«УТВЕРЖДАЮ»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г.

**ДОКУМЕНТАЦИЯ ОБ АУКЦИОНЕ В ЭЛЕКТРОННОЙ ФОРМЕ**

**на поставку, монтаж, пуско-наладку системы периметральной защиты ИТ инфраструктуры Академии от сетевых угроз**

Болгар 2020 г.

# Часть 1. Информационная карта

|  |  |  |
| --- | --- | --- |
| 1 | Способ процедуры закупки  | Аукцион в электронной форме |
| 2 | Наименование покупателя  | Мусульманская религиозная организация духовная образовательная организация высшего образования «Болгарская исламская академия» |
| 3 | ИНН/КПП покупателя  | 1637008095/163701001 |
| 4 | Место нахождения покупателя  | 422840, Республика Татарстан Спасский р-н, Болгар, ул. Кул Гали, д. 1А |
| 5 | Номер контактного телефона покупателя, Адрес электронной почты  | 89673675345alinatkachuk1987@inbox.ru |
| 6 | Предмет закупки  | Поставка, монтаж, пуско-наладка системы периметральной защиты ИТ инфраструктуры Академии от сетевых угроз |
| 7 | Количество поставляемого товара, объема выполняемых работ, оказываемых услуг | В соответствии с частью 4 «Техническое задание» настоящей Документации |
| 8 | Место поставки товара (выполнения работ, оказания услуг) | 422840, Республика Татарстан Спасский р-н, Болгар, ул. Кул Гали, д. 1А |
| 9 | Дата начала подачи заявок  | 23.12.2020 г. |
| 10 | Дата и время окончания подачи заявок на участие в процедуре закупке  | 21.01.2021 г. в 11 час. 00 мин. |
| 11 | Дата рассмотрения заявок на участие в процедуре закупки  | 21.01.2021 г. в 14 час. 00 мин. – дата рассмотрения первых частей заявок на участие в аукционе;25.01.2021 г. в 10 час. 00 мин. – дата рассмотрения вторых частей заявок на участие в аукционе |
| 12 | Дата и время проведения аукциона  | 22.01.2021 г. в 11 час. 00 мин.  |
| 13 | Начальная (максимальная) цена договора  | 1 699 803, 00  |
| 14 | Размер обеспечения заявки  | 16 998,03 (1%) |
| 15 | Размер обеспечения исполнения контракта | 169 980,30 (10%) |
| 16 | Адрес электронной площадки, на которой будет проводиться процедура закупки  | https://etpzakupki.tatar |

# Часть 2. Общие сведения

**1. Приглашение к участию в электронном аукционе**

Настоящим приглашаются к участию в электронном аукционе, проводимом на сайте электронной площадки <https://etpzakupki.tatar>, любые юридические лица независимо от организационно-правовой формы, формы собственности, места нахождения и места происхождения капитала либо любое физическое лицо, в том числе индивидуальный предприниматель.

На сайте <https://etpzakupki.tatar> будут публиковаться все разъяснения, касающиеся настоящей документации, а также все изменения или дополнения документации, в случае возникновения таковых.

**2. Общие сведения о покупателе и законодательное регулирование закупки**

2.1. Покупатель: Мусульманская религиозная организация духовная образовательная организация высшего образования «Болгарская исламская академия» (далее – Покупатель).

Место нахождения, почтовый адрес Покупателя: 422840, Республика Татарстан Спасский р-н, Болгар, ул. Кул Гали, д. 1А.

Адрес электронной почты: alinatkachuk1987@inbox.ru

Номер контактного телефона: 89673675345

Контактное лицо: Ткачук Алина Илдусовна

2.2. Предмет электронного аукциона:поставка, монтаж, пуско-наладка системы периметральной защиты ИТ инфраструктуры Академии от сетевых угроз

**3. Требования к содержанию и составу заявки на участие в электронном аукционе.**

Для участия в электронном аукционе участник закупки, получивший аккредитацию на электронной площадке, подает заявку на участие в электронном аукционе. Порядок получения аккредитации на электронной площадке регулируется оператором электронной площадки.

Подача участниками закупки заявки на участие в электронном аукционе означает согласие и присоединение участника закупки к регламенту проведения торгов оператора электронной площадки.

Заявка на участие в аукционе в электронной форме подготавливается и подается посредством программных и технических средств электронной площадки согласно регламенту работы электронной площадки.

**Заявка на участие в электронном аукционе состоит из двух частей. Первая часть заявки на участие в электронном аукционе должна содержать**:

1. Согласие участника электронного аукциона на поставку товара (выполнение работы, оказание услуги) на условиях, предусмотренных документацией об аукционе и не подлежащих изменению по результатам проведения аукциона;

2. Конкретные показатели предлагаемого для поставки товара, соответствующие значениям эквивалентности, установленным документацией о закупке, если участник закупки предлагает для поставки товар, который является эквивалентным товару, указанному в документации о закупке, при условии содержания в документации о закупке указания на товарный знак, а также требования о необходимости указания в заявке на участие в электронном аукционе на товарный знак (в случае, если участник закупки предлагает для поставки товар, указание на товарный знак которого содержится в документации о закупке, указание сведений о конкретных показателях не требуется).

**Вторая часть заявки на участие в электронном аукционе должна содержать следующие документы и информацию:**

1. Для юридического лица:

а) фирменное наименование, адрес местонахождения, почтовый адрес (для юридического лица), фамилия, имя, отчество, паспортные данные (для физического лица), банковские реквизиты, номер контактного телефона;

б) для участников аукциона - российских юридических лиц копию полученной не ранее чем за шесть месяцев до дня опубликования извещения о проведении данного аукциона выписки из единого государственного реестра юридических лиц;

в) документ, подтверждающий полномочия лица на осуществление действий от имени участника закупки - юридического лица (копия решения о назначении или об избрании либо приказа о назначении физического лица на должность, в соответствии с которым такое физическое лицо обладает правом действовать от имени участника закупки);

г) копии учредительных документов участника аукциона.

