Договор подписан посредством ЭЦП
Номер договора: 129150
Дата подписания: 24.10.2017 04:07:41
Место подписания: ЭТП OTC.RU
Реестровый номер на сайте zakupki.gov.ru: 31705598896

ДОГОВОР № 129150
на оказание услуг по аттестации рабочих мест для работы с базой данных реципиентов крови

г. Ангарск "____" _____ 2017 г.

Акционерное общество «Восточно-Сибирский центр ЕВРААС», именуемое в дальнейшем "**Исполнитель**", в лице Управляющего директора Фереферова Андрея Альбертовича, действующего на основании приказа №01/08 от 17 августа 2016 года, с одной стороны, и областное государственное автономное учреждение здравоохранения "Ангарская городская больница № 1", именуемое в дальнейшем "**Заказчик**", в лице главного врача Крывовязого Ивана Викторовича, действующей на основании Устава, с другой стороны, далее именуемые "Стороны", заключили настоящий Договор о нижеследующем:

I. ПРЕДМЕТ ДОГОВОРА

1. Предметом настоящего Договора является оказание услуг по аттестации рабочих мест для работы с базой данных реципиентов крови (далее Услуги), согласно Спецификации (Приложение № 1), являющегося неотъемлемой частью настоящего Договора.
2. Исполнитель обязуется оказывать Услуги в соответствии с условиями настоящего Договора, Заказчик обязуется принять оказанные Услуги и оплатить их на условиях, предусмотренных настоящим Договором.
3. Работы должны выполняться в рабочее время по будням с 8:00 до 17:00 по местному времени. Срок выполнения работ - 30 календарных дней с момента подписания Договора:
   - предпроектное обследование объекта информатизации – 3 дня;
   - поставка СЗИ – 15 дней;
   - установка средств защиты информации – 1 день;
   - разработка нормативно-распорядительной документации – 6 дней;
   - разработка комплекта аттестационной документации – 3 дня.
4. Место оказания Услуг – г. Ангарск, ул. Горького, дом 24.

II. УСЛОВИЯ ОКАЗАНИЯ УСЛУГИ

1. *Термины и описания:*

АИС «ЕИБД» - Единая база данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов.
АИС - Автоматизированная информационная система.
СЗНСД - Система защиты от несанкционированного доступа.
СЗИ - Средства защиты информациии.
СЗИ от НСД - Средство защиты информации от несанкционированного доступа.
ТЗ - Техническое задание.
АС - Автоматизированная система.
ПО - Программное обеспечение.
ОС - Операционная система

2. Назначение и цели оказания услуг

2.1. Основной целью оказываемых Исполнителем услуг является создание, предотвращение несанкционированного доступа автоматизированной системы и аттестация информационной системы «ЕИБД» Заказчика в соответствии с требованиями законодательства Российской Федерации по обеспечению безопасности.

2.2. При оказании услуг Исполнитель должен руководствоваться следующей нормативной документацией:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 19.12.2005 г. № 160-ФЗ «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральный закон от 04.05.2011№ 99-ФЗ «О лицензировании отдельных видов деятельности»;
- ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»;
- ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»;
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждённая приказом № 282 от 30.08.2002;
- Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам, Гостехкомиссия России, 2002г.;
- ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;
- ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированных систем»;
- ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
- ГОСТ 34.601- 90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания»;
- ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
- ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения»;
- ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения»;
- ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».
- Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622;
- а также иной действующей на территории Российской Федерации нормативной документацией, определяющей порядок и качество оказания услуг, являющихся предметом Договора.

2.3. СЗИ предназначены для защиты персональных данных с целью реализации конституционных прав граждан на неприкосновенность частной жизни, а также с целью выполнения:

– Требований по защите информации, не составляющей государственную тайну, содержащихся в государственных информационных системах», утвержденным Приказом ФСТЭК России от 11 февраля 2013 года № 17;

– Приказа от 17 апреля 2015 г. №63 «Об утверждении порядка организации информационного обмена учреждений, осуществляющих деятельность в сфере обращения донорской крови и (или) ее компонентов, в составе единой информационной базы данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов».

3. Характеристика объекта Заказчика

3.1.Объектами защиты Заказчика являются: ОГАУЗ "Ангарская городская больница № 1" – адрес в составе 1 АРМ.

3.2. Наименование ИС, имеющихся у Заказчика: АИС «ЕИБД» (АРМ «Реципиент») – 2 АРМ.

4. Требования к оказываемым услугам:

4.1. Требования к оценке и оптимизации разработанных требований и организационно - распорядительной документации Заказчика в разрезе обеспечения защиты информации вТребования к разработке моделей угроз:

4.2. Цель оказания услуг:

- выполнить требования нормативных документов ФСБ России и ФСТЭК России;
- определить актуальные угрозы безопасности;
- определить требования к классам средств защиты информации.

4.3. Состав услуг:

- разработка модели угроз и нарушителя безопасности ПДн, с учетом требований методических документов ФСТЭК России и ФСБ России (при необходимости), в частности формирование:
  - по требованиям ФСТЭК России:

– описания объекта защиты (цели защиты, состав и структура ИС, информационная характеристика ИС, описание информационных и технологических процессов);
– перечня возможных угроз;
– оценки исходной защищенности ИС;
– оценок возможности угроз;
– оценок опасности угроз;
– определенного перечня актуальных угроз;
– требований к классам средств защиты;

  - по требованиям ФСБ России (при необходимости):

– описания объекта защиты (цели защиты, состав и структура ИС, информационная характеристика ИС, описание информационных и технологических процессов);
– описания угроз (модель угроз);
– типизации нарушителей;
– предположений об имеющейся у нарушителей информации;
– предположений об имеющихся у нарушителей средствах атак;
– предположений об ограничениях на возможности нарушителей;
– выводов о типах нарушителей, требуемых классах средств криптографической защиты информации.

4.4. Результат оказания услуг: актуальная модель угроз и нарушителей безопасности ПДн Заказчика.

4.5. Отчетность: результаты оказанных услуг должны быть включены в актуальную модель угроз и нарушителей безопасности ПДн Заказчика.

5. Требования к разработке технического проекта Заказчика на создание системы защиты АИС

5.1. Цель оказания услуг: разработать требования по защите АИС Заказчика

5.2. Состав услуг:

- разработать технический проект Заказчика на создание системы защиты АИС на основании Модели угроз и нарушителя безопасности ПДн и в соответствии с нормативными документами ФСТЭК России.
- разработка технического проекта Заказчика на создание системы защиты АИС, направленного на минимизацию выявленных рисков безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010

5.3. Отчетность: результаты оказанных услуг должны быть отражены в техническом проекте Заказчика на создание системы защиты АИС.

6. Требования к проектированию системы защиты АИС Заказчика.

6.1. Цель оказания услуг: оптимизировать выбранный единый комплекс технических решений, обеспечивающих решение задач защиты АИС Заказчика.

6.2. Состав услуг:

- оптимизация перечня контрмер нейтрализующих или уменьшающих вероятность реализации угрозы;
- оптимизация и обоснование технических решений;
- определение необходимости, а в случае необходимости описание и обоснование организационных решений;
- оптимизация структурных схем комплекса технических средств.

6.3. Отчетность: результаты оказанных услуг должны быть отражены в техническом проекте Заказчика на создание системы защиты АИС.

7. **Требования к внедрению системы защиты АИС Заказчика**

7.1. Цель оказания услуг: внедрение средств защиты в АИС Заказчика в соответствии с разработанной проектной документацией.

7.2. Состав услуг:

- Услуги по установке СЗИ;
- Услуги по проверке эффективности СЗИ.

7.3. Отчетность:

- Акт установки СЗИ;
- Протокол проверки эффективности СЗИ.

8. Требования к разработке программы - методики проведения аттестационных испытаний АИС Заказчика

8.1. Программа – методика проведения аттестационных испытаний должна включать в себя все необходимые проверки для проведения аттестационных испытаний. Общие требования к проводимым проверкам:

- Производится проверка достаточности представленных документов и соответствия их содержания требованиям стандартов и иных руководящих документов по безопасности информации.
- Состав и структура технических средств, включенных в реальный технологический процесс обработки информации, сверяется с представленной документацией.
- Проверка уровня подготовки кадров и распределения ответственности производится на основе следующих показателей:
  - экспертной оценки знания инструкций по безопасности информации пользователями;
  - экспертной оценки системы технической учебы и повышения квалификации персонала.
  - путем опроса персонала проверяется доведение до конкретных исполнителей руководящих документов, технологических инструкций, предписаний, актов, заключений и уровень овладения персоналом технологией безопасной обработки информации, описанной в этих инструкциях.
- Производится проверка наличия документов, подтверждающих возможность применения технических средств обработки информации, средств защиты для обработки конфиденциальной информации (сертификатов соответствия), экспертиза отчетов и протоколов по специальным исследованиям, предписаний на эксплуатацию, а также их соответствия требованиям нормативных документов.

