**ДОГОВОР №**

**на приобретение средств защиты информации**

 **(СЗИ) Secret Net Studio 8**

|  |  |
| --- | --- |
| г. Челябинск | «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

**Муниципальное автономное учреждение «Многофункциональный центр по предоставлению государственных и муниципальных услуг города Челябинска»**, именуемое в дальнейшем **«Заказчик»**, в лице директора Барашковой Ксении Михайловны, действующей на основании Устава, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем **«Поставщик»**, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_, с другой стороны, вместе именуемые «Стороны», руководствуясь Федеральным законом № 223-ФЗ от 18.07.2011 «О закупках товаров, работ, услуг отдельными видами юридических лиц», путем проведения закупки через ППЮУ, заключили настоящий Договор (далее - Договор) о нижеследующем:

1. **ПРЕДМЕТ ДОГОВОРА**
	1. В соответствии с условиями Договора Заказчик поручает, а Поставщик принимает на себя обязательства по поставке и установке Заказчику средств защиты информации (СЗИ) Secret Net Studio 8, полное наименование, состав, количество, технические характеристики которых указаны в Спецификации (Приложение № 1 к настоящему договору) и Техническом задании (Приложение №2 к настоящему Договору) (далее – Товар), а Заказчик обязуется принять и оплатить Товар в соответствии с условиями настоящего Договора.

1.2.Место, время поставки Товара: 454091, Челябинская область**,** г. Челябинск**,** ул. Труда, д. 164 с 9-00 до 17-30 часов, за исключением выходных и праздничных дней.

1.3. Срок поставки Товара: в течение **14 (четырнадцати)** рабочих дней со дня заключения договора.

**2. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

2.1. **Обязанности Поставщика:**

2.1.1. Обеспечить передачу и установку неисключительных прав в объеме и соответствии требованиям и характеристиками, изложенным в Техническом задании, в течение срока, установленного пунктом 1.6 настоящего Договора, своими силами и средствами;

2.1.2. Сохранять конфиденциальность информации, полученной в процессе исполнения обязательств по настоящему Договору.

* + 1. Оказать Заказчику консультативную помощь по передаваемому Товару на основании индивидуальной информации Заказчика.
		2. Воздержаться от каких-либо действий, способных затруднить осуществление Заказчиком предоставленного ему неисключительного права использования средств защиты информации.
		3. Предоставить Заказчику надлежащим образом заверенную копию лицензионного договора и (или) иных документов, предоставляющих Поставщику право осуществлять передачу неисключительных прав на использование средства защиты информации, указанного в Техническом задании и Спецификации.
		4. Поставщик предоставляет Заказчику копии сертификатов соответствия на поставляемые Товары, которые подлежат сертификации в соответствии с законодательством Российской Федерации.

2.2. **Права Поставщика:**

2.2.1. Поставщик вправе требовать от Заказчика оплаты поставленного Товара в порядке и сроки, предусмотренные Договором.

2.3. **Обязанности Заказчика:**

2.3.1. Назначить ответственное лицо, осуществляющее контроль за исполнением настоящего договора Поставщиком.

2.3.2. Ставить в известность Поставщика обо всех недостатках, выявленных в ходе оказания услуг, для принятия необходимых мер.

2.3.3. Произвести оплату Товара Поставщику в порядке и сроки, установленные настоящим Договором.

2.4. **Права Заказчика:**

2.4.1. Заказчик вправе требовать от Поставщика полного, своевременного и качественного исполнения обязательств по Договору, а также своевременного устранения выявленных недостатков.

* + 1. Заказчик вправе проверять качество поставляемого Товара.
		2. Запрашивать у Поставщика информацию по вопросам использования Товара.

**3. ПОРЯДОК ПОСТАВКИ ТОВАРА**

3.1. Поставщик передает Заказчику Товар по акту приема-передачи.

3.2. В течение 10 (десяти) рабочих дней со дня передачи Товара и предоставления Поставщиком подписанного акта приема-передачи и счета (счет-фактуры), Заказчик при отсутствии недостатков подписывает акт приема-передачи, предоставленный Поставщиком, либо направляет мотивированный отказ от его подписания в тот же срок.