2. Для индивидуального предпринимателя:

а) фамилия, имя, отчество;

б) паспортные данные;

в) место жительства;

г) номер контактного телефона;

д) идентификационный номер налогоплательщика (при наличии) участника закупки или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика (при наличии) участника закупки;

е) копия выписки из единого государственного реестра индивидуальных предпринимателей, полученной не ранее чем за шесть месяцев до даты размещения в единой информационной системе извещения о проведении процедуры закупки.

**4. Порядок подачи заявки участником процедуры закупки**.

Участник закупки вправе подать только одну заявку на участие в закупке в отношении предмета закупки (лота) в любое время с момента размещения извещения о ее проведении до предусмотренных документацией о закупке даты и времени окончания срока подачи заявок на участие в закупке.

Участник закупки вправе изменить или отозвать свою заявку до окончания срока подачи заявок. Заявка на участие в закупке является измененной или отозванной, если изменение осуществлено или уведомление об отзыве заявки получено Покупателем до окончания срока подачи заявок на участие в закупке.

Участнику закупки при заполнении заявки рекомендуется использовать общепринятые обозначения и наименования, а также избегать формулировок, допускающих неоднозначное толкование.

Обязательства участника закупки, связанные с подачей заявки, включают:

1) обязательство заключить договор на условиях, указанных в проекте договора, являющегося неотъемлемой частью документации о проведении электронного аукциона, и заявки, а также обязательство предоставить Покупателю обеспечение исполнения договора в случае, если такая обязанность установлена условиями документации;

2) обязательство не предоставлять в составе заявки заведомо недостоверные сведения, информацию, документы;

3) согласие на обработку персональных данных.

**5. Дата и время окончания срока подачи заявок на участие в электронном аукционе**

В соответствии с пунктом 10 часть 1 «Информационная карта» настоящей документации.

**6. Дата окончания срока рассмотрения заявок на участие в электронном аукционе**

В соответствии с пунктом 11 «Информационная карта» настоящей документации.

**7. Дата и время проведения электронного аукциона**

В соответствии с пунктом 12 часть 1 «Информационная карта» настоящей документации.

**8. Порядок формирования цены договора**

Цена договора включает в себя стоимость товара, его доставку и установку, а так же уплату налогов и других обязательных платежей в соответствии с действующим законодательством Российской Федерации, с учетом расходов на перевозку, страхование, уплату таможенных пошлин и других обязательных платежей.

**9. Начальная (максимальная) цена договора**

**Начальная (максимальная) цена договора 1 699 803** **(один миллион шестьсот девяносто девять тысяч восемьсот три рубля) 00 копеек.**

Обоснование начальной (максимальной) цены договора приведено в части 3 «Обоснование начальной максимальной цены договора» к настоящей документации.

**10. Сведения о валюте, используемой для формирования цены договора и расчётов с поставщиками (исполнителями, подрядчиками)**

Российский рубль.

**11. Требования к безопасности, качеству, техническим характеристикам, функциональным характеристикам (потребительским свойствам) товара, работы, услуги, к размерам, упаковке, отгрузке товара, к результатам работы, установленные покупателем и предусмотренные техническими регламентами в соответствии с законодательством Российской Федерации о техническом регулировании, документами, разрабатываемыми и применяемыми в национальной системе стандартизации, принятыми в соответствии с законодательством Российской Федерации о стандартизации, иные требования, связанные с определением соответствия поставляемого товара, выполняемой работы, оказываемой услуги потребностям покупателя. Если покупателем в документации о закупке не используются установленные в соответствии с законодательством Российской Федерации о техническом регулировании, законодательством Российской Федерации о стандартизации требования к безопасности, качеству, техническим характеристикам, функциональным характеристикам (потребительским свойствам) товара, работы, услуги, к размерам, упаковке, отгрузке товара, к результатам работы, в документации о закупке должно содержаться обоснование необходимости использования иных требований, связанных с определением соответствия поставляемого товара, выполняемой работы, оказываемой услуги потребностям Покупателя.**

В соответствии с частью 4 «Техническое задание» настоящей Документации.

**12. Место поставки товара, выполнения работ, оказания услуг**

В соответствии с пунктом 8 часть 1 «Информационная карта» настоящей документации.

**13. Условия и сроки (периоды) поставки товара, выполнения работ, оказания услуг**

В соответствии с частью 4 «Техническое задание» настоящей Документации.

**14. Форма, сроки и порядок оплаты товара, работ, услуг**

В соответствии с частью 5 «Проект договора с приложениями» настоящей Документации.

**15. Срок, место и порядок предоставления документации о закупке**

Документация находится в свободном доступе в единой информационной системе и доступна в любое время с момента размещения без взимания платы.

**16. Критерии и порядок оценки и сопоставления заявок на участие в закупке**

Единственным критерием закупки является цена договора.

При проведении электронного аукциона его участники подают предложения о цене договора, предусматривающие снижение текущего минимального предложения о цене договора на величину в пределах «шага аукциона».

Величина снижения начальной (максимальной) цены договора («шаг аукциона») составляет от 0,5 процента до 5 процентов начальной (максимальной) цены договора.

**17. Заключение договора по результатам проведения аукциона**

1. Договор по результатам проведения электронного аукциона заключается в течение десяти дней с даты размещения на электронной площадке итогового протокола, составленного по результатам закупки.

2. В случае уклонения победителя электронного аукциона от заключения договора, Покупатель вправе принять решение о заключении договора с участником закупки, который предложил такую же, как и победитель закупки, цену договора или предложение которого содержит лучшую цену договора, следующую после цены, предложенной победителем закупки. Такой участник закупки не вправе отказаться от заключения договора. В случае уклонения такого участника закупки от заключения договора, Покупатель вправе осуществить закупку у единственного поставщика (исполнителя, подрядчика).