8.2. По результатам проверки сделать выводы о соответствии (или несоответствии) предъявленных документов и исходных данных установленным требованиям по безопасности информации.

8.3. Отчетность: программа – методика проведения аттестационных испытаний АИС Заказчика.

9. Требования к проведению контроля защищенности информации, аттестационных испытаний объекта информатизации и анализу информационных потоков АИС Заказчика:

9.1. Требования к проведению аттестационных испытаний объекта информатизации АИС Заказчика:

9.1.1. Проведение аттестационных испытаний должно быть произведено на основании разработанной программы-методики проведения аттестационных испытаний АИС Заказчика.

9.2. Требования к контролю защищенности информации АИС Заказчика

9.2.1. Для оценки уровня исходной защищенности и проведения аттестационных испытаний необходимо провести:

- выявление уязвимостей и ошибок конфигурации программного обеспечения компонентов сети;

мониторинг и отслеживание изменений конфигураций и настроек программного обеспечения компонентов сети на момент проведения аттестационных испытаний;
- инвентаризация компонентов информационных систем (программной и аппаратной части);
- проверить соответствие исполнения требований ФСТЭК России;
- на момент проведения аттестационных испытаний провести контроль и отслеживание изменений настроек операционных систем серверов и рабочих станций, СУБД и прикладных систем;
- на момент проведения аттестационных испытаний провести контроль и регистрацию событий, относящихся к информационной безопасности;
- провести тестирование функций защиты серверов и рабочих станций с использованием специализированных программных средств анализа защищенности;
- провести оценку эффективности ключевых процессов ИТ и ИБ.

10.2.2. Все проверки должны соответствовать требованиям Приказов ФСТЭК России от 11.02.2013 № 17.

11.Требования к аттестации АИС Заказчика

11.1. Разрабатываемая Исполнителем аттестационная документация должна включать в себя:

- Протоколы аттестационных испытаний;
- Технический паспорт объекта информатизации;
- Описание конфигурации и топологии АИС, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения, а также режимов обработки персональных данных;
- Программу и методику аттестационных испытаний.

11.2. До начала аттестационных работ в составе АИС должны быть установлены средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия по требованиям безопасности информации. Данные средства должны быть настроены в соответствии с требованиями, предъявляемыми к определенному уровню защищенности АИС, и документацией на данные средства.

11.3. В рамках аттестации должна быть произведена комплексная проверка (аттестационные испытания) защищаемых АИС в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требованиям, предъявляемым к установленному классу защищаемых АИС.

11.4. Аттестационные испытания включают в себя:

- анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
- определение правильности классификации АИС, выбора и применения сертифицированных средств и систем защиты информации;
- проверку уровня подготовки кадров и распределения ответственности персонала за обеспечение выполнения требований по безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации.

11.5. По результатам аттестационных испытаний должны быть оформлены протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений (в случае выявления таковых).

11.6. После утверждения заключения по результатам аттестации Исполнителем должен быть оформлен и выдан Заказчику «Аттестат соответствия».

12. Требования к Исполнителю

12.1. Исполнитель должен соответствовать требованиям, устанавливаемым законодательством Российской Федерации к организациям, осуществляющим поставки товаров, выполнение работ, оказание услуг, являющихся предметом данного ТЗ, включая наличие следующих лицензий:

- Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации на осуществление деятельности по технической защите конфиденциальной информации по видам работ и услуг предусмотренными подпунктам, а), б), г), д), е) п. 4 «Положения о лицензировании деятельности по технической защите конфиденциальной

информации», утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79:
а) контроль защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации;
технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;
помещениях со средствами (системами), подлежащими защите;
помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);
б) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
г) аттестационные испытания и аттестация на соответствие требованиям по защите информации:
средств и систем информатизации;
помещений со средствами (системами) информатизации, подлежащими защите;
защищаемых помещений;
д) проектирование в защищенном исполнении:
средств и систем информатизации;
помещений со средствами (системами) информатизации, подлежащими защите;
защищаемых помещений;
е) установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации);

- Лицензия ФСБ России «На деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), в соответствии с подпунктом 1) пункта 1 статьи 12 Федерального закона Российской Федерации «О лицензировании отдельных видов деятельности» от 4 мая 2011 года N 99-ФЗ, на осуществление деятельности по:
  - распространению шифровальных (криптографических) средств;
  - выполнению работ, оказанию услуг в области шифрования информации;
  - техническому обслуживанию шифровальных (криптографических) средств;
- Сертификат соответствия Системы менеджмента ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) применительно к выполнению работ по разработке, производству, поставке, инсталляции и обслуживанию технических средств комплексных систем безопасности; выполнение работ по проектированию, внедрению, сопровождению, технической поддержке решений по обеспечению информационной безопасности автоматизированных систем; выполнение работ по разработке, производству, поставке, инсталляции и обслуживанию технических средств комплексных систем безопасности, в том числе шифровальных (криптографических) средств защиты информации; оказание услуг консалтинга и аудита в области обеспечения информационной безопасности; реализация, монтаж, наладка, установка, ремонт, сервисное обслуживание специализированных защищённых технических средств обработки информации, технических средств защиты информации; управление проектами по перечисленным видам деятельности.

13. Требования к организации оказания услуг, предусмотренных настоящим Перечнем услуг:

- оказание услуг должно строиться таким образом, чтобы оптимизировать объем задействованных ресурсов со стороны Заказчика;

- при оказании услуг Исполнителем должен быть предложен ролевой состав проектной группы со стороны Исполнителя и Заказчика, а именно:
  - должны быть указаны лица, ответственные за разработку документации, проведение технических работ;
  - должен быть описан формат взаимодействия лиц, ответственных, со стороны Заказчика и Исполнителя;
  - должен быть описан формат и периодичность отчетности о ходе оказания услуг.

14. Требования по обеспечению конфиденциальности информации в ходе оказания услуг:

Согласно действующему законодательству Российской Федерации и нормативным документам, принятым у Заказчика, должны приниматься следующие меры по обеспечению конфиденциальности оказываемых Исполнителем услуг:

- информация, полученная Исполнителем в процессе оказания услуг, не может быть передана третьим лицам без согласия Заказчика;
- Исполнитель должен обеспечивать безопасность передаваемой ему информации Заказчика.

15. Дополнительные требования к услугам:

Для технических решений должна предусматриваться разработка исполнительной и эксплуатационной документации в объеме, достаточном для поддержания силами Заказчика уровня эксплуатационных характеристик в соответствии с принятыми проектными решениями.

Материалы, полученные по результатам оказания услуг, должны быть подготовлены и оформлены Исполнителем на русском языке с использованием MS Office 2007/2010/2013/2016 (Word, Excel, PowerPoint, Visio).

Разрабатываемая Исполнителем документация должна быть представлена Заказчику в электронном и бумажном видах в 2 экземплярах.

16. Условия обслуживания результата оказанных услуг, предъявляемые к Исполнителю в течение гарантийного срока:

Заказчик имеет право на восстановление (изменение) комплектующих автоматизированных рабочих мест, не внося изменений в состав средств защиты информации и не изменяя конфигурации средства защиты, без проведения переаттестации автоматизированного рабочего места при условии обязательного информирования Исполнителя о факте восстановления (изменения) комплектующих автоматизированных рабочих мест.

Гарантийный срок на услуги составляет не менее 12 месяцев.

Базовый набор услуг в течение гарантийного срока по гарантийному обслуживанию АИС должен включать:

- устранение ошибок, выявленных в процессе эксплуатации, и консультирование специалистов Заказчика по вопросам устранения неисправностей посредством телефонной связи или электронной почты;
- в случае возникновения отказов созданной системы - обеспечение в течение двух рабочих дней прибытия специалистов Исполнителя для проведения работ по локализации неисправности и восстановлению работоспособности.

В случае наличия обоснованных замечаний ФСТЭК России, ФСБ России или Роскомнадзора к конфигурации установленных Исполнителем средствам защиты и оказанным Исполнителем услугам, Исполнитель безвозмездно устраняет указанные замечания за исключением случаев, связанных с:

вступлением в силу законов и подзаконных актов Российской Федерации в области защиты персональных данных, устанавливающих иные правила и требования по сравнению с теми законодательными актами Российской Федерации, в соответствии с которыми Исполнителем были оказаны услуги;

изменениями в системах и технологических процессах Заказчика, связанных с защитой персональных данных, которые были произведены Заказчиком после сдачи-приемки оказанных услуг по настоящему Контракту;

консультирование специалистов Заказчика по вопросам эксплуатации системы защиты АИС в режиме «вопрос-ответ» (посредством телефонной связи или электронной почты).