3.3. В случае получения Поставщиком мотивированного отказа Заказчика от подписания акта приема-передачи, Стороны подписывают акт о выявленных недостатках с детальным описанием недочетов, которые должны быть устранены с целью подписания такого акта. Поставщик должен принять необходимые меры для устранения недочетов в согласованные Сторонами сроки.

3.4. Для проверки оказанных услуг в части их соответствия условиям Договора, Заказчик вправе провести экспертизу. Экспертиза результатов, предусмотренных Договором, может проводиться Заказчиком своими силами или к ее проведению могут привлекаться эксперты, экспертные организации. Срок проведения экспертизы в течение 10 (десяти) рабочих дней со дня оказания услуги согласно п. 3.2 договора. Если Товар, подвергшийся экспертизе не будет соответствовать условиям договора, Заказчик может отказаться от него, и Поставщик должен в срок не позднее 2 (двух) рабочих дней заменить забракованный Товар либо внести все необходимые изменения с целью приведения Товара в соответствие с условиями договора, без каких-либо дополнительных затрат со стороны Заказчика.

3.5. Обязательства по фактической передаче Товара считаются исполненными с даты подписания Сторонами акта приема-передачи.

* 1. Для взаимодействия ответственных лиц со стороны Заказчика и Поставщика стороны обмениваются контактными данными (номер телефона, электронный почтовый ящик).
1. **ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА**

4.1. Поставщик гарантирует соответствие качества Товара по настоящему Договору действующим стандартам, и нормативам для данного вида услуг и соответствие стандартам, показателям, параметрам, изложенным в Техническом задании.

4.2. Поставщик гарантирует функционирование Товара в целях, предусмотренных Техническим заданием, и возможность использования его в рабочем процессе Заказчика в соответствии с техническим (функциональным) назначением.

4.3. Поставщик гарантирует **у**странение выявленных недостатков за свой счет в установленные Заказчиком сроки.

4.4. Поставщик гарантирует, что имеет законные основания на предоставление Товара Заказчику в порядке и объеме, предусмотренном настоящим договором и Техническим заданием.

4.5. Поставщик гарантирует качество и надежность Товара, а также его соответствие действующим стандартам и нормам в этой области.

1. **ЦЕНА ДОГОВОРА, ПОРЯДОК И СРОКИ ОПЛАТЫ.**
	1. Цена настоящего Договора составляет \_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_) рублей \_\_\_\_коп., в том числе НДС в размере, предусмотренном действующим законодательством /НДС не предусмотрен.
	2. Цена Договора включает в себя стоимость товара, а также стоимость всех затрат, издержек и иных расходов Поставщика (транспортные расходы, страхование, уплата таможенных пошлин (при необходимости), налогов, сборов и других обязательных платежей).
	3. По соглашению сторон возможно изменение размера и (или) сроков оплаты и (или) объема товаров, работ, услуг в случае уменьшения в соответствии с Бюджетным кодексом Российской Федерации получателю бюджетных средств, предоставляющему субсидии, ранее доведенных в установленном порядке лимитов бюджетных обязательств на предоставление субсидии.
	4. Оплата по договору осуществляется Заказчиком за поставленный Товар, в течение 30 (тридцати) календарных дней с даты подписания Заказчиком акта приема-передачи и выставления платежных документов (счет либо счет-фактура) путем перечисления безналичных денежных средств на расчетный счет Поставщика.
	5. Днем оплаты считается день списания денежных средств со счета Заказчика.
	6. Платежи по Договору осуществляются в российских рублях.
2. **ОТВЕТСТВЕННОСТЬ СТОРОН**

6.1. За неисполнение или ненадлежащее исполнение Сторонами своих обязательств по настоящему Договору Стороны несут ответственность в соответствии с действующим законодательством РФ.

6.2. При нарушении сроков, установленных Договором виновная сторона уплачивает пеню из расчета 1/300 ключевой ставки ЦБ РФ от суммы настоящего договора за каждый день просрочки исполнения обязательств, на основании письменного заявления, представленного заинтересованной стороной.

6.3. Стороны договорились, что все возникшие разногласия будут разрешаться путем переговоров. При этом настоящим договором предусматривается претензионный порядок урегулирования возникших разногласий путем предъявления претензий, срок рассмотрения которых – 10 (десять) рабочих дней с момента получения.