# Часть 3. Обоснование начальной максимальной цены договора

Для определения и обоснования начальной (максимальной) цены договора использовался метод сопоставимых рыночных цен (анализа рынка), путем выбора наименьшей цены из рассмотренных коммерческих предложений:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование | Коммерческое предложение 1 | Коммерческое предложение 2 | Итоговая цена |
|  | Поставка оборудования для системы хранения данных  | 1 699 803,00 | 2 894 430,00 | **1 699 803, 00** |

**Часть 4**.

**Техническое задание на поставку, монтаж, пуско-наладку системы периметральной защиты ИТ инфраструктуры Академии от сетевых угроз.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование товара** | **Наименование характеристик и требуемые значения** | **Ед. изм.** | **Кол-во** |
| **1.** | **Аппаратная платформа сертифицированной ФСТЭК версии UserGate D 500** | Производительность Межсетевой экран: до 20 Гб/c Система обнаружения вторжений: до 2 000 Мб/с Контентная фильтрация: до 2 100 Мб/c Инспектирование SSL: до 750 Мб/c Контроль Приложений L7: до 2 100 Мб/c Одновременных TCP сессий: до 16 000 000 Новых сессий в секунду до 160 000Поддержка VRRP кластеризации – поддерживаетСпецификация оборудования Портов 10/100/1000Base-T: 5 встроено, 2 SFP 1 GbpsУправление по IPMI: есть Процессор, количество ядер: 8 Память: 32 Гбайт Диск: 1х1000 Гбайт Размеры Габариты: 1U 438 x 321 x 44 мм Вес: 7.5 кг Крепление в стойку: Кронштейны Электропитание Сеть питания: 140-220 Вольт Потребляемая мощность (Макс): 220 ВаттСистема должна иметь действующий сертификат соответствия ФСТЭК России на соответствие следующим требованиям:- «Требования к межсетевым экранам» (ФСТЭК России, 2016) к межсетевым экраном типов «А» и «Б», «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты» ИТ.МЭ.А4.ПЗ (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты» ИТ.МЭ.Б4.ПЗ (ФСТЭК России, 2016);- «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012).Поставляемое оборудование должно быть собрано в промышленных условиях, удовлетворяющих стандарту ISO9001, иметь сертификаты соответствия требованиям системы сертификации ЕАС.Исполнитель должен обеспечить срок гарантийного обслуживания не менее 3 (трех) лет. | **шт.** | **2** |
| **2.** | **Лицензия без ограничения числа пользователей для UserGate D500 на кластер из 2-х нод с сертификатом ФСТЭК** | Требования к программной составляющей:Общие требования к архитектуре* + 1. Программное обеспечение должно обладать следующей функциональностью:
* Межсетевой экран (МСЭ) следующего поколения (Next Generation Firewall) с фильтрацией по сетевым протоколам, контролем приложений на уровне L7 и контролем пользователей;
* Система обнаружения и предотвращения вторжений (СОВ), распознающая вредоносную активность внутри сети;
* Защита от DOS-атак и сетевого флуда;
* Работа с внешними системами безопасности I-CAP и DLP;
* Поддержка контроля трафика АСУ ТП;
* Дополнительную антивирусную проверку трафика с использованием эвристического анализа;
* Мониторинг действий, совершаемых пользователями при работе с сетью Интернет, а также формирование отчетности.
	+ 1. Функционал настройки средств фильтрации входящего и исходящего трафика должен позволять указывать в качестве фильтра маску или регулярное выражение.
		2. Функционал применения правил МСЭ к фрагментированным, не фрагментированным, любым пакетам.
		3. Наличие события о успешной загрузке системы в журнале событий
		4. Логирования изменения времени в консоли администрирования.
		5. Наличие оповещений по SNMP при срабатывании запрещающих правил межсетевого экрана
		6. Блокировка всего трафика при инциденте, нарушении функционирования системы. Если исполняемый файл, из состава МСЭ, будет изменен, то весь трафик должен быть заблокирован.
		7. Функционал решения должен иметь возможность запрашивать ввод пароля на разблокировку трафика и изменения, добавления правила в МСЭ в случае несанкционированного доступа к: изменениям правил МСЭ, правил оповещения, сетевым интерфейсам, добавлению учетной записи нового администратора, экспорту логов системы.
		8. Возможность удаленного подключения технической поддержки в случае полного отказа системы.
		9. Фильтрация входящего и исходящего Интернет-трафика должна осуществляться с одновременным обеспечением проверки на наличие вредоносного программного обеспечения.
		10. Средства, реализующие функционал мониторинга работоспособности и формирования отчетности, должны предоставлять функционал автоматизированного получения данных о действиях пользователей, совершаемых в сети Интернет, от средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.
		11. Наличие функционала настройки интерфейсов:
* Поддержка VLAN;
* Поддержка bonding, объединения интерфейсов в один логический агрегированный интерфейс с поддержкой протокола LACP для повышения пропускной способности и отказоустойчивости;
* Поддержка режимов моста L2 и L3 для фильтрации трафика в прозрачном режиме, не затрагивающим сетевую инфраструктуру Заказчика.
	+ 1. Средства управления трафиком, контроля доступа в сеть Интернет и фильтрации трафика сети Интернет, должны иметь функциональность:
* Обеспечивать маршрутизацию трафика с использованием статических маршрутов, динамической маршрутизации по протоколам OSPF и BGP и использования политик маршрутизации;
* Обеспечивать публикацию ресурсов с помощью reverse-прокси для HTTP/HTTPS и DNAT для других протоколов;
* Иметь функционал балансировки нагрузки;
* Поддерживать управление пропускной способностью;
* Работать в качестве непрозрачного и прозрачного сервера-Интернет и обеспечивать кэширование HTTP, HTTPS;
* Поддерживать аутентификацию пользователей, интегрироваться с доменами, построенными на базе Microsoft Active Directory и поддерживать технологию Single Sign-On;
* Поддерживать аутентификацию пользователей с внешними серверами Radius, Kerberos, Active Directory, FreeIPA, TACACS+, локальной базой учетных записей. Поддержка мультифакторной аутентификации;
* Поддерживать аутентификацию пользователей, работающих на терминальных серверах Microsoft Windows, и на рабочих станциях, работающих под управлением ОС Microsoft Windows, с использованием агентов авторизации.
* Поддерживать аутентификацию пользователей, находящихся за NAT без дополнительного ПО;
* Обеспечивать разделение прав при доступе к сети Интернет на основе доменных и локальных групп и поддерживать управление разрешениями;
* Поддерживать работу гостевого портала;
* Управлять доступом в сеть Интернет программ и сетевых служб путём разрешения и назначения портов и использованием сигнатур приложений;
	+ 1. Система обнаружения и предотвращения вторжений (СОВ) должна иметь следующую функциональность:
* Распознавать вредоносную активность внутри сети;
* Иметь возможность создания различных профилей СОВ, релевантных защите определенных сервисов;
* Иметь возможность создание правил СОВ, определяющих действия для выбранного типа трафика, проверяемого модулем СОВ в соответствии с назначенным профилем СОВ.
	+ 1. Функционал антивирусной фильтрации с эвристическим анализом должен обеспечивать:
* Фильтрацию трафика методами эвристического анализа для модуля контентной фильтрации;
	+ 1. Требования к доступности и производительности
* Программное обеспечение должно иметь возможность реализации в соответствии с методом обеспечения высокой доступности, гарантируя минимальное время простоя, и полного решения возложенных задач при выходе из строя одного из компонентов, путем объединения двух и более узлов. Должен обеспечиваться режим работы отказоустойчивого режима кластера Активный-Активный и Активный-Пассивный с синхронизацией пользовательских сессий;
* Программное обеспечение должно иметь возможность создания кластера конфигураций;
* Программное обеспечение должно обеспечивать резервное копирование конфигураций компонентов и журналов регистрации событий с функцией исторического хранения данных с глубиной хранения не менее 12 месяцев;
* Программное обеспечение должно обеспечивать доступ в сеть Интернет без ограничения числа пользователей, подключенных к Интернет;
* Программное обеспечение должно иметь возможность работы с несколькими провайдерами Интернет с возможностью настройки балансировки и переключения в случае отказа одного из них;
* Программное обеспечение должно иметь возможность масштабирования. Увеличение числа обслуживаемых пользователей и объема обрабатываемого трафика сети Интернет должно осуществляться путем подключения дополнительных программно-аппаратных компонентов;
* Программное обеспечение должно позволять в любое время выводить часть узлов фильтрации из эксплуатации для обслуживания с автоматическим перераспределением нагрузки на оставшиеся узлы прозрачно для пользователей. При наличии дополнительных узлов;
* Должен обеспечиваться функционал настройки программно-аппаратных средств, входящих в состав, без остановки всей Системы;
* Программное обеспечение должно обеспечивать функцию планового отключения для выполнения профилактических мероприятий, изменений или наращивания аппаратного обеспечения, установки обновлений на программное обеспечение;
* Программное обеспечение должно предоставлять инструменты диагностирования состояния собственных компонентов;
* В Программное обеспечение должна быть предусмотрена ролевая модель разграничения доступа. Роли должны иметь ограничения по доступу к Программному обеспечению на уровне интерфейсов, функционала, отчетов и производственных объектов;
* Входящие в состав Программного обеспечение программные компоненты должны быть российского производства.