17. Поставка СЗИ включает в себя:

№ п/п	Наименование товара	Кол-во	Технические характеристики	Примечание
1.	Передача неисключительных прав на использование комплекса программного обеспечения, реализующего защиту от несанкционированного доступа	2	Приложение 2	
2.	Поставка установочного комплекта на комплекс программного обеспечения, реализующего защиту от несанкционированного доступа	1	Приложение 3	
3.	Передача неисключительных прав на использование программного обеспечения, реализующего функции криптографического клиента для работы с автоматизированной информационной системой	2	Приложение 4	
4.	Передача установочного комплекта на программное обеспечение, реализующее функции криптографического клиента для работы с автоматизированной информационной системой	1	Приложение 5	
5.	Передача сертификата активации сервиса прямого технического сопровождения сроком на 12 месяцев на программное обеспечение, реализующее функции криптографического клиента для работы с автоматизированной информационной системой	2	Приложение 6	
6.	Передача неисключительных прав на использование комплекса программного обеспечения, реализующего антивирусную защиту	5	Приложение 7	
7.	Поставка установочного комплекта на комплекс программного обеспечения, реализующего защиту от несанкционированного доступа	1	Приложение 8	

18. Гарантии качества поставляемых СЗИ:

Не менее 12 месяцев, начиная с момента подписания Заказчиком акта оказанных услуг.

19. Требования к надежности

СЗИ должны обладать высокой степенью надежности, т.е. должна безотказно выполнять определенные в настоящем ТЗ функции. Надежность СЗИ следует рассматривать без учета числа сбоев и отказов, вызванных ненадежностью аппаратных средств, программного обеспечения операционной системы и СУБД. Интенсивность отказов СЗИ, не выявленных при отладке и испытаниях, должна быть минимальна.

20.Требования к взаимосвязям подсистем с существующими системами Заказчика

СЗИ должны обеспечивать полную интеграцию и совместимость между собой и установленными у оператора АРМ «Реципиент» ViPNet 4.x (номер сети 2029).

IV. ЦЕНА ДОГОВОРА И ПОРЯДОК РАСЧЕТОВ

1. Цена договора составляет: **73 950 (семьдесят три тысячи девятьсот пятьдесят) рублей 00 копеек, без НДС, в связи с тем, что Исполнитель применяет УСН**.
2. Цена договора включает в себя все расходы, связанные с оказанием Услуг, в том числе выезд специалистов, транспортные расходы, уплату налогов, сборов и других, обязательных платежей,

установленных законодательством Российской Федерации, в том числе НДС (если Исполнитель является плательщиком НДС), т.е. является конечной.

3. Оплата производится на основании счета, счета-фактуры при наличии подписанного Акта оказанных услуг, в течение 30 (двадцати) календарных дней со дня подписания Акта оказанных услуг. Оплата производится безналичным расчетом путем перечисления денежных средств на расчетный счет Исполнителя.
4. Финансирование по настоящему Договору производится за счет средств:
   - средства обязательного медицинского страхования (ОМС);

   - от приносящей доход деятельности.

5. Цена договора может быть снижена по соглашению сторон при изменении объема оказываемых Услуг, без изменения цены за единицу Услуги**.**

6. В ходе исполнения Договора предусмотренное объем Услуг может быть изменено при изменении потребности в объеме Услуг.

V. ОТВЕТСТВЕННОСТЬ СТОРОН

1. За неисполнение или ненадлежащее исполнение своих обязательств по настоящему Договору виновная Сторона несет ответственность в соответствии с действующим законодательством РФ и настоящим Договором.

2. Стороны не несут ответственности, предусмотренной действующим законодательством РФ и настоящим Договором, если надлежащее исполнение условий Договора оказалось невозможным вследствие обстоятельств непреодолимой силы (форс-мажорных обстоятельств) согласно п. 3 раздела V настоящего договора.

3. Обстоятельствами непреодолимой силы являются: введение нормативно-правовых актов, запрещающих или ограничивающих поставку или реализацию товара, пожары, военные действия, блокады, землетрясения и другие стихийные бедствия. Факт, время наступления и продолжительность действия форс-мажорных обстоятельств должны быть подтверждены официальными документами уполномоченных органов и сообщены другим сторонам не позднее двух недель со дня наступления форс-мажорных обстоятельств.

4. За нарушение срока исполнения обязательств, предусмотренных настоящим договором Исполнитель уплачивает Заказчику неустойку в размере одной трехсотой действующей на день уплаты неустойки учетной ставки Центрального Банка Российской Федерации от цены договора за каждый день просрочки исполнения обязательств, начиная со дня, следующего после дня истечения установленного настоящим договором срока исполнения обязательств. Исполнитель освобождается от уплаты неустойки, если докажет, что просрочка исполнения указанного обязательства произошла вследствие непреодолимой силы или по вине Заказчика.

5. Удержание штрафов, предусмотренных п. 4 раздела V настоящего договора, производится Заказчиком путем уменьшения стоимости оказанных услуг при подписании Акта оказанных услуг. Уплата неустойки не освобождает Исполнителя от выполнения своих обязательств в натуре по настоящему договору.

6. За нарушение сроков исполнения обязательств, предусмотренных п. 3 раздела IV настоящего договора, Исполнитель вправе требовать от Заказчика уплату неустойки в размере одной трехсотой действующей на день уплаты неустойки учетной ставки ЦБ РФ. Неустойка начисляется от суммы неисполненного обязательства за каждый день просрочки исполнения обязательства, начиная со дня, следующего после дня истечения установленного настоящим договором срока исполнения обязательства. Заказчик освобождается от уплаты неустойки, если докажет, что просрочка исполнения указанного обязательства произошла вследствие непреодолимой силы или по вине другой Стороны.

VI. РАССМОТРЕНИЕ СПОРОВ

1. Все споры и разногласия, которые могут возникнуть между Сторонами по настоящему Договору, решаются путем проведения переговоров.

2. В случае если споры и разногласия не будут урегулированы путём проведения переговоров в течение 30 (тридцати) календарных дней с момента возникновения, они подлежат разрешению в Арбитражном суде Иркутской области. Моментом возникновения спора является дата получения претензий (рекламаций) одной из Сторон.

3. Расторжение договора допускается по соглашению сторон (путем направления уведомления о расторжении Договора другой стороне за 5 (пять) рабочих дней до момента расторжения), по решению суда, в случае одностороннего отказа стороны договора от исполнения договора в соответствии с гражданским законодательством.
4. Договор может быть расторгнут Заказчиком в одностороннем порядке.
5. Заказчик обязан принять решение об одностороннем отказе от исполнения договора, если в ходе исполнения договора установлено, что Исполнитель 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.
6. При расторжении договора в одностороннем порядке по вине Исполнителя Заказчик обязан предъявить требование об уплате неустоек (штрафов, пеней) в связи с неисполнением или ненадлежащим исполнением обязательств, предусмотренных договором, а также обратиться к Исполнителю с требованием о возмещении понесенных убытков при их наличии.
7. Расторжение договора влечет за собой прекращение обязательств сторон по договору, но не освобождает от ответственности за неисполнение обязательств, которые имели место быть до расторжения договора.
8. Заказчик вправе обратиться в Арбитражный суд Иркутской области с исковым требованием о расторжении Договора в следующих случаях:
   - систематического нарушения Исполнителем условий Договора;
   - иных, предусмотренных действующим законодательством Российской Федерации.

VIII. СРОК ДЕЙСТВИЯ ДОГОВОРА

1. Настоящий Договор вступает в силу с момента подписания его Сторонами и действует до полного исполнения Сторонами своих обязательств по настоящему Договору.

VIII. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

1. Все уведомления и сообщения, направленные Сторонам в связи с исполнением настоящего договора, должны быть сделаны в письменной форме. Под письменной формой подразумеваются также сообщения, направленные с использованием факсимильной связи.
2. Стороны обязуются незамедлительно извещать друг друга обо всех изменениях своих адресов и реквизитов.
3. Изменение существенных условий договора при его исполнении не допускается, за исключением их изменения по соглашению сторон в следующих случаях:

   1) если возможность изменения условий договора была предусмотрена документацией о закупке и договором:

   - при снижении цены договора без изменения предусмотренных договором количества товара, объема работы, качества поставляемого товара, оказываемой услуги и иных условий договора;

   - если по предложению Заказчика увеличиваются предусмотренные договором количество товара, объем работ не более чем на десять процентов или уменьшаются предусмотренные договором количество поставляемого товара, объем выполняемой работы не более чем на десять процентов. При этом по соглашению сторон допускается изменение цены договора пропорционально дополнительному количеству товара, дополнительному объему работы исходя из установленной в договоре цены единицы товара, работы, но не более чем на десять процентов цены договора. При уменьшении предусмотренных договором количества товара, объема работы стороны договора обязаны уменьшить цену договора исходя из цены единицы товара, работы. Цена единицы дополнительно поставляемого товара или цена единицы товара при уменьшении предусмотренного договором количества поставляемого товара должна определяться как частное от деления первоначальной цены договора на предусмотренное в договоре количество такого товара;

   2) изменение в соответствии с законодательством Российской Федерации регулируемых цен (тарифов) на товары, услуги.