6.4. При не достижении согласия споры разрешаются в Арбитражном суде Челябинской области в порядке, предусмотренном действующим законодательством РФ.

7. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ (ФОРС — МАЖОР)

7.1.Стороны не несут ответственность за невыполнение своих обязательств по настоящему Договору, если такое невыполнение обязательств является результатом действия непреодолимой силы.

7.2.Для целей настоящего Договора «непреодолимая сила» означает чрезвычайное, непредотвратимое при данных условиях обстоятельство, неподвластное контролю Сторон, не связанное с их просчетом или небрежностью, как - то: стихийные бедствия, эмбарго, забастовки, военные действия, вновь принятые нормативные акты Российской Федерации.

7.3.При возникновении обстоятельств непреодолимой силы Сторона должна незамедлительно направить другой Стороне письменное уведомление о возникновении таких обстоятельств и их причинах, в котором обязуется предпринять все возможные меры для надлежащего выполнения своих обязательств по Договору.

**8.ВНЕСЕНИЕ ИЗМЕНЕНИЙ И/ИЛИ ДОПОЛНЕНИЙ, РАСТОРЖЕНИЕ ДОГОВОРА**

8.1. Договор может быть изменен по соглашению Сторон при снижении цены договора без изменения предусмотренных договором объема работы, его качества и иных условий договора.

Все изменения и/или дополнения к Договору осуществляются путем подписания Сторонами дополнительных соглашений, являющихся его неотъемлемой частью.

8.2.Расторжение Договора допускается по соглашению Сторон, по решению суда, в случае одностороннего отказа Стороны Договора от исполнения Договора в соответствии с законодательством РФ.

8.3.Расторжение настоящего Договора в одностороннем порядке осуществляется по основаниям, предусмотренным Гражданским Кодексом РФ для одностороннего отказа от исполнения отдельных видов обязательств, в том числе:

а) существенным нарушением Поставщиком требований к товару и оказанию услуг, а именно обнаружение Заказчиком неустранимых недостатков, недостатков, которые не могут быть устранены без несоразмерных расходов или затрат времени, или выявляются неоднократно, либо проявляются вновь после их устранения, и других подобных недостатков;

б) нарушение установленного срока поставки;

Заказчик вправе принять решение об одностороннем отказе от исполнения договора, если в ходе исполнения договора установлено, что Поставщик не соответствует установленным документацией о закупке требованиям к участникам закупки или предоставил недостоверную информацию о своем соответствии таким требованиям, что позволило ему стать победителем закупки.

Договор считается измененным или расторгнутым с момента получения одной стороной уведомления другой стороны об одностороннем отказе от исполнения договора полностью или частично, если иной срок расторжения или изменения договора не предусмотрен в уведомлении либо не определен соглашением сторон.

**9.** **ПРОЧИЕ УСЛОВИЯ**

9.1. Настоящий Договор регулируется законодательством Российской Федерации.

9.2.Настоящий Договор вступает в силу с даты заключения договора и действует по 31 октября 2020 года, а в части расчетов (в том числе уплаты неустоек, штрафов) до полного их исполнения.

9.3.Любое уведомление, которое в соответствии с настоящим Договором одна Сторона направляет другой, высылается на адрес место нахождения, указанный в разделе 10 настоящего договора.

**10. МЕСТА НАХОЖДЕНИЯ И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН**

|  |  |
| --- | --- |
| **Поставщик** | **ЗАКАЗЧИК****МАУ «МФЦ города Челябинска»**454091 г. Челябинск, ул. Труда д, 164 ОГРН 1117451012854, ИНН/КПП 7451326343/745301001, р/сч. 40703810190004000295 в ПАО «ЧЕЛЯБИНВЕСТБАНК»,БИК 047501779,кор/сч. 30101810400000000779 Директор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/К.М. Барашкова/мп |

Приложение № 1 к договору

на приобретение средств защиты информации

 (СЗИ) Secret Net Studio 8

№ \_\_\_\_\_\_ от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2020г.

