Утверждаю
Заместитель генерального директора
(по цифровому развитию)

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На приобретение неисключительных прав (лицензий) на использование системы криптографической защиты информации, работы по внедрению и техническую поддержку для нужд АО «БСК»

СОДЕРЖАНИЕ

ГЛОССАРИЙ

ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
ФСБ	Федеральная служба безопасности Российской Федерации
ОС	Операционная система
ТЗ	Техническое задание
Исполнитель	Победитель по результатам проведения процедуры закупки в соответствии с требованиями Федерального закона от 18 июля 2011 года № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»
ПО	Программное обеспечение
ПАК	Программно-аппаратный комплекс
СКЗИ	Система криптографической защиты информации

АННОТАЦИЯ

Настоящее Техническое задание (далее – ТЗ) регламентирует требования к внедрению системы криптографической защиты информации в компании Акционерное Общество «Башкирская содовая компания» (АО «БСК»).

Документ содержит описание текущего состояния объекта автоматизации, требования к составу ПО, базовые требования к системе, требования к составу и содержанию работ по внедрению системы, требования к оформлению документации.

1. ОБЩИЕ СВЕДЕНИЯ

1.1.Полное наименование системы

Система криптографической защиты информации (далее – Система).

1.2.Наименование заказчика системы

Акционерное Общество «Башкирская содовая компания».

1.3.Сроки начала и окончания работ

96 (девяносто шесть) рабочих дней с даты заключения Договора.

1.4.Сведения об источниках и порядке финансирования работ

Источник финансирования – собственные средства Заказчика.

1.5.Перечень нормативно-технических документов, методических материалов

ГОСТ 34.201-2020. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем».

ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

1.6.Место выполнения работ

Республика Башкортостан, г. Стерлитамак, ул. Техническая, 32.

Выполнение работ может осуществляться Исполнителем удаленно или на территории Заказчика в присутствии представителей Заказчика.

1.7. Порядок оформления и предъявления Заказчику результатов выполнения работ

Порядок оформления и предъявления Заказчику результатов выполнения работ определен разделами 5 и 6 настоящего ТЗ.

Совместно с предъявлением Системы производится сдача разработанного Исполнителем комплекта документации согласно Приложению № 2 настоящего ТЗ.

Оформление и предъявление Заказчику результатов работ должно выполняться в соответствии с условиями настоящего ТЗ и Договора.

Работы должны быть выполнены в соответствии с разделами 4 и 5 настоящего ТЗ.

Программное обеспечение передается согласно спецификации, представленной в Приложении № 1 настоящего ТЗ.

Документы, разработанные в рамках Договора согласовываются (утверждаются) Заказчиком, в следующем порядке:

1) Заказчик в течение 15 (Пятнадцати) рабочих дней после дня получения документов от Подрядчика, рассматривает их и, при отсутствии замечаний, обеспечивает их согласование (утверждение) со своей стороны;

2) При наличии замечаний к документам в течение 15 (Пятнадцати) рабочих дней после дня получения этих документов, направляет Подрядчику мотивированный отказ от согласования (утверждения) документов с перечнем выявленных недостатков;

3) Подрядчик обязан своими силами и за свой счет устранить недостатки в течение 5 (Пяти) рабочих дней с момента получения мотивированного отказа Заказчика и вновь представить документы на рассмотрение Заказчику;

4) Рассмотрение представленных после устранения недостатков документов осуществляется в соответствии с пунктами 1-3 настоящего раздела.

2. НАЗНАЧЕНИЕ, ЦЕЛИ И ЗАДАЧИ ВНЕДРЕНИЯ СИСТЕМЫ

2.1.Назначение Системы

Система криптографической защиты информации представляют собой программно-аппаратный комплекс (далее - ПАК), который используются для шифрования защищаемой информации при обмене по открытым (не защищенным) каналам связи.

2.2.Основные цели и задачи внедрения Системы

Целью внедрения Системы является выполнения требований Федерального закона "О персональных данных" от 27.07.2006 N 152-ФЗ, Приказа ФСБ России от 10 июля 2014г. N378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

3. ХАРАКТЕРИСТИКА ОБЪЕКТА АВТОМАТИЗАЦИИ

В настоящее время у Заказчика отсутствует система криптографической защиты информации.

4. ТРЕБОВАНИЯ К СИСТЕМЕ

4.1. Требования к происхождению

ПО должно быть внесено в Единый реестр российских программ для электронных вычислительных машин и баз данных.