Требования к автоматизации* + 1. Контроль доступа пользователей в сеть Интернет с функционалом установки различных политик доступа для различных групп пользователей на основе членства в группах безопасности службы каталогов Microsoft Active Directory;
		2. Обновление баз сигнатур с периодичностью не реже 1 (одного) раза в неделю;
		3. Настраиваемые оповещения администраторов Системы о событиях в работе средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет;
		4. Уведомление в окне браузера пользователя сети Интернет о блокировании доступа к запрашиваемому пользователем web-ресурсу в случае нарушения корпоративных требований информационной безопасности, а также на основании наличия потенциально опасного кода (с функцией правки кода и текста уведомления);
		5. Поддержка автоматизации безопасности при помощи механизмов сценариев (концепция SOAR), сокращающая время реакции на события безопасности;
		6. Автоматическое или ручное обновление программных компонентов с сайта производителя, а также обновление в режиме off-line;
		7. Управление доступом к средствам контроля доступа в сеть Интернет и фильтрации трафика сети Интернет с использованием ролевой модели;
		8. Протоколирование действий администраторов Системы.

Требования к функционалу средств мониторинга и отчетностиСредства мониторинга функционирования и формирования отчетности должны обеспечивать выполнение следующих функций:* + 1. Протоколирование действий пользователей и администраторов Системы.
		2. Возможность, в режиме on-line, отслеживания текущей сессии пользователя, определения сервера, через который установлена сессия, подключения к серверу и разбора пользовательской сессии.
		3. Определение геолокации на основе IP-адреса домена.
		4. Формирование отчетности с функционалом:
* объявления пользовательских (новых) полей;
* формирования запросов с использованием перекрестных запросов.
	+ 1. Формирование отчетности с предоставлением функционала:
* задания фильтров по всем (любым) полям, поддерживаемым средствами мониторинга функционирования и формирования отчетности;
* формирования запросов к базе данных;
* задания формата отчетов.
	+ 1. Отправку отчетов по расписанию и по запросу администраторов Системы.
		2. Отключение мониторинга функционирования и формирования отчетности для конкретных пользователей/IP-адресов.
		3. Управление доступом к средствам мониторинга и отчетности с использованием ролевой модели.

Требования к функционалу средств контентного анализа:Средства контентного анализа передаваемой информации должны обеспечивать выполнение следующих функций:* + 1. Получение информации от средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.
		2. Обеспечение следующих видов фильтрации (анализа) передаваемого контента:
* анализ передаваемых объектов по типу передаваемых объектов, в том числе определение и корректная обработка распространенных форматов файлов, применяемых в офисном ПО (Microsoft Office, PDF, TXT и т.д.);
* поиск и анализ регулярных выражений (ключевых слов);
* лингвистический (морфологический) анализ.
	+ 1. Управление доступом к средствам контентного анализа с использованием ролевой модели.