СПЕЦИФИКАЦИЯ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  № п/п | Наименование  | Ед.изм. | Кол-во | Цена, руб.С НДС/без НДС | Стоимость, руб. с НДС/без НДС | Страна происхождения товара |
| 1 | Право на использование модулей защиты от НСД и персонального межсетевого экрана средства защиты информации Secret Net Studio 8SNS-8.x-BL3-NS-SP1Y | шт | 2 |  |  |  |
| 2 | Право на использование модулей обнаружения и предотвращения вторжений средства защиты информации Secret Net Studio 8, срок 1 год. Inc. TS Basic lvlSNS-8.x-IPS-SB-SP1Y | шт | 2 |  |  |  |
| 3 | Установочный комплект средства защиты информации Secret Net Studio 8SNS-DISC\* | шт. | 1 |  |  |  |
| 4 | Установка и настройка Secret Net Studio 8 | услуга | 2 |  |  |  |
|  | **ИТОГО:** |  |  |  |  |  |

Общая стоимость Товара составляет \_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_) рублей \_\_\_\_коп., в том числе НДС в размере, предусмотренном действующим законодательством /НДС не предусмотрен.

Общая стоимость Товара включает в себя: стоимость товара, а также стоимость всех затрат, издержек и иных расходов Поставщика (транспортные расходы, страхование, уплата таможенных пошлин (при необходимости), налогов, сборов и других обязательных платежей).

|  |  |
| --- | --- |
| ЗАКАЗЧИКМАУ «МФЦ города Челябинска» Директор \_\_\_\_\_\_\_\_\_\_\_\_/К.М. Барашкова/ М.П. | ПОСТАВЩИК\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Руководитель \_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/ М.П. |
|  |  |

Приложение № 2 к договору

на приобретение средств защиты информации

 (СЗИ) Secret Net Studio 8

 **№\_\_\_\_\_\_ от «\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_2020 г.**

**Техническое задание**

**на приобретение средств защиты информации (СЗИ) Secret Net Studio 8:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование товара, включая торговое (фирменное) наименование товара, модель, марка товара, предлагаемого к поставке** | **Ед.****изм.** | **Кол-во** | **Сведения о технических характеристиках товара, безопасности, функциональных характеристиках (потребительских свойствах) товара, комплектации, размерах, качественных характеристиках товара.** |
|  | Право на использование модулей защиты от НСД и персонального межсетевого экрана средства защиты информации Secret Net Studio 8SNS-8.x-BL3-NS-SP1Y\* | Шт. | 2 | ***Должно осуществлять:**** защиту серверов и рабочих станций от НСД;
* контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты;
* разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации;
* разграничение доступа пользователей к информации;
* контроль утечек информации;
* аутентификацию входящих и исходящих сетевых запросов в локальной сети методами, устойчивыми к пассивному и/или активному прослушиванию сети;
* фильтрацию сетевых пакетов;
* защиту установленных сетевых соединений;
* регистрацию событий безопасности и аудит.

***Требования к сертификации и применению в информационных системах:***СЗИ должны соответствовать требованиям руководящих документов по 4 уровню контроля отсутствия НДВ, 5 классу защищенности СВТ, 4 классу защиты СКН (ИТ.СКН.П4.ПЗ), 4 классу защиты САВЗ (ИТ.САВЗ.А4.ПЗ, ИТ.САВЗ.Б4.ПЗ, ИТ.САВЗ.В4.ПЗ, ИТ.САВЗ.Г4.ПЗ), 3 классу защищенности МЭ, 4 классу защиты СОВ (ИТ.СОВ.У4.ПЗ). СЗИ должно допускать использование в следующих информационных системах:* автоматизированные системы - до класса защищенности 1 Г (включительно);
* государственные информационные системы – до 1 класса защищенности (включительно);
* информационные системы персональных данных – до систем 1 уровня защищенности (включительно)

 ***Требования к операционной платформе и аппаратной части:**** СЗИ должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы):
	+ Windows 10;
	+ Windows 8/8.1;
	+ Windows 7 SP1;
	+ Windows Vista SP2;
	+ Windows Server 2012/2012 R2;
	+ Windows Server 2008 SP2/2008 R2 SP1.
* СЗИ должно поддерживать работу и обеспечивать защиту в системах терминального доступа, построенных на базе терминальных служб сетевых ОС MS Windows или ПО Citrix.
* СЗИ должно поддерживать работу на виртуальных машинах, функционирующих в системах виртуализации, построенных на базе гипервизоров VMware ESX(i) и Microsoft Hyper-V.
* СЗИ с централизованным управлением должно функционировать совместно с Microsoft Active Directory;
* СЗИ должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ.
* В инфраструктуре должно быть в наличии устройство, считывающее DVD (для чтения установочного диска – хотя бы на одном компьютере в информационной системе).