4.2.Требование к сертификации

Наличие сертификата соответствия ФСБ России

4.3.Функциональные требования

4.4.Требования к ПАК

Требования к ПАК представлены в таблице 1

Таблица 1. – Требования к ПАК

Программно-аппаратный комплекс ViPNet Coordinator HW 1000 4.x (или эквивалент)	Исполнение:	для установки в стойку 19”, высота 1U	для установки в стойку 19”, высота не более 1U
	Встроенная операционная система - адаптированная ОС Linux	наличие	наличие
	Сетевые интерфейсы 10/100/1000 Mbit/sec RJ45	4 шт.	не менее 4 шт.
	Производительность шифрования	400 Мбит/с	не менее 400 Мбит/с;
	Количество одновременно туннелируемых IP-адресов	не ограничено	не ограничено
	Возможность эксплуатации в пределах температурного режима от 0 до +50 °С, влажность от 0 до 90%	наличие	наличие

	Программное обеспечение, реализующее функции криптографического шлюза, использующее IP-адресацию для организации защищённых каналов связи с другими криптографическими шлюзами и защищёнными терминальными клиентами, основанную на шестнадцатеричных индентификаторах	наличие	наличие
	Программное обеспечение, реализующее функции криптографического шлюза, обеспечивающее шифрование каждого IP-пакета на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью	наличие	наличие
	Действующий сертификат на соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3 и возможности использования для криптографической защиты (шифрования и имитозащиты IP-трафика) информации	наличие	наличие
	Действующий сертификат на соответствие требованиям ФСБ России к устройствам типа межсетевые экраны по 4 классу защищенности	наличие	наличие
	Действующий сертификат на соответствие требованиям ФСТЭК России к межсетевым экранам типа «А» четвертого класса защиты	наличие	наличие
	Система управления	наличие	наличие
	Функционал обеспечения отказоустойчивости путём организации кластера на базе 2-х одинаковых программно-аппаратных комплексов в конфигурации «активный – пассивный»	наличие	наличие
	Функционал прокси-сервера защищенных соединений	наличие	наличие
	Функционал прозрачности для NAT-устройств (для защищенного трафика).	наличие	наличие
	Функционал работы в качестве DHCP-клиента, сервера	наличие	наличие
	Функционал поддержки Web-интерфейса для мониторинга текущего состояния	наличие	наличие

	Функционал IP TOS-мапирования поверх зашифрованных IP-пакетов (IP #241 или UDP), сохранение классификации трафика для защищенных пакетов, приоритетная обработка голосового и видеотрафика	наличие	наличие
	Функционал работы при изменении собственных IP-адресов, IP-адресов NAT–устройств, возможность работы за устройствами с динамическими правилами NAT	наличие	наличие
	Функционал туннелирующего сервера	наличие	наличие
	Функционал каскадирования в сегментированных сетях с целью разграничения доступа.	наличие	наличие
	Функционал назначения виртуальных IP-адресов для любых удаленных узлов.	наличие	наличие
	Функционал динамического NAT для открытых пакетов (организация доступа рабочих станций или сетевого оборудования в открытую сеть/Интернет)	наличие	наличие

4.5.Требования к средствам защиты информации для клиентских компонент VPN-сети

В качестве средства защиты информации для клиентских компонент VPN-сети (далее – VPN-клиент) должен использоваться программный комплекс (ПК), отвечающий следующим требованиям:

1. VPN-клиент должен быть полностью совместим с ПК управления VPN-сетью, в части:
- обновления программного обеспечения (ПО);
- автоматического обновления справочной и ключевой информации VPN-сети;
- управления политиками безопасности
2. VPN-клиент должен быть полностью совместим с VPN-шлюзами, представленными выше, в части шифрования/расшифрования отправляемого/принимаемого IP-трафика.
3. Поддерживать прозрачную работу через различные NAT-устройства.
4. Обеспечивать безопасную передачу (прием) данных VPN-шлюзам и VPN-клиентам (точка-точка) с использованием произвольной телекоммуникационной инфраструктуры IP-сетей, включая сети связи общего пользования.
5. Содержать драйвер сетевой защиты, непосредственно взаимодействующий с драйвером сетевого интерфейса и осуществляющий контроль, и фильтрацию сетевого трафика.
6. Содержать 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.
7. Содержать драйвер шифрования IP-пакетов, осуществляющий шифрование и имитозащиту сетевого трафика на ключах, созданных в ПК управления VPN-сетью.

8. Обеспечивать конфиденциальность, целостность и аутентификацию каждого IP-пакета.
9. Обеспечивать настройки сетевых фильтров, параметров доступа к VPN-узлам и аудита событий.
10. Содержать приложение, осуществляющее настройку фильтров, подготовку необходимых фильтров и ключевой информации для загрузки в драйвер, 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.
11. Содержать систему обновления, обеспечивающую обновление ключевой и справочной информации, а также ПО VPN-клиента.
12. Содержать сервис регистрации пользователя, обеспечивающий обработку событий аутентификации пользователя.
13. Содержать модуль, реализующий обмен управляющей, адресной и ключевой информацией с программным обеспечением централизованного управления защищенной сетью, отправку, прием и маршрутизацию электронных документов (почтовых конвертов), отправку, прием и маршрутизацию электронных документов (почтовых конвертов).
14. Содержать службу контроля приложений, осуществляющая контроль сетевой активности приложений и позволяющая реализовывать политики доступа приложений в сеть.
15. Содержать ПО для обмена зашифрованными и подписанными сообщениями.
16. Содержать программу, осуществляющую