Связь с существующим окружением и интеграция * + 1. Разграничение полномочий доступа для работы с Системой и доступа пользователей в сеть Интернет должно быть реализовано на ролевой основе с использованием групп существующих доменов Active Directory.
		2. Система должна взаимодействовать со следующими смежными системами:
* Система авторизации в соответствии с типом используемого механизма с системами авторизации пользователей Заказчика;
* Система синхронизации времени, в части взаимодействия с системой синхронизации времени должна поддерживать определение точного времени;
* Система доменных имен (DNS), в части взаимодействия с системой DNS должно поддерживать определение IP-адресов узлов сети по имени узла;
* Система мониторинга SNMP, в части взаимодействия с системой мониторинга SNMP должно поддерживать оповещение и работу в режиме запросов состояния системы по протоколам SNMP v2 и SNMP v3;
* Корпоративная почтовая система (E-mail), в части взаимодействия с корпоративной почтовой системой должно поддерживать отправку по E-mail оповещений администраторам о событиях в работе средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет;
* Система сбора и корреляции событий информационной безопасности, в части взаимодействия с системами сбора и корреляции событий информационной безопасности должно предоставлять механизм экспорта журнальных сообщений в режиме реального времени. Формат и детализация данных сообщений должны настраиваться;
* Системы дополнительного контентного анализа, в части взаимодействия с системами дополнительного контентного анализа должно предоставлять модуль интеграции по протоколу I-CAP с указанными системами в части условий доступа на основании результатов анализа контента.

Требования к пользовательскому интерфейсу* + 1. Программный интерфейс компонентов Системы, включая средства управления, а также формы оповещений и уведомлений администраторов Системы и пользователей сети Интернет должен полностью поддерживать русский язык, используя кодировку текста UTF-8.
		2. Наличие web-интерфейса для доступа к компонентам узла фильтрации Интернет-трафика, включая средства управления, полностью поддерживающего русский язык, используя кодировку текста UTF-8.

Требования к наличию отчетовСистема должна обеспечивать формирование отчетности в табличном и графическом виде о совершаемых пользователями действиях в сети Интернет за различные периоды времени.1.8 Требования к сертификацииСистема имеет действующий сертификат соответствия ФСТЭК России на соответствие следующим требованиям:* «Требования к межсетевым экранам» (ФСТЭК России, 2016) к межсетевым экраном типов «А» и «Б», «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты» ИТ.МЭ.А4.ПЗ (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты» ИТ.МЭ.Б4.ПЗ (ФСТЭК России, 2016);
* «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012).
 | **шт.** | **1** |
| **3.** | **Модуль Advanced Threat Protection на 1 год для UserGate D500 без ограничения числа пользователей** | Программное обеспечение должно обладать следующей функциональностью, в течение не менее 1 (одного) календарного года с момента активации, без ограничения числа пользователей:* Контроль доступа пользователей в сеть Интернет и фильтрации трафика сети Интернет с обеспечением защиты от вредоносного программного обеспечения;
* Анализ трафика сети Интернет по категориям сайтов, URL-адресам и контенту данных, включая морфологический анализ;
* Обеспечивать категорирование ресурсов сети Интернет и обеспечивать фильтрацию доступа пользователей на основе данных категорий;
* Обеспечивать фильтрацию доступа пользователей к ресурсам сети Интернет на основе контентной фильтрации;
* Поддерживать и автоматически обновлять базу данных ресурсов сети Интернет и присвоенных им категорий;
* Управлять доступом к сайтам сети Интернет на основе «чёрных» и «белых» списков, составленных с использованием категоризации сайтов;
* Функционал настройки фильтрации входящего и исходящего трафика должен позволять указывать в качестве фильтра маску или регулярное выражение. Списки категорий сайтов должны предоставляться производителем средств контроля доступа в сеть Интернет. Для Администраторов Программное обеспечения должна быть реализована функция внесения корректировок в данные списки, а также создания собственных категорий. Списки должны формироваться путём внесения не только одиночных сайтов, но и их списков (в формате текстовых файлов с разделителями);
* Иметь возможность отключения функционала контроля доступа в сеть Интернет и фильтрации трафика сети Интернет для конкретных пользователей/IP-адресов.
* Обеспечивать управление доступом пользователей к различным типам информации в сети Интернет (видео, аудио, изображения и т.д.);
* Обеспечивать управление доступом пользователей к возможности передачи в сеть Интернет информации различных типов (видео, аудио, изображения и т.д.);
* Предоставлять интерфейс гибкой настройки правил фильтрации на основе различных параметров, в частности, групп доступа пользователей, категорий ресурсов (в том числе и ресурсов, не отнесенных ни к одной из категорий) и типов передаваемого контента;
* Поддерживать и автоматически обновлять список сайтов на основе единой автоматизированной информационной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»;
* Обеспечивать фильтрацию передаваемого контента и блокировку определенных типов файлов, в том числе в SSL-трафике, а также поддерживать выполнение антивирусной проверки передаваемого контента;
* Предоставлять функционал гибкой настройки правил фильтрации на основе различных параметров, в частности, групп доступа пользователей, категорий ресурсов, отдельных ресурсов (в том числе ресурсов, не отнесенных ни к одной из категорий) и типов передаваемого контента;
* Обеспечивать выборочную блокировку рекламы;
* Обеспечивать активацию безопасного поиска;
* Обеспечивать DNS-фильтрацию запросов пользователей и режим DNS-прокси;
* Предоставлять интегрированные механизмы оповещения и уведомления администраторов и пользователей о событиях;
* Предоставлять клиента для авторизации и фильтрации на АРМ пользователей.
 | **Шт.** | **1** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование товара** | **Наименование характеристик и требуемые значения** | **Ед. изм.** | **Кол-во** |
| **4.** | **Аппаратная платформа сертифицированной ФСТЭК версии UserGate С 100** | **Производительность**Межсетевой экран: до 2 Гб/c Система обнаружения вторжений: до 800 Мб/с Контентная фильтрация: до 200 Мб/c Инспектирование SSL: до 70 Мб/c Контроль Приложений L7: до 850 Мб/c Одновременных TCP сессий: до 2 000 000 Новых сессий в секунду до 34 000 Поддержка VRRP кластеризации – поддерживает**Спецификация оборудования**Количество портов: 5 Управление по IPMI: есть Процессор, количество ядер: 4Память: 8 Гбайт Диск: 1х500 Гбайт **Размеры**Габариты: Tabletop 230 x 170 x 47.7 ммВес: 1,2 кг **Электропитание**Сеть питания: 140-220 Вольт Потребляемая мощность (Макс): 36 ВаттСистема должна иметь действующий сертификат соответствия ФСТЭК России на соответствие следующим требованиям:- «Требования к межсетевым экранам» (ФСТЭК России, 2016) к межсетевым экраном типов «А» и «Б», «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты» ИТ.МЭ.А4.ПЗ (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты» ИТ.МЭ.Б4.ПЗ (ФСТЭК России, 2016);- «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012).Поставляемое оборудование должно быть собрано в промышленных условиях, удовлетворяющих стандарту ISO9001, иметь сертификаты соответствия требованиям системы сертификации ЕАС.Исполнитель должен обеспечить срок гарантийного обслуживания не менее 3 (трех) лет. | **шт.** | **2** |
| **5.** | **Лицензия для UserGate до 50 пользователей на кластер из 2-х нод с сертификатом ФСТЭК** | Требования к программной составляющей:Общие требования к архитектуре* + 1. Программное обеспечение должно обладать следующей функциональностью:
* Межсетевой экран (МСЭ) следующего поколения (Next Generation Firewall) с фильтрацией по сетевым протоколам, контролем приложений на уровне L7 и контролем пользователей;
* Система обнаружения и предотвращения вторжений (СОВ), распознающая вредоносную активность внутри сети;
* Защита от DOS-атак и сетевого флуда;
* Работа с внешними системами безопасности I-CAP и DLP;
* Поддержка контроля трафика АСУ ТП;
* Дополнительную антивирусную проверку трафика с использованием эвристического анализа;
* Мониторинг действий, совершаемых пользователями при работе с сетью Интернет, а также формирование отчетности.
	+ 1. Функционал настройки средств фильтрации входящего и исходящего трафика должен позволять указывать в качестве фильтра маску или регулярное выражение.
		2. Функционал применения правил МСЭ к фрагментированным, не фрагментированным, любым пакетам.
		3. Наличие события о успешной загрузке системы в журнале событий
		4. Логирования изменения времени в консоли администрирования.
		5. Наличие оповещений по SNMP при срабатывании запрещающих правил межсетевого экрана
		6. Блокировка всего трафика при инциденте, нарушении функционирования системы. Если исполняемый файл, из состава МСЭ, будет изменен, то весь трафик должен быть заблокирован.
		7. Функционал решения должен иметь возможность запрашивать ввод пароля на разблокировку трафика и изменения, добавления правила в МСЭ в случае несанкционированного доступа к: изменениям правил МСЭ, правил оповещения, сетевым интерфейсам, добавлению учетной записи нового администратора, экспорту логов системы.
		8. Возможность удаленного подключения технической поддержки в случае полного отказа системы.
		9. Фильтрация входящего и исходящего Интернет-трафика должна осуществляться с одновременным обеспечением проверки на наличие вредоносного программного обеспечения.
		10. Средства, реализующие функционал мониторинга работоспособности и формирования отчетности, должны предоставлять функционал автоматизированного получения данных о действиях пользователей, совершаемых в сети Интернет, от средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.
		11. Наличие функционала настройки интерфейсов:
* Поддержка VLAN;
* Поддержка bonding, объединения интерфейсов в один логический агрегированный интерфейс с поддержкой протокола LACP для повышения пропускной способности и отказоустойчивости;
* Поддержка режимов моста L2 и L3 для фильтрации трафика в прозрачном режиме, не затрагивающим сетевую инфраструктуру Заказчика.
	+ 1. Средства управления трафиком, контроля доступа в сеть Интернет и фильтрации трафика сети Интернет, должны иметь функциональность:
* Обеспечивать маршрутизацию трафика с использованием статических маршрутов, динамической маршрутизации по протоколам OSPF и BGP и использования политик маршрутизации;
* Обеспечивать публикацию ресурсов с помощью reverse-прокси для HTTP/HTTPS и DNAT для других протоколов;
* Иметь функционал балансировки нагрузки;
* Поддерживать управление пропускной способностью;
* Работать в качестве непрозрачного и прозрачного сервера-Интернет и обеспечивать кэширование HTTP, HTTPS;
* Поддерживать аутентификацию пользователей, интегрироваться с доменами, построенными на базе Microsoft Active Directory и поддерживать технологию Single Sign-On;
* Поддерживать аутентификацию пользователей с внешними серверами Radius, Kerberos, Active Directory, FreeIPA, TACACS+, локальной базой учетных записей. Поддержка мультифакторной аутентификации;
* Поддерживать аутентификацию пользователей, работающих на терминальных серверах Microsoft Windows, и на рабочих станциях, работающих под управлением ОС Microsoft Windows, с использованием агентов авторизации.
* Поддерживать аутентификацию пользователей, находящихся за NAT без дополнительного ПО;
* Обеспечивать разделение прав при доступе к сети Интернет на основе доменных и локальных групп и поддерживать управление разрешениями;
* Поддерживать работу гостевого портала;
* Управлять доступом в сеть Интернет программ и сетевых служб путём разрешения и назначения портов и использованием сигнатур приложений;
	+ 1. Система обнаружения и предотвращения вторжений (СОВ) должна иметь следующую функциональность:
* Распознавать вредоносную активность внутри сети;
* Иметь возможность создания различных профилей СОВ, релевантных защите определенных сервисов;
* Иметь возможность создание правил СОВ, определяющих действия для выбранного типа трафика, проверяемого модулем СОВ в соответствии с назначенным профилем СОВ.
	+ 1. Функционал антивирусной фильтрации с эвристическим анализом должен обеспечивать:
* Фильтрацию трафика методами эвристического анализа для модуля контентной фильтрации;
	+ 1. Требования к доступности и производительности
* Программное обеспечение должно иметь возможность реализации в соответствии с методом обеспечения высокой доступности, гарантируя минимальное время простоя, и полного решения возложенных задач при выходе из строя одного из компонентов, путем объединения двух и более узлов. Должен обеспечиваться режим работы отказоустойчивого режима кластера Активный-Активный и Активный-Пассивный с синхронизацией пользовательских сессий;
* Программное обеспечение должно иметь возможность создания кластера конфигураций;
* Программное обеспечение должно обеспечивать резервное копирование конфигураций компонентов и журналов регистрации событий с функцией исторического хранения данных с глубиной хранения не менее 12 месяцев;
* Программное обеспечение должно обеспечивать доступ в сеть Интернет не менее чем 50 пользователей, подключенных к Интернет;
* Программное обеспечение должно иметь возможность работы с несколькими провайдерами Интернет с возможностью настройки балансировки и переключения в случае отказа одного из них;
* Программное обеспечение должно иметь возможность масштабирования. Увеличение числа обслуживаемых пользователей и объема обрабатываемого трафика сети Интернет должно осуществляться путем подключения дополнительных программно-аппаратных компонентов;
* Программное обеспечение должно позволять в любое время выводить часть узлов фильтрации из эксплуатации для обслуживания с автоматическим перераспределением нагрузки на оставшиеся узлы прозрачно для пользователей. При наличии дополнительных узлов;
* Должен обеспечиваться функционал настройки программно-аппаратных средств, входящих в состав, без остановки всей Системы;
* Программное обеспечение должно обеспечивать функцию планового отключения для выполнения профилактических мероприятий, изменений или наращивания аппаратного обеспечения, установки обновлений на программное обеспечение;
* Программное обеспечение должно предоставлять инструменты диагностирования состояния собственных компонентов;
* В Программное обеспечение должна быть предусмотрена ролевая модель разграничения доступа. Роли должны иметь ограничения по доступу к Программному обеспечению на уровне интерфейсов, функционала, отчетов и производственных объектов;
* Входящие в состав Программного обеспечение программные компоненты должны быть российского производства.

Требования к автоматизации* + 1. Контроль доступа пользователей в сеть Интернет с функционалом установки различных политик доступа для различных групп пользователей на основе членства в группах безопасности службы каталогов Microsoft Active Directory;
		2. Обновление баз сигнатур с периодичностью не реже 1 (одного) раза в неделю;
		3. Настраиваемые оповещения администраторов Системы о событиях в работе средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет;
		4. Уведомление в окне браузера пользователя сети Интернет о блокировании доступа к запрашиваемому пользователем web-ресурсу в случае нарушения корпоративных требований информационной безопасности, а также на основании наличия потенциально опасного кода (с функцией правки кода и текста уведомления);
		5. Поддержка автоматизации безопасности при помощи механизмов сценариев (концепция SOAR), сокращающая время реакции на события безопасности;
		6. Автоматическое или ручное обновление программных компонентов с сайта производителя, а также обновление в режиме off-line;
		7. Управление доступом к средствам контроля доступа в сеть Интернет и фильтрации трафика сети Интернет с использованием ролевой модели;
		8. Протоколирование действий администраторов Системы.

Требования к функционалу средств мониторинга и отчетностиСредства мониторинга функционирования и формирования отчетности должны обеспечивать выполнение следующих функций:* + 1. Протоколирование действий пользователей и администраторов Системы.
		2. Возможность, в режиме on-line, отслеживания текущей сессии пользователя, определения сервера, через который установлена сессия, подключения к серверу и разбора пользовательской сессии.
		3. Определение геолокации на основе IP-адреса домена.
		4. Формирование отчетности с функционалом:
* объявления пользовательских (новых) полей;
* формирования запросов с использованием перекрестных запросов.
	+ 1. Формирование отчетности с предоставлением функционала:
* задания фильтров по всем (любым) полям, поддерживаемым средствами мониторинга функционирования и формирования отчетности;
* формирования запросов к базе данных;
* задания формата отчетов.
	+ 1. Отправку отчетов по расписанию и по запросу администраторов Системы.
		2. Отключение мониторинга функционирования и формирования отчетности для конкретных пользователей/IP-адресов.
		3. Управление доступом к средствам мониторинга и отчетности с использованием ролевой модели.

Требования к функционалу средств контентного анализа:Средства контентного анализа передаваемой информации должны обеспечивать выполнение следующих функций:* + 1. Получение информации от средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.
		2. Обеспечение следующих видов фильтрации (анализа) передаваемого контента:
* анализ передаваемых объектов по типу передаваемых объектов, в том числе определение и корректная обработка распространенных форматов файлов, применяемых в офисном ПО (Microsoft Office, PDF, TXT и т.д.);
* поиск и анализ регулярных выражений (ключевых слов);
* лингвистический (морфологический) анализ.
	+ 1. Управление доступом к средствам контентного анализа с использованием ролевой модели.