***Требования к функциональности СЗИ:*** СЗИ должно выполнять следующие функции по защите информации:* Контроль входа пользователей в систему и работа пользователей в системе:
	+ проверка пароля пользователя при входе в систему;
	+ поддержка персональных идентификаторов (USB-токенов и смарт-карт) для входа в систему и разблокировки компьютера – iButton, eToken Pro (Java), Рутокен S, Рутокен ЭЦП, Рутокен Lite, Jacarta PKI, Jacarta Gost, Jacarta PKI Flash, Jacarta Gost Flash, Esmart USB Token, Esmart, Esmart ГОСТ;
	+ возможность блокировки сеанса работы пользователя при отключении персонального идентификатора;
	+ возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI);
	+ однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI);
	+ возможность блокирования входа в систему локальных пользователей;
	+ возможность блокирования операций вторичного входа в систему в процессе работы пользователей;
	+ возможность блокировки сеанса работы пользователя по истечении интервала неактивности;
	+ возможность управления политикой сложности паролей;
	+ поддержка возможности входа в систему по сертификатам;
	+ возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей.
* Избирательное (дискреционное) управление доступом:
	+ возможность назначения прав доступа на файлы, каталоги, принтеры, устройства;
	+ возможность наследования прав доступа для файлов, каталогов и устройств;
	+ возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту.
* Полномочное (мандатное) управление доступом:
	+ возможность выбора уровня конфиденциальности сессии для пользователя;
	+ возможность назначения мандатных меток файлам, каталогам, внешним устройствам, принтерам, сетевым интерфейсам;
	+ возможность изменения количества мандатных меток в системе и их названий;
	+ контроль потоков конфиденциальной информации в системе;
	+ возможность контроля потоков информации в системах терминального доступа при передаче информации между клиентом и сервером по протоколу RDP.
* Контроль вывода конфиденциальных данных на печать:
	+ возможность ограничить перечень мандатных меток информации для печати на заданном принтере;
	+ теневое копирование информации, выводимой на печать;
	+ автоматическая маркировка документов, выводимых на печать;
	+ управление грифами (видом маркировки) при печати конфиденциальных и секретных документов. При этом должна быть возможность задать:
		- отдельный вид грифа для каждой мандатной метки;
		- отдельный вид маркировки для первой страницы документа;
		- отдельный вид маркировки для последней страницы документа;
		- вид маркировки для оборота последнего листа;
	+ поддержка функции печати в файл;
	+ поддержка управления запретом перенаправления принтеров в терминальных (RDP) сессиях.
* Контроль аппаратной конфигурации компьютера и подключаемых устройств:
	+ Должны контролироваться следующие устройства:
		- последовательные и параллельные порты;
		- локальные устройства;
		- сменные, физические и оптические диски;
		- программно реализованные диски;
		- USB-устройства;
		- PCMCIA-устройства;
		- IEEE1394 (FireWire)- устройства;
		- устройства, подключаемые по шине Secure Digital.
	+ Должна быть возможность задать настройки контроля на уровне шины, класса устройства, модели устройства, экземпляра устройства.
	+ Должен осуществляться контроль неизменности аппаратной конфигурации компьютера с возможностью блокировки при нарушении аппаратной конфигурации.
	+ Должна быть возможность присвоить устройствам хранения информации мандатную метку. Если метка устройства не соответствует сессии пользователя – работа с устройством хранения должна блокироваться.
	+ Должен осуществляться контроль вывода информации на внешние устройства хранения с возможностью теневого копирования отчуждаемой информации.
	+ В инфраструктуре виртуальных рабочих станций (VDI) должны контролироваться устройства, подключаемые к виртуальным рабочим станциям с рабочего места пользователя.
	+ При терминальном подключении (RDP) должна быть возможность управления запретом подключения устройств, COM- и LPT-портов, локальных дисков и PnP-устройств.
* Контроль сетевых интерфейсов:
	+ Должна быть возможность включения/выключения явно заданного сетевого интерфейса или интерфейса, определяемого типом – Ethernet, WiFi, IrDA, Bluetooth, FireWire (IEEE1394).
	+ Должна быть возможность управления сетевыми интерфейсами в зависимости от уровня сессии пользователя.
* Создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера. При этом должны контролироваться исполняемые файлы (EXE-модули), файлы загружаемых библиотек (DLL-модули), запуск скриптов по технологии Active Scripts.
	+ Список модулей, разрешенных для запуска, должен строиться:
		- с помощью явного указания модулей;
		- по информации об установленных на компьютере программах;
		- по зависимостям исполняемых модулей;
		- по ярлыкам в главном меню;
		- по событиям журнала безопасности.
* Контроль целостности файлов, каталогов, элементов системного реестра:
	+ Должна быть возможность проведения контроля целостности, в процессе загрузки ОС, в фоновом режиме при работе пользователя.
	+ Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов.
	+ Должна быть возможность восстановления исходного состояния контролируемого объекта.
	+ Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП.
	+ При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ.
* Изоляция программных модулей и контроль доступа к буферу обмена и операциям перетаскивания (drag-and-drop) для изолированных модулей.
* Автоматическое затирание удаляемой информации на локальных и сменных дисках компьютера при удалении пользователем конфиденциальной информации с возможностью настройки количества проходов затирания информации.
* Возможность управления запретом передачи буфера обмена в терминальную (RDP) сессию.
* Защита сетевого взаимодействия и фильтрация трафика:
	+ Должны быть механизмы аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.
	+ Должны удостоверяться субъекты доступа (пользователи и компьютеры) и защищаемые объекты (компьютеры).
	+ Механизмы должны быть защищены от прослушивания, попыток подбора и перехвата паролей, подмены защищаемых объектов, подмены MAC- и IP-адресов.
	+ Должны быть предусмотрены механизмы защиты установленных сетевых соединений между субъектами доступа (пользователями и компьютерами) и защищаемыми объектами (серверами и информационными системами) на основе открытых стандартов протоколов семейства IPsec, которые позволяют контролировать аутентичность и целостность передаваемых данных.
	+ Должна быть предусмотрена настройка режима защиты сетевого взаимодействия, при этом должны быть предусмотрены следующие режимы защиты:
		- соединение без защиты;
		- маркируется каждый пакет;
		- подписывается заголовок каждого пакета;
		- подписывается каждый пакет целиком.
	+ Должна быть возможность ограничивать сетевые соединения по правилам фильтрации:
		- на уровне отдельных протоколов из стека TCP/IP;
		- на уровне параметров протоколов стека TCP/IP;
		- на уровне параметров служебных протоколов стека TCP/IP;
		- на уровне периодов времени;
		- на уровне пользователей или групп пользователей;
		- на уровне параметров прикладных протоколов;
		- на уровне исполняемого файла/процесса;
		- на уровне сетевого адаптера.
	+ Должен быть предусмотрен выбор действий для определения реакции системы на срабатывание правил фильтрации:
		- регистрация информации в журнале;
		- звуковая сигнализация;
		- запуск программы или сценария.
* Функциональный контроль ключевых компонентов системы.
* Регистрация событий безопасности в журнале.
	+ Должна быть возможность формирования отчетов по результатам аудита.
	+ Должна быть возможность поиска и фильтрации при работе с данными аудита.
* Получение отчета по параметрам системы защиты.

