отчета о поведении проверенного образца, в котором будет приведено краткое описание поведения наблюдаемого образца.</li> </ul> <p>В Отчете о файле должна содержаться следующая информация:</p> <ul style="list-style-type: none"> <li>• Имя компьютера, отправившего файл</li> <li>• указание Пользователя на исходном компьютере, отправившего файл. В некоторых случаях это может быть системный пользователь</li> <li>• Причина отправки (автоматически, вручную),</li> <li>• указана Часть облака, получившая файл</li> <li>• Хеш SHA1 отправленного файла.</li> <li>• Имя файла и его полный путь в файловой системе отправителя.</li> <li>• Размер файла.</li> <li>• Категория файла (тип файла).</li> </ul> <p>Наличие в отчете параметров: <b>Состояние</b> и <b>Статус</b>:</p> <ul style="list-style-type: none"> <li>• <b>Состояние</b> означает текущее состояние файла в процессе выполнения анализа</li> <li>• <b>Статус</b> означает результат анализа поведения или отсутствие результата</li> </ul> <p>Наличие категории статуса, присвоенного проверенным образцам, которое отображается в консоли центра управления или в отчете по образцу:</p>
--	--



	<p>• Не заражено - Модули обнаружения не идентифицируют образцы как вредоносны.</p> <p>• <b>Подозрительный</b> - Модуль обнаружения определил поведение файла как подозрительно, но не вредоносное.</p> <p>• <b>Вредоносный</b> - Поведение файла считается вредоносным.</p> <p>• Наличие функциональности распространения результатов о проверенных файлах во все продукты для обеспечения безопасности в компании пользователя в течение не более 2 минут</p> <p>• Наличие функциональности предоставления списка о всех переданных файлах в консоль Центра обеспечения безопасности. Можно просмотреть список отправленных файлов в выделенном разделе консоли.</p> <p>• Возможность настройки отправки образцов в консоли Центра обеспечения безопасности</p> <p>• Возможность настройки исключений для образцов и настройки политик для продуктов обеспечения безопасности в консоли Центра обеспечения безопасности.</p>
	<p><b>Требования к обновлению антивирусных баз</b></p> <p>Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:</p>
	<ul style="list-style-type: none"> <li>• реализована возможность создания зеркала обновлений для экономии трафика;</li> <li>• зеркала обновлений можно создать на любом ПК сети не зависимо от используемой операционной системы Windows/Linux, в том числе и на конечной рабочей станции при помощи AV-клиента с обязательным наличием как минимум двух путей раздачи обновлений (NTPP и SMB), для активации зеркала не должна требоваться установка дополнительных модулей, как на сервер, так и на рабочую станцию;</li> <li>• типы обновлений: обновление БД сигнатур вирусов, программных компонентов, обновление ядра;</li> <li>• пакеты обновления зеркала можно загружать двумя способами: по протоколу HTTP (рекомендуется) и с помощью общего сетевого диска (SMB);</li> <li>• обновления можно распространять на электронных носителях информации (FDD\CD\DVD\ USB-drive);</li> <li>• осуществляется проверка целостности и подлинности обновлений средствами электронной цифровой подписи.</li> </ul> <p><b>Требования к эксплуатационной документации</b></p> <p>Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы на русском языке, в том числе:</p> <ul style="list-style-type: none"> <li>• руководство пользователя (администратора);</li> </ul>

5	Срок оказания услуги		<ul style="list-style-type: none"> <li>• руководство администратора средств удаленного администрирования.</li> </ul> <p>Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.</p> <p><b>Требования к технической поддержке</b></p> <p>Техническая поддержка программного обеспечения должна:</p> <ul style="list-style-type: none"> <li>• предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории следующих стран: Российская Федерация, Республика Казахстан, Республика Беларусь, Киргизская Республика, Республика Молдова, Республика Таджикистан, Республика Узбекистан, круглосуточно без праздников и выходных (24x7) по электронной почте и через Интернет, а также по телефону.</li> <li>• Веб-сайт производителя АЗ должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке, поопыляемую базу знаний и русскоязычный форум.</li> </ul>
---	----------------------	--	---

Составил:



Ахборот коммуникация  
технологиялари жорий  
этиш бўлими бош  
мутахассиси



А. Власенко

Ташкилот номи	Сони
Кўмита марказий аппарати	93
Ўзбекчорванасл агентлиги	39
Давлат чегараси ва транспортдаги давлат ветеринария назорати бошқармаси	15
Виртуальные машины и сервера	10
Захира	43
Жами	200

Ветеринария ва чорвачиликни  
ривожлантириш давлат  
қўмитаси расми ўринбосари  
С.Бердикүлова



**Ахборот коммуникация  
технологияларини жорий  
этиш бўлими бош мутахассиси**



**А. Влащенко**

“Киберхавфсизлик тўғрисида”ги Ўзбекистон Республикасининг Қонуни ҳамда Ветеринария ва чорвачиликни ривожлантириш давлат қўмитаси раисининг 2022 йил 27 апрелдаги 52-и/ч-сон бўйруғининг ижросини таъминлаш мақсадида соҳада ахборот тизимлари ресурсларини киберхимоя қилиш учун сертификатлаштирилган 200 та компьютер жамланмасига етадиган Esset nod 32 smart security антивирус дастурий таъминотини олишда амалий ёрдам беришни тизини сураймиз.

**БИЛДИРГИ**

**Ветеринария ва чорвачиликни  
ривожлантириш давлат  
қўмитаси раиси ўринбосари  
С. Бердикүлова**

*Handwritten signature and stamp in blue ink*  
U. Zokirov  
P. Qulobekov  
Kuputov