Связь с существующим окружением и интеграция * + 1. Разграничение полномочий доступа для работы с Системой и доступа пользователей в сеть Интернет должно быть реализовано на ролевой основе с использованием групп существующих доменов Active Directory.
		2. Система должна взаимодействовать со следующими смежными системами:
* Система авторизации в соответствии с типом используемого механизма с системами авторизации пользователей Заказчика;
* Система синхронизации времени, в части взаимодействия с системой синхронизации времени должна поддерживать определение точного времени;
* Система доменных имен (DNS), в части взаимодействия с системой DNS должно поддерживать определение IP-адресов узлов сети по имени узла;
* Система мониторинга SNMP, в части взаимодействия с системой мониторинга SNMP должно поддерживать оповещение и работу в режиме запросов состояния системы по протоколам SNMP v2 и SNMP v3;
* Корпоративная почтовая система (E-mail), в части взаимодействия с корпоративной почтовой системой должно поддерживать отправку по E-mail оповещений администраторам о событиях в работе средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет;
* Система сбора и корреляции событий информационной безопасности, в части взаимодействия с системами сбора и корреляции событий информационной безопасности должно предоставлять механизм экспорта журнальных сообщений в режиме реального времени. Формат и детализация данных сообщений должны настраиваться;
* Системы дополнительного контентного анализа, в части взаимодействия с системами дополнительного контентного анализа должно предоставлять модуль интеграции по протоколу I-CAP с указанными системами в части условий доступа на основании результатов анализа контента.

Требования к пользовательскому интерфейсу* + 1. Программный интерфейс компонентов Системы, включая средства управления, а также формы оповещений и уведомлений администраторов Системы и пользователей сети Интернет должен полностью поддерживать русский язык, используя кодировку текста UTF-8.
		2. Наличие web-интерфейса для доступа к компонентам узла фильтрации Интернет-трафика, включая средства управления, полностью поддерживающего русский язык, используя кодировку текста UTF-8.

Требования к наличию отчетовСистема должна обеспечивать формирование отчетности в табличном и графическом виде о совершаемых пользователями действиях в сети Интернет за различные периоды времени.1.8 Требования к сертификацииСистема имеет действующий сертификат соответствия ФСТЭК России на соответствие следующим требованиям:* «Требования к межсетевым экранам» (ФСТЭК России, 2016) к межсетевым экраном типов «А» и «Б», «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты» ИТ.МЭ.А4.ПЗ (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты» ИТ.МЭ.Б4.ПЗ (ФСТЭК России, 2016);
* «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012).
 | **шт.** | **1** |
| **3.** | **Модуль Advanced Threat Protection на 1 год для UserGate до 50 пользователей** | Программное обеспечение должно обладать следующей функциональностью, в течение не менее 1 (одного) календарного года с момента активации, для не менее чем 50 пользователей:* Контроль доступа пользователей в сеть Интернет и фильтрации трафика сети Интернет с обеспечением защиты от вредоносного программного обеспечения;
* Анализ трафика сети Интернет по категориям сайтов, URL-адресам и контенту данных, включая морфологический анализ;
* Обеспечивать категорирование ресурсов сети Интернет и обеспечивать фильтрацию доступа пользователей на основе данных категорий;
* Обеспечивать фильтрацию доступа пользователей к ресурсам сети Интернет на основе контентной фильтрации;
* Поддерживать и автоматически обновлять базу данных ресурсов сети Интернет и присвоенных им категорий;
* Управлять доступом к сайтам сети Интернет на основе «чёрных» и «белых» списков, составленных с использованием категоризации сайтов;
* Функционал настройки фильтрации входящего и исходящего трафика должен позволять указывать в качестве фильтра маску или регулярное выражение. Списки категорий сайтов должны предоставляться производителем средств контроля доступа в сеть Интернет. Для Администраторов Программное обеспечения должна быть реализована функция внесения корректировок в данные списки, а также создания собственных категорий. Списки должны формироваться путём внесения не только одиночных сайтов, но и их списков (в формате текстовых файлов с разделителями);
* Иметь возможность отключения функционала контроля доступа в сеть Интернет и фильтрации трафика сети Интернет для конкретных пользователей/IP-адресов.
* Обеспечивать управление доступом пользователей к различным типам информации в сети Интернет (видео, аудио, изображения и т.д.);
* Обеспечивать управление доступом пользователей к возможности передачи в сеть Интернет информации различных типов (видео, аудио, изображения и т.д.);
* Предоставлять интерфейс гибкой настройки правил фильтрации на основе различных параметров, в частности, групп доступа пользователей, категорий ресурсов (в том числе и ресурсов, не отнесенных ни к одной из категорий) и типов передаваемого контента;
* Поддерживать и автоматически обновлять список сайтов на основе единой автоматизированной информационной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»;
* Обеспечивать фильтрацию передаваемого контента и блокировку определенных типов файлов, в том числе в SSL-трафике, а также поддерживать выполнение антивирусной проверки передаваемого контента;
* Предоставлять функционал гибкой настройки правил фильтрации на основе различных параметров, в частности, групп доступа пользователей, категорий ресурсов, отдельных ресурсов (в том числе ресурсов, не отнесенных ни к одной из категорий) и типов передаваемого контента;
* Обеспечивать выборочную блокировку рекламы;
* Обеспечивать активацию безопасного поиска;
* Обеспечивать DNS-фильтрацию запросов пользователей и режим DNS-прокси;
* Предоставлять интегрированные механизмы оповещения и уведомления администраторов и пользователей о событиях;
* Предоставлять клиента для авторизации и фильтрации на АРМ пользователей.
 | **Шт.** | **1** |
| **6.** | **Услуги по развертыванию межсетевого экрана UserGate** | * 1. Настройка сетевых интерфейсов;
* 2. Интеграция с Глобальным каталогом;
* 3. Настройка правила для доступа из зоны “trust” в зону “un trust” для всех пользователей;
* 4. Настройка блокировки одной нежелательной категории для всех пользователей;
* 5. Проведение ПМИ;
* 6. Корректировка настроек по результатам ПМИ;
* 7. Подписание актов о выполненных работах.
 | **1** | **1** |
| **7.** | **Обучение** | Сертификат на услуги учебного центра «Информзащита» - Практический курс Многофункциональный межсетевой экран UserGate 5, КП76 | **1** | **1** |