***Требования к централизованному управлению в доменной сети:***СЗИ должно предоставлять следующие возможности по управлению системой: * Отображение структуры доменов, организационных подразделений, серверов безопасности и защищаемых компьютеров.
* Динамическое отображение состояния каждого защищаемого компьютера с учетом критичности состояния с точки зрения системы защиты.
* Отображение тревог, происходящих на защищаемых компьютерах, возможность задать признак того, что тревога обработана администратором безопасности.
* Разделение тревог по уровням критичности события и важности отдельных защищаемых компьютеров.
* Выполнение оперативных команд для немедленного реагирования на инциденты безопасности (заблокировать работу пользователя, выключить компьютер).
* Выполнение команд, специфичных для защитных подсистем.
* Оперативное управление защищаемыми компьютерами, возможность централизованно изменить параметры работы защищаемого компьютера.
* Возможность создавать централизованные политики безопасности, распространяемые на разные (заданные) группы защищаемых компьютеров.
* Централизованный сбор журналов безопасности с защищаемых компьютеров, их хранение, возможность обработки и архивирования.
* Анализ собранных журналов на наличие заданных угроз безопасности с поддержкой редактирования правил детектирования угроз.
* Централизованное управление в сложной доменной сети (domain tree) должно функционировать по иерархическому принципу, при этом система должна позволять:
	+ распространить настройки, заданные для сервера безопасности, на все подчиненные компьютеры (в том числе – по иерархии серверов);
	+ посмотреть состояние и выполнить команду на любом компьютере, подчиненном серверу безопасности (в том числе – по иерархии серверов).
* Создавать домены безопасности в территориально распределенной сети, при этом должна предоставляться возможность делегирования административных полномочий лицам, ответственным за подразделения (домены безопасности).
* Создавать отчеты по ресурсам и параметрам защищаемых компьютеров, используемых в системе.