   Изменения и (или) дополнения к настоящему договору могут быть внесены только по

взаимному согласию Сторон, выраженному в форме дополнительных соглашений, подписанных, скрепленных печатями и являющихся неотъемлемой частью настоящего договора.

4. Недействительность какого-либо из условий договора не влечет за собой недействительность других условий или всего договора в целом.
5. Все взаимоотношения Сторон, не урегулированные настоящим Договором, регулируются действующим законодательством Российской Федерации.
6. При получении от одной из Сторон письменного предложения об изменении настоящего Договора другая Сторона обязана рассмотреть его в течение 10 (десяти) календарных дней и дать письменный ответ.
7. Неотъемлемой частью настоящего Договора являются:
   - Спецификация (Приложение № 1);
   - Технические требования, предъявляемые к услугам по передаче неисключительных прав на воспроизведение и использование комплекса программного обеспечения, реализующего защиту от несанкционированного доступа (Приложение № 2);
   - Технические требования, предъявляемые к услугам по поставке установочного комплекта на комплекс программного обеспечения, реализующего защиту от несанкционированного доступа (Приложение № 3);
   - Технические требования, предъявляемые к услугам по передаче неисключительных прав на использование программного обеспечения, реализующего функции криптографического клиента для работы с автоматизированной информационной системой (Приложение № 4);
   - Технические требования, предъявляемые к услугам по поставке установочного комплекта на программное обеспечение, реализующее функции криптографического клиента для работы с автоматизированной информационной системой (Приложение № 5);
   - Технические требования, предъявляемые к услугам по поставке сертификата активации сервиса прямой технической поддержки сроком на 12 месяцев на программное обеспечение, реализующее функции криптографического клиента для работы с автоматизированной информационной системой (Приложение № 6);
   - Технические требования, предъявляемые к услугам по передаче неисключительных прав на использование комплекса программного обеспечения, реализующего антивирусную защиту (Приложение № 7);
   - Технические требования, предъявляемые к услугам по поставке установочного комплекта на комплекс программного обеспечения, реализующего антивирусную защиту (Приложение № 8);
   - Форма сведений об исполнении договора – (Приложение 9).
8. В течении 30 календарных дней со дня истечения срока выполнения Работ по настоящему Договору Стороны обязуются подписать Сведения об исполнении договора (Приложение №4) в двух экземплярах по одному для каждой из Сторон.
9. Договор составлен на основании протокола подведения итогов процедуры запроса котировок в электронной форме на **оказание услуг по аттестации рабочих мест для работы с базой данных реципиентов крови** от 13.10.2017 № 826.

IX. АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

Исполнитель: Акционерное общество «Восточно-Сибирский центр ЕВРААС», 664003, г. Иркутск, пер. Пионерский, д.11, тел.: (3952) 211-777, ИНН 3808001025, КПП 380801001, ОГРН 1033801011419, ОКПО 22861949, Банк: р/сч. 40702810808030000736 к/сч. 30101810200000000777 Филиал ПАО Банк ВТБ в г. Красноярске г. Красноярск, БИК 040407777

Управляющий директор
АО «ВСЦ ЕВРААС»

_____ А.А. Фереферов

Заказчик: областное государственное автономное учреждение здравоохранения «Ангарская городская больница №1», 665830, Иркутская область, г. Ангарск, ул. Горького, дом 24, тел. (3955) 52-37-

87, ИНН 3801012780, КПП 380101001, Минфин Иркутской области (ОГАУЗ «Ангарская городская больница № 1», л/с 80303090110 , л/с 80303050110), р/с 40601810500003000002, БИК 042520001
Банк: Отделение Иркутск г. Иркутск

Главный врач
ОГАУЗ «Ангарская городская больница № 1»

_____И.В.Крывовязый

Приложение № 1
к договору № 129150
от «_____» _____ 2017г.

Спецификация

на оказание услуг по аттестации рабочих мест для работы с базой данных реципиентов крови

№ п/п	Наименование Услуг	Характеристика Услуг	Производитель/, страна происхождения	Срок годности	Ед. изм.	Кол-во	Цена за единицу, руб.	Цена Договора, руб.
1.	Медиа-пакет Dr.Web, сертифицированная версия	В установочный комплект должно входить: 1. CD-дистрибутив ПО – 1 шт.; 2. Формуляр в печатном виде – 1 шт.; 3. Копия сертификата соответствия – 1 шт.	Россия	б/с	шт.	1	900,00	900,00
2.	Dr.Web Desktop Security, право на 5 пользователей	Комплекс программного обеспечения, реализующего антивирусную защиту должен осуществлять: - защиту компьютера от атак по сети TCP/IP; - антивирусную защиту от вредоносного программного обеспечения; - защиту от спама и вредоносного контента веб-серверов; - самозащиту от воздействия со стороны вредоносного программного обеспечения; - регистрацию событий безопасности;	Россия	б/с	усл. ед.	1	2 750,00	2 750,00
…	Передача неисключительных прав Dallas Lock 8.0-K с модулем «СОВ». Право на использование (СЗИ НСД, СКН, СОВ) (включена годовая техническая поддержка)	Комплекс программного обеспечения, реализующего защиту от несанкционированного доступа должен осуществлять: 1. СЗИ НСД должна представлять собой программный комплекс средств защиты информации в операционных системах семейства Windows с возможностью подключения аппаратных идентификаторов. 1.1. СЗИ НСД должна быть сертифицирована по требованиям Руководящих документов (РД)	Россия	б/с	усл. ед.	2	7 650,00	15 300,00

№ п/п	Наименование Услуг	Характеристика Услуг	Производи-тель/, страна происхожд ения	Срок годно сти	Ед. изм .	Кол-во	Цена за единицу, руб.	Цена Договора, руб.
		ФСТЭК России (Гостехкомиссии России) по 5-му классу защиты от НСД для СВТ и 4-му уровню контроля отсутствия НДВ, разрабатываться и производиться на основании лицензии органов, имеющих федеральные полномочия в указанной сфере. 1.2. СЗИ НСД может быть использована при создании защищенных автоматизированных систем до класса защищенности 1Г включительно, для обеспечения 1 уровня защищенности персональных данных, в государственных информационных системах 1 класса защищённости и в автоматизированных системах управления до 1 класса защищённости включительно. 1.3. Подсистема СКН должна быть сертифицирована по требованиям профиля защиты средств контроля подключения съемных машинных носителей информации (ИТ.СКН.П4.ПЗ) по 4 классу. 2. 2.1 СОВ должна быть сертифицирована на соответствие требованиям ФСТЭК России к системам обнаружения вторжений по 4-му классу защиты, в соответствии с профилем защиты систем обнаружения вторжений уровня узла четвертого класса защиты (ИТ.СОВ.У4.ПЗ) и 4-му уровню контроля отсутствия НДВ (РД НДВ, Гостехкомиссия России, 1999 г.), разрабатываться и производиться на						

№ п/п	Наименование Услуг	Характеристика Услуг	Производи-тель/, страна происхожд ения	Срок годно сти	Ед. изм .	Кол-во	Цена за единицу, руб.	Цена Договора, руб.
		основании лицензии федеральных органов, имеющих полномочия в указанной сфере. 2.2. СОВ может быть использована при создании защищенных автоматизированных систем до класса защищенности 1Г включительно, для обеспечения 1 уровня защищенности персональных данных, в государственных информационных системах 1 класса защищённости и в автоматизированных системах управления до 1 класса защищённости включительно. 3. СЗИ НСД должна обеспечивать: 3.1. Регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере. 3.2. Идентификацию и проверку подлинности пользователей при входе в операционную систему. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность аппаратного идентификатора конкретному пользователю. Поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим						

№ п/п	Наименование Услуг	Характеристика Услуг	Производитель/, страна происхождения	Срок годности	Ед. изм.	Кол-во	Цена за единицу, руб.	Цена Договора, руб.
		центром Windows.						
	Право на использование сертифицированных средств криптографической защиты информации ViPNet Client (сеть 2029)	Программное обеспечение, реализующее функции криптографического клиента для работы с автоматизированной информационной системой (далее – ПО VPN-клиента), должно отвечать следующим требованиям: 1. Должно быть полностью совместимо с ПО ViPNet Administrator 4.x номер сети 2029 в части: • обновления ПО; • автоматического обновления справочной и ключевой информации VPN-сети; • управления политиками безопасности. 2. Должно быть полностью совместимо с ПАК ViPNet Coordinator HW100/1000/2000 4.x номер сети 2029, в части шифрования/расшифрования отправляемого/принимаемого IP-трафика. 3. Обеспечивать безопасную передачу (прием) данных VPN-шлюзам и VPN-клиентам (точка-точка) с использованием произвольной телекоммуникационной инфраструктуры IP-сетей, включая сети связи общего пользования.	Россия	б/с	усл. ед.	2	15 000,00	30 000,00
	Аттестация объекта информатизации по требованиям безопасности информации 1 АРМ	- Требования к оценке и оптимизации разработанных требований и организационно - распорядительной документации Заказчика в разрезе обеспечения защиты информации в АИС. - Требования к разработке моделей угроз:	Россия	б/с	усл. ед.	1	25 000,00	25 000,00

№ п/п	Наименование Услуг	Характеристика Услуг	Производитель/, страна происхождения	Срок годности	Ед. изм.	Кол-во	Цена за единицу, руб.	Цена Договора, руб.
		Цель оказания услуг: • выполнить требования нормативных документов ФСБ России и ФСТЭК России; • определить актуальные угрозы безопасности; • определить требования к классам средств защиты информации. Состав услуг: • разработка модели угроз и нарушителя безопасности ПДн, с учетом требований методических документов ФСТЭК России и ФСБ России (при необходимости), в частности формирование: о по требованиям ФСТЭК России: - описания объекта защиты (цели защиты, состав и структура ИС, информационная характеристика ИС, описание информационных и технологических процессов); - перечня возможных угроз; - оценки исходной защищенности ИС; - оценок возможности угроз; - оценок опасности угроз; - определенного перечня актуальных угроз; - требований к классам средств защиты; о по требованиям ФСБ России (при необходимости): - описания объекта защиты (цели защиты, состав и структура ИС, информационная характеристика ИС, описание информационных и технологических процессов); - описания угроз (модель угроз);						

№ п/п	Наименование Услуг	Характеристика Услуг	Производи-тель/, страна происхожд ения	Срок годно сти	Ед. изм .	Кол-во	Цена за единицу, руб.	Цена Договора, руб.
		- типизации нарушителей; - предположений об имеющейся у нарушителей информации; - предположений об имеющихся у нарушителей средствах атак; - предположений об ограничениях на возможности нарушителей; - выводов о типах нарушителей, требуемых классах средств криптографической защиты информации. Результат оказания услуг: • актуальная модель угроз и нарушителей безопасности ПДн Заказчика. Отчетность: • результаты оказанных услуг должны быть включены в актуальную модель угроз и нарушителей безопасности ПДн Заказчика.						
	ИТОГО:							73 950,00

ИТОГО: 73 950 (семьдесят три тысячи девятьсот пятьдесят) рублей 00 копеек, без НДС, в связи с тем, что Исполнитель применяет УСН.

ИСПОЛНИТЕЛЬ:
Управляющий директор
АО «ВСЦ ЕВРААС»

_____ **А.А. Фереферов**
МП

ЗАКАЗЧИК:
Главный врач
ОГАУЗ Ангарская городская больница № 1»

_____ **И.В. Крывовязый**
МП

Приложение № 2
к договору № 129150
от «_____» _____ 2017г.

Технические требования, предъявляемые к услугам по передаче неисключительных прав на воспроизведение и использование комплекса программного обеспечения, реализующего защиту от несанкционированного доступа

Комплекс программного обеспечения, реализующего защиту от несанкционированного доступа должен осуществлять:

1. СЗИ НСД должна представлять собой программный комплекс средств защиты информации в операционных системах семейства Windows с возможностью подключения аппаратных идентификаторов.
2. СЗИ НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows 10, Windows Server 2012 R2/Debian 7.8, Centos 7.0, Fedora 20, OpenSuse 12.3, Red Hat Enterprise Linux 7 в многопользовательском режиме их эксплуатации.
3. СЗИ НСД должна поддерживать 32- и 64-битные версии операционных систем.
4. СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go.
5. СЗИ НСД должна быть сертифицирована по требованиям Руководящих документов (РД) ФСТЭК России (Гостехкомиссии России) по 5-му классу защиты от НСД для СВТ и 4-му уровню контроля отсутствия НДВ, разрабатываться и производиться на основании лицензии органов, имеющих федеральные полномочия в указанной сфере.
6. СЗИ НСД может быть использована при создании защищенных автоматизированных систем до класса защищенности 1Г включительно, для обеспечения 1 уровня защищенности персональных данных, в государственных информационных системах 1 класса защищённости и в автоматизированных системах управления до 1 класса защищённости включительно.
7. Подсистема СКН должна быть сертифицирована по требованиям профиля защиты средств контроля подключения съемных машинных носителей информации (ИТ.СКН.П4.ПЗ) по 4 классу.
8. Система обнаружения и предотвращения вторжений (далее СОВ) должна представлять собой программный модуль средства защиты информации в операционных системах семейства Windows и должна быть предназначена для обнаружения и блокирования основных угроз безопасности информации, выполняя одновременно функции и сетевой, и хостовой системы обнаружения вторжений.

8.1. СОВ должна быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, в многопользовательском режиме их эксплуатации.

8.2. СОВ должна поддерживать 32- и 64-битные версии операционных систем.

8.3. СОВ должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go.

8.4. СОВ должна быть сертифицирована на соответствие требованиям ФСТЭК России к системам обнаружения вторжений по 4-му классу защиты, в соответствии с профилем защиты систем обнаружения вторжений уровня узла четвертого класса защиты (ИТ.СОВ.У4.ПЗ) и 4-му уровню контроля отсутствия НДВ (РД НДВ, Гостехкомиссия России, 1999 г.), разрабатываться и производиться на основании лицензии федеральных органов, имеющих полномочия в указанной сфере.

8.5. СОВ может быть использована при создании защищенных автоматизированных систем до класса защищенности 1Г включительно, для обеспечения 1 уровня защищенности персональных данных, в государственных информационных системах 1 класса защищённости и в автоматизированных системах управления до 1 класса защищённости включительно.

8.6. СОВ должна обеспечивать:

8.7. сбор и анализ информации о сетевом трафике и событиях, регистрируемых в журналах аудита ОС;

8.8. анализ собранных данных СОВ о сетевом трафике в режиме, близкому к реальному масштабу времени;

8.9. использование сигнатурных и эвристических методов для анализа сетевого трафика, журналов ОС и приложений на предмет нештатных ситуаций, а также попыток проведения вторжений. Эвристический метод анализа собранных данных должен быть основан на методах выявления аномалий сетевого трафика и аномалий в действиях пользователя ОС;

8.10. возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем (OSI);
8.11. блокировку IP-адреса атакующего ПК с возможностью настройки времени блокировки;
8.12. возможность автоматизированного обновления базы решающих правил СОВ;
8.13. возможность настройки эвристики и реакции для следующих типов событий (атак):
8.14. - сканирование портов;
8.15. - ARP spoofing/poisoning;
8.16. - IP spoofing.
8.17. Атаки на TCP/IP стек, такие как:
8.18. - Ping of death;
8.19. - Smurf;
8.20. - Land;
8.21. - Short Headers;
8.22. - Open Tear;
8.23. - TearDrop (для ICMP протокола);
8.24. - перекрытие заголовков сетевых пакетов;
8.25. - атаки на фрагментацию IGMP;
8.26. - реагирование на аномальную сетевую активность.
8.27. контроль приложений с возможностью настройки правил контроля. Перехват вызовов функций от приложений к ОС и отслеживание следующих событий:
8.28. обращения ПО к системному реестру и критическим объектам операционной системы. Критическими являются объекты, удаление, блокирование или модификация которых оказывает влияние на функционирование или безопасность ОС;
8.29. DDE- и OLE- взаимодействие;
8.30. вызов DNS API;
8.31. попытки модификации или удаления объектов ПО СОВ;
8.32. обращения ПО к объектам файловой системы, в том числе прямой доступ к диску;
8.33. попытки внедрения компонент – подмена и установка сторонних библиотек, установка системных перехватчиков, через которые посторонний код может быть внедрен в другой процесс, оконные перехватчики;
8.34. внедрение в память процесса;
8.35. запросы на завершение и запуск процессов;
8.36. низкоуровневый сетевой доступ;
8.37. попытки снятия скриншота экрана, несанкционированного доступа к буферу обмена или перехват нажатия клавиш приложениями.
8.38. фиксацию факта обнаружения вторжений или нарушения безопасности в журналах аудита, ведение статистики сетевых атак и возможность уведомления администратора об обнаруженных вторжениях. Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки и архивации записей;
8.39. возможность сохранения конфигурации для последующего восстановления настроек СОВ;
8.40. возможность настройки всех параметров СОВ из единой консоли администрирования;
8.41. возможность локального и удаленного администрирования (управления наборами сигнатур, настройкой переменных и параметров СОВ, просмотр статистки и журналов);
8.42. возможность подключения к модулям администрирования пользователя с ограниченными правами (права только на просмотр настроек; только на просмотр журналов аудита; полные права с возможностью делегирования);
8.43. Реализация СОВ должна быть полностью программной с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, а также аппаратных идентификаторов: USB-Flash-накопители, Touch Memory (iButton), eToken Pro/Java (USB-ключи и смарт-карты), USB-ключи Rutoken, JaCarta ГОСТ/PKI (USB-ключи и смарт-карты), карты HID Proximity.
8.44. Поставка СОВ должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием требуемого количества лицензий. Вариант формулировки:
8.45. неисключительное право на использование модуля СОВ (программное обеспечение).

9. СЗИ НСД должна обеспечивать:
9.1. Регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере.
9.2. Идентификацию и проверку подлинности пользователей при входе в операционную систему. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность

аппаратного идентификатора конкретному пользователю. Поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows.

9.3. Возможность автоматического выбора аппаратного идентификатора в окне авторизации при входе в операционную систему.

9.4. Возможность настройки принудительной двухфакторной аутентификации для учётной записи с правами администратора и/или пользователя.

9.5. Возможность средствами СЗИ НСД выполнить настройку периода действия учётной записи.

9.6. Возможность настройки предупреждения пользователя до входа в систему о том, что в информационной системе реализованы меры по обеспечению безопасности информации.

9.7. Возможность при создании учётной записи выбрать тип учётной записи (внутренний, внешний, системный, приложение, гостевой, временный).

9.8. Реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам.

9.9. Должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), реестру, сети, съемным носителям информации. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных.

9.10. Должен выполняться контроль аппаратной конфигурации компьютера и следующих подключаемых устройств:

– Android-устройств;
– iOS-устройств;
– Bluetooth-устройств;
– DVD- и CD-ROM-дисководов;
– устройств HID, MTD, PCMCIA, IEEE 1394, Secure Digital;
– USB-контроллеров;
– беспроводных устройств (Wireless Communication Devices);
– биометрических устройств;
– дисководов магнитных дисков;
– звуковых, видео- и игровых устройств;
– инфракрасных устройств (IrDA);
– контроллеров магнитных дисков;
– ленточных накопителей;
– модемов;
– переносных устройств;
– портов (COM и LPT);
– сенсоров;
– сетевых адаптеров;
– сканеров и цифровых фотоаппаратов;
– принтеров;
– съемных носителей информации (CD-ROM, FDD, USB-Flash-накопителей).

9.11. Для предотвращения утечки информации с использованием съемных носителей информации СЗИ НСД должна позволять разграничивать доступ, как к отдельным типам носителей, так и к конкретным экземплярам.

9.12. Должно обеспечиваться преобразование информации:

– на съемных носителях информации, для создания доверенной среды при работе со съемными носителями;
– при работе с виртуальными дисками (преобразование выполняется незаметно для пользователя);
– при создании преобразованных файлов-контейнеров, используемых для хранения информации на внешних носителях или для передачи по различным каналам связи.

9.13. Должна выполняться блокировка виртуальных дисков с преобразованной информацией при отключении аппаратного идентификатора.

9.14. Должна быть обеспечена возможность работы с преобразованными файлами-контейнерами на компьютерах, где программное обеспечение СЗИ НСД не установлено.

9.15. Сохранение теневых копий файлов, записываемых на съемные носители.

9.16. В соответствии с требованиями к СЗИ НСД должен использоваться дискреционный принцип контроля доступа:

– обеспечивает доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа).

9.17. Возможность ограничивать средствами СЗИ НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа).
9.18. Регистрация и учет (аудит) действий пользователей независимыми от ОС средствами (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки и архивации записей.
9.19. Расширенные возможности аудита печати: печать документов с возможностью добавления штампа (произвольного или по ГОСТу), возможность сохранения теневых копий распечатываемых документов, разграничение доступа пользователей к печати и нанесению штампов.
9.20. Возможность организации замкнутой программной среды (ЗПС) и различные способы ее настройки.
9.21. Возможность разграничения доступа к буферу обмена.
9.22. Возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов).
9.23. Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений. Возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности.
9.24. Очистку остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Запрет смены пользователей без перезагрузки.
9.25. Выполнение регистрации действий по зачистке остаточной информации.
9.26. Возможность самодиагностики основного функционала СЗИ НСД с возможностью сохранения отчета.
9.27. Возможность сохранения конфигурации для последующего восстановления СЗИ НСД.
9.28. Ведение двух копий программных средств защиты информации и возможность возврата к настройкам по умолчанию.
9.29. Возможность настройки репликации серверов безопасности.
9.30. Централизованное управление лицензиями на терминальные подключения и на клиентов в нескольких доменах безопасности, при использовании отдельного модуля «Сервер лицензий».
9.31. Централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учетными записями пользователей, политиками, правами пользователей, преобразованными съемными носителями информации. Должна поддерживаться многоуровневая иерархия групп компьютеров и наследование установленных параметров. Также этим модулем должен осуществляться периодический сбор журналов со всех защищенных рабочих станций. Возможность блокировки компьютера, завершения сеанса работы пользователя по команде администратора.
9.32. Возможность нотификации о наличии обновлений для СЗИ НСД на сервере компании.
9.33. Возможность сигнализации администратору безопасности о ситуациях несанкционированного доступа на клиентских рабочих станциях:
– нарушение контроля целостности объекта;
– попытка работы после блокировки при нарушении целостности;
– попытка входа на клиентскую рабочую станцию с неправильным паролем;
– блокировка пользователя после многократного ввода неправильного пароля;
– СЗИ НСД на клиенте не отвечает (возможная причина – несанкционированная деактивация системы защиты);
– клиент недоступен долгое время (с возможностью задания периода времени);
– попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами.
9.34. Блокировка доступа к файлам по расширению.
9.35. Возможность настройки всех параметров СЗИ НСД из единой консоли администрирования.
9.36. Возможность создания отчета по назначенным правам, формирование паспорта программного обеспечения, установленного на ПЭВМ, формирование паспорта аппаратной части ПЭВМ.
9.37. Возможность построения иерархии управления при помощи специального модуля – менеджера, управляющего несколькими модулями централизованного управления.
9.38. Возможность использования механизма удаленной установки и обновления СЗИ НСД средствами модуля централизованного управления самой СЗИ или средствами групповых политик Active Directory.
9.39. Возможность визуализации сети защищаемых компьютеров.

9.40. Возможность подключения к модулям администрирования пользователя с ограниченными правами (права только на просмотр настроек; только на просмотр журналов аудита; полные права с возможностью делегирования).
9.41. Возможность выполнять синхронизацию времени между сервером безопасности и клиентами.
9.42. Должен быть реализован модуль межсетевого экрана. Данный модуль должен обеспечивать защиту рабочих станций и серверов от НСД посредством осуществления контроля и фильтрации проходящих через сетевые интерфейсы рабочих станций сетевых пакетов в соответствии с заданными администратором правилами.
9.43. Интеграцию с SIEM-системами.
10. Реализация СЗИ НСД должна быть полностью программной, но с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, включая идентификаторы: USB-Flash-накопители, Touch Memory (iButton), eToken Pro/Java (USB-ключи и смарт-карты), USB-ключи Rutoken, JaCarta ГОСТ/PKI (USB-ключи и смарт-карты), карты HID Proximity.
11. Поставка СЗИ НСД должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием всех необходимых модулей и требуемого количества лицензий по каждому модулю. Варианты формулировок:
– Неисключительное право на использование СЗИ НСД (программное обеспечение)
– Неисключительное право на использование сервера безопасности для СЗИ НСД (программное обеспечение)
– Неисключительное право на использование сервера лицензий для СЗИ НСД (программное обеспечение)
– Неисключительное право на терминальное подключение СЗИ НСД (программное обеспечение).
11.1. Возможность выполнять синхронизацию времени между сервером безопасности и клиентами.
11.2. Должен быть реализован модуль межсетевого экрана. Данный модуль должен обеспечивать защиту рабочих станций и серверов от НСД посредством осуществления контроля и фильтрации проходящих через сетевые интерфейсы рабочих станций сетевых пакетов в соответствии с заданными администратором правилами.
11.3. Интеграцию с SIEM-системами.
12. Реализация СЗИ НСД должна быть полностью программной, но с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, включая идентификаторы: USB-Flash-накопители, Touch Memory (iButton), eToken Pro/Java (USB-ключи и смарт-карты), USB-ключи Rutoken, JaCarta ГОСТ/PKI (USB-ключи и смарт-карты), карты HID Proximity.
13. Поставка СЗИ НСД должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием всех необходимых модулей и требуемого количества лицензий по каждому модулю. Варианты формулировок:
– Неисключительное право на использование СЗИ НСД (программное обеспечение)
– Неисключительное право на использование сервера безопасности для СЗИ НСД (программное обеспечение)
– Неисключительное право на использование сервера лицензий для СЗИ НСД (программное обеспечение)
– Неисключительное право на терминальное подключение СЗИ НСД (программное обеспечение).

ИСПОЛНИТЕЛЬ:
Управляющий директор
АО «ВСЦ ЕВРААС»

_____ А.А. Фереферов
МП

ЗАКАЗЧИК:
Главный врач
ОГАУЗ Ангарская городская больница № 1»

_____ И.В. Крывовязый
МП

Приложение № 3
к договору № 129150
от «_____» _____ 2017г.

Технические требования, предъявляемые к услугам по поставке установочного комплекта на комплекс программного обеспечения, реализующего защиту от несанкционированного доступа

В установочный комплект на программное обеспечение, реализующего антивирусную защиту должно входить:

1. Установочный диск – 1 шт.;
2. Формуляр в печатном виде – 1 шт.;
3. Лицензия на право воспроизведения в печатном виде - 1 шт.;
4. Копия сертификата соответствия – 1 шт.

ИСПОЛНИТЕЛЬ:
Управляющий директор
АО «ВСЦ ЕВРААС»

_____ А.А. Фереферов
МП

ЗАКАЗЧИК:
Главный врач
ОГАУЗ Ангарская городская больница № 1»

_____ И.В. Крывовязый
МП

Приложение № 4
к договору № 129150
от «_____» _____ 2017г.

Технические требования, предъявляемые к услугам по передаче неисключительных прав на использование программного обеспечения, реализующего функции криптографического клиента для работы с автоматизированной информационной системой

Общие требования:

Программное обеспечение, реализующее функции криптографического клиента для работы с автоматизированной информационной системой (далее – ПО VPN-клиента), должно отвечать следующим требованиям:

1. Должно быть полностью совместимо с ПО ViPNet Administrator 4.x номер сети 2029 в части:
- обновления ПО;
- автоматического обновления справочной и ключевой информации VPN-сети;
- управления политиками безопасности.

2. Должно быть полностью совместимо с ПАК ViPNet Coordinator HW100/1000/2000 4.x номер сети 2029, в части шифрования/расшифрования отправляемого/принимаемого IP-трафика.
3. Обеспечивать безопасную передачу (прием) данных VPN-шлюзам и VPN-клиентам (точка-точка) с использованием произвольной телекоммуникационной инфраструктуры IP-сетей, включая сети связи общего пользования.

В состав ПО VPN-клиента должны входить:

1. Драйвер сетевой защиты, непосредственно взаимодействующий с драйвером сетевого интерфейса компьютера и осуществляющий контроль и фильтрацию сетевого трафика.
2. Сервис управления драйвером сетевой защиты, обеспечивающий функционирование узла в защищенной сети, а именно загрузку в драйвер защиты правил фильтрации, справочной информации о структуре защищенной сети и ключей шифрования, сведений о сетевых параметрах доступа для узлов защищенной сети, передачу в ПО VPN-клиента результатов обработки IP-пакетов.
3. Драйвер шифрования IP-пакетов, осуществляющий шифрование и имитозащиту сетевого трафика на ключах, созданных в ПК управления VPN-сетью.
4. Приложение, осуществляющее настройку фильтров, подготовку необходимых фильтров и ключевой информации для загрузки в драйвера, аудит основных событий, ограничение интерфейса пользователя и администратора в ПО VPN-клиента, а также установку соответствующих фильтров IP-трафика в дополнение к собственным настроенным правилам фильтрации трафика.
5. Система обновления, обеспечивающая обновление ключевой и справочной информации, а также ПО VPN-клиента.
6. Сервис регистрации пользователя, обеспечивающий обработку событий аутентификации пользователя VPN-клиента.
7. Транспортный модуль, реализующий обмен управляющей, адресной и ключевой информацией с ПК управления защищенной сетью, отправку, прием и маршрутизацию электронных документов (почтовых конвертов), отправку, прием и маршрутизацию электронных документов (почтовых конвертов).
8. Службу контроля приложений, осуществляющая контроль сетевой активности приложений и позволяющая реализовывать политики доступа приложений в сеть.
9. ПО для обмена зашифрованными и подписанными сообщениями.
10. ПО для осуществления защищенных почтовых услуг с возможностями аутентификации отправителя и получателя, квитирования (доставлено, прочитано), электронной подписи (далее – ЭП).
11. ПО для реализации дополнительных сервисов: защищенный чат, защищенная конференция, защищенный обмен файлами.
12. Средство криптографической защиты информации.

Функциональные требования:

ПО VPN-клиента должно выполнять следующие функции:

1. Обеспечивать шифрование и имитозащиту IP-трафика, файлов и почтовых сообщений.
2. Шифрование и имитозащита IP-трафика должны обеспечиваться по алгоритму ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
3. Осуществлять функции персонального межсетевого экрана, обеспечивающие:
- контроль сетевого трафика, проходящего через сетевые интерфейсы;

- фильтрацию IP-пакетов по заданным правилам для зашифрованного и открытого сетевых трафиков по совокупности критериев (IP-адреса, протоколы, порты);
- реализацию режима инициативных соединений.

4. Осуществлять функцию обмена зашифрованными и подписанными сообщениями (электронная почта), а также контроль за прохождением и состоянием сообщений.
5. Поддерживать прозрачную работу через различные NAT-устройства.
6. Обеспечивать конфиденциальность, целостность и аутентификацию каждого IP-пакета.
7. Создание и проверка ЭП.
8. Создание ЭП, проверка ЭП, создание ключей ЭП и ключей проверки ЭП должны осуществляться в соответствии с алгоритмом ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
9. Хэширование данных в соответствии с алгоритмами ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция Хэширования» и ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».
10. Формирование ключей шифрования для алгоритма ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
11. Аутентификация, передача данных по протоколу TLS с использованием алгоритмов ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 и ГОСТ 28147-89.
12. Формирование сообщений PKCS #7 (CMS) с использованием алгоритмов ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 и ГОСТ 28147-89.
13. Формирование транспортных ключевых контейнеров в формате PKCS #12 (PFX) с использованием алгоритмов ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 и ГОСТ 28147-89
14. Автоматически обрабатывать обновления, полученные из ПК управления VPN-сетью.
15. Автоматически формировать и отправлять квитанции о результатах обработки обновлений, полученные из ПК управления VPN-сетью.

Требования к аппаратному обеспечению

ПО VPN-клиента должно корректно функционировать со следующими минимальными требованиями:

1. Процессор — IntelCore 2 Duo или другой схожий по производительности x86-совместимый процессор.

- Объем оперативной памяти — не менее 1 Гбайт.
- Свободное место на жестком диске — не менее 150Мбайт.
- Операционная система:
- Microsoft Windows Vista (32/64-разрядная);
- Microsoft Windows 7 (32/64-разрядная);
- Microsoft Windows 8 (32/64-разрядная);
- Microsoft Windows 8.1 (32/64-разрядная);
- Microsoft Windows 10 (32/64-разрядная);
- Microsoft Windows Small Business Server 2008 (64-разрядная);
- Microsoft Windows Small Business Server 2008 SP2 (64-разрядная);
- Microsoft Windows Small Business Server 2011 (64-разрядная);
- Microsoft Windows Server 2012 R2 (64-разрядная);
- Microsoft Windows Server 2008 (32/64-разрядная);
- Microsoft Windows Server 2008 R2 (64-разрядная);
- Microsoft Windows Server 2012 (64-разрядная).

Требования по сертификации

Вариант исполнения 1

1. Должен быть сертифицирован на соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1.
2. Должен быть сертифицирован на соответствие требованиям ФСБ России устройствам типа межсетевые экраны по 4 классу защищенности.
3. Должен быть сертифицирован на соответствие требованиям ФСТЭК России к устройствам типа межсетевые экраны по 3 классу защищенности.

ИСПОЛНИТЕЛЬ:
Управляющий директор

АО «ВСЦ ЕВРААС»

_____ А.А. Фереферов
МП

ЗАКАЗЧИК:
Главный врач
ОГАУЗ Ангарская городская больница № 1»

_____ И.В. Крывовязый
МП

Приложение № 5
к договору № 129150
от «_____» _____ 2017г.

Технические требования, предъявляемые к услугам по поставке установочного комплекта на программное обеспечение, реализующее функции криптографического клиента для работы с автоматизированной информационной системой

В установочный комплект должно входить:
1. CD-дистрибутив ПО – 1 шт.;
2. Формуляр в печатном виде – 1 шт.;
3. Копия сертификата соответствия – 1 шт.

ИСПОЛНИТЕЛЬ:
Управляющий директор
АО «ВСЦ ЕВРААС»

_____ А.А. Фереферов
МП

ЗАКАЗЧИК:
Главный врач
ОГАУЗ Ангарская городская больница № 1»

_____ И.В. Крывовязый
МП

Приложение № 6
к договору № 129150
от «_____» _____ 2017г.

Технические требования, предъявляемые к услугам по поставке сертификата активации сервиса прямой технической поддержки сроком на 12 месяцев на программное обеспечение, реализующее функции криптографического клиента для работы с автоматизированной информационной системой

Сертификат активации сервиса прямой технической поддержки сроком на 12 месяцев на программное обеспечение, реализующее функции криптографического клиента для работы с автоматизированной информационной системой, должен распространяться на 1 лицензию номер сети 2029, указанную в Приложении 5 настоящего ТЗ.

На первой линии технической поддержки должна выступать служба технической поддержки Производителя.

Услуги по технической поддержке должны включать:

1. Время и способ приема сообщений (включая запросы через web-форму с сайта Производителя):
1.1. Прием обращений и консультирование по электронной почте с 9:00 до 18:00 (по московскому времени).
1.2. Прием обращений и консультирование по электронной почте с 1:00 до 20:00 (по московскому времени).
1.3. Прием обращений и консультирование по телефону горячей линии с 9:00 до 18:00 (по московскому времени).
1.4. Прием обращений и консультирование по телефону горячей линии с 1:00 до 20:00 (по московскому времени).
2. Консультирование при установке Продуктов:
2.1. Рекомендации по процессу установки продукта в объеме эксплуатационной документации.
3. Консультирование при эксплуатации Продуктов:
3.1. Рекомендации по настройке продукта в объеме эксплуатационной документации
3.2. Рекомендации по «тонкой» настройке продукта после знакомства с особенностями системы Заказчика
3.3. Диагностика с целью установления факта ошибки в работе программного продукта. Выявленная ошибка, в зависимости от сложности, устраняется в процессе диагностики или в последующих обновлениях ПО.
4. Обновление Продуктов:
4.1. Предоставление обновления (hotfix), устраняющее дефекты, выявленные в продукте.
4.2. Предоставление обновления (hotfix), а также все изменения, производимые в рамках минорной (minor) версии продукта (service pack).
4.3. Предоставление новых версий (изменение мажорной (major) версии, поколения) продукта без взимания дополнительной платы (для ПАК — только программные компоненты).
5. Ремонт или замена неисправного оборудования:

Восстановление работоспособности (ремонт) вышедшего из строя оборудования (аппаратной платформы ПАК) из состава Продуктов Заказчика в соответствии с гарантийными обязательствами Производителя. Доставка не входит в стоимость.

ИСПОЛНИТЕЛЬ:
Управляющий директор
АО «ВСЦ ЕВРААС»

_____ А.А. Фереферов
МП

ЗАКАЗЧИК:
Главный врач
ОГАУЗ Ангарская городская больница № 1»

_____ И.В. Крывовязый
МП

Приложение № 7
к договору № 129150
от «_____» _____ 2017г.

Технические требования, предъявляемые к услугам по передаче неисключительных прав на использование комплекса программного обеспечения, реализующего антивирусную защиту

Комплекс программного обеспечения, реализующего антивирусную защиту должен осуществлять:
- защиту компьютера от атак по сети TCP/IP;
- антивирусную защиту от вредоносного программного обеспечения;
- защиту от спама и вредоносного контента веб-серверов;
- самозащиту от воздействия со стороны вредоносного программного обеспечения;
- регистрацию событий безопасности;

Комплекс программного обеспечения, реализующего межсетевое экранирование, антивирусную защиту, обнаружение вторжений должно функционировать на следующих операционных системах и аппаратной части:
- Windows 8, 7, Vista, XP x86/x64; Windows Server 2012 x64; Windows Server 2008 R2 x64, Server 2008 x86/x64;Windows Server 2003 R2 x86/x64, Server 2003 x86/x64;
- наличие привода CD-ROM;
- минимально необходимый размер оперативный памяти: не менее 512 Мбайт.

Требования к функциональности комплекса программного обеспечения, реализующего антивирусную защиту:
- должно контролировать входящие и исходящие соединения;
- должно обеспечивать контроль для приложений, использующихся на компьютере, при обращении к сети и создание правил сетевого доступа для приложений;
- режим обучения для сетевого доступа для приложений;
- разделение доступа к узлам сети;
- создание разрешенного и запрещенного списков сетевых ресурсов;
- возможность экспорта/импорта настроек межсетевого экрана с одного компьютера на другой;
- должно обеспечивать блокировку активного содержимого страниц веб-серверов;
- должно обеспечивать блокировку активного содержимого входящих электронных писем;
- должно обеспечивать регистрацию событий безопасности.
- - должно обеспечивать настройку на обнаружение типовых сетевых атак;
- должно обеспечивать блокировку сетевых сканеров;
- должно обеспечивать блокировку вредоносных процессов при их попытках воздействия на рабочие процессы;
- должно обеспечивать непрерывный мониторинг;
- должно обеспечивать регистрацию событий безопасности.
- должно соответствовать: требованиями руководящего документа "Требования к средствам антивирусной защиты" (утвержден приказом ФСТЭК России от 20 марта 2012 г. № 28) для типов "А" (при наличии), "Б", "В" и "Г" не ниже 4-го класса защиты;
- должно обеспечивать автоматическую проверку наличия вредоносных программ по типовым сигнатурам и с помощью эвристического анализа;
- должно обеспечивать сканирование локальных дисков, подключаемых дисков, отчуждаемых носителей, в том числе по команде и по расписанию;
- должно обеспечивать удаление вредоносного программного обеспечения и его блокировку (перемещение в “карантин”);
- должно обеспечивать откат операций удаления программного обеспечения, воспринятого как вредоносное;
- должно обеспечивать кэширование данных сканирования для сокращения времени обнаружения вредоносного программного обеспечения;
- должно иметь возможность обновления антивирусных баз;
- должно обеспечивать проверку вложений почтовых сообщений на наличие вредоносного программного обеспечения;
- должно обеспечивать блокировку активных элементов веб-страниц (ActiveX, Flash, Java, Visual Basic);
- должно обеспечивать защиту электронной почты (Outlook 2000, 2002, 2003, 2007; Microsoft Outlook Express 5.0, 5.5 и 6.0; Vista Mail;The Bat!) от спама;
- должно обеспечивать регистрацию событий безопасности;

- иметь соответствующие сертификаты ФСТЭК России.

ИСПОЛНИТЕЛЬ:
Управляющий директор
АО «ВСЦ ЕВРААС»

_____ А.А. Фереферов
МП

ЗАКАЗЧИК:
Главный врач
ОГАУЗ Ангарская городская больница № 1»

_____ И.В. Крывовязый
МП

Приложение № 8
к договору № 129150
от «_____» _____ 2017г.

Технические требования, предъявляемые к услугам по поставке установочного комплекта на комплекс программного обеспечения, реализующего антивирусную защиту

В установочный комплект на программное обеспечение, реализующего антивирусную защиту должно входить:

1. Установочный диск – 1 шт.;
2. Формуляр в печатном виде – 1 шт.;
3. Лицензия на право воспроизведения в печатном виде - 1 шт.;
4. Копия сертификата соответствия – 1 шт.

ИСПОЛНИТЕЛЬ:
Управляющий директор
АО «ВСЦ ЕВРААС»

_____ А.А. Фереферов
МП

ЗАКАЗЧИК:
Главный врач
ОГАУЗ Ангарская городская больница № 1»

_____ И.В. Крывовязый
МП

Приложение № 9
к договору № 129150
от «_____» _____ 2017г.

Форма сведений об исполнении договора

Сведения об исполнении договора
на оказание услуг по аттестации рабочих мест для работы с базой данных реципиентов крови
№ 129150 от «__» _____2017г.

г. Ангарск «__»_____ 201_г.

Акционерное общество «Восточно-Сибирский центр ЕВРААС», именуемое в дальнейшем "Исполнитель", в лице Управляющего директора Фереферова Андрея Альбертовича, действующего на основании приказа №01/08 от 17 августа 2016 года, с одной стороны, и областное государственное автономное учреждение здравоохранения "Ангарская городская больница № 1", именуемое в дальнейшем Заказчик, в лице главного врача Крывовязого Ивана Викторовича, действующего на основании Устава, с другой стороны, далее именуемые Стороны, составили настоящие Сведения о нижеследующем:

1. Стороны пришли к соглашению о том, что договор **на оказание услуг по аттестации рабочих мест для работы с базой данных реципиентов крови** № 129150 от «___» _____ 201_г. исполнен на общую сумму_____***(_____) рублей 00 копеек, включая НДС.***

2. Услуга оказана Исполнителем Заказчику по цене, указанной в Спецификации.

3. Оплата за оказанную Услугу Заказчиком оплачена Исполнителю в полном объеме.

Спецификация

№ п/п	Наименование Услуг	Характеристика Услуг	Производи-тель/, страна происхождения	Срок годности	Ед. изм.	Кол-во	Цена за единицу, руб.	Цена Договора, руб.
.								
.								
							ИТОГО:	

ИСПОЛНИТЕЛЬ:

Управляющий директор
АО «ВСЦ ЕВРААС»

_____ А.А. Фереферов

ЗАКАЗЧИК:

Главный врач

ОГАУЗ «Ангарская городская больница № 1»

_____И.В. Крывовязый

Подписи сторон:
Крывовязый Иван Викторович **Фереферов Андрей Альбертович**