Состав:Лицензия бессрочная + ТП уровня Базовый, срок 1 год. |
|  | Право на использование модулей обнаружения и предотвращения вторжений средства защиты информации Secret Net Studio 8, срок 1 год. Inc. TS Basic lvlSNS-8.x-IPS-SB-SP1Y\* | шт. | 2 | ***Модули обнаружения и предотвращения вторжений СЗИ Secret Net Studio 8:*** * Должна обеспечиваться защита от вторжений с помощью сигнатурных и эвристических механизмов.
* Сигнатурные механизмы должны обеспечивать проверку HTTP-трафика на наличие заданных конструкций как для входящего, так и для исходящего сетевого трафика. При обнаружении признаков атаки прохождение подозрительных сетевых пакетов должно быть заблокировано.
* Эвристические механизмы должны распознавать и фиксировать следующие типы атак:
	+ - сканирование портов;
		- подделка ARP (ARP-spoofing);
		- SYN-флуд;
		- атаки, направленные на отказ в обслуживании (DoS);
		- распределенные атаки, направленные на отказ в обслуживании (DDoS).

При обнаружении признаков атаки эвристическими методами должен осуществляться временный запрет на прием сетевых пакетов с IP-адреса атакующего компьютера.* Должны обеспечиваться обнаружение и блокировка аномальных сетевых пакетов.

Состав:Лицензия на 1 год + ТП уровня Базовый, срок 1 год. |
|  | Установочный комплект средства защиты информации Secret Net Studio 8SNS-DISC\* | шт. | 1 | Комплектность поставки:1. Установочный диск - 1 шт.2. Формуляр в печатном виде.3. Копия сертификата соответствия ФСТЭК. |
|  | Установка и настройка Secret Net Studio 8 | шт. | 2 | Установка и настройка Secret Net Studio 8 |

\*Предоставление неисключительного права на использование эквивалентного программного обеспечения не допускается в целях обеспечения совместимости (взаимодействия) с используемым Заказчиком программным обеспечением.

**Сроки (периоды) поставки товара:**

1.1. Условия поставки товара: Поставщик должен известить Заказчика о готовности товара к отгрузке не позднее, чем за 5 рабочих дней до дня отгрузки. Поставить весь объем товара единовременной поставкой.

1.2. Сроки поставки товара: Поставка товара производится в течение 14 (четырнадцати) рабочих дней с даты заключения договора.

Поставляемые товары должны соответствовать **ГОСТ Р 50739-95**.

|  |  |
| --- | --- |
| **ЗАКАЗЧИК****МАУ «МФЦ города Челябинска»** **Директор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/К.М. Барашкова/** **М.П.** | **ПОСТАВЩИК**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Руководитель \_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/** **М.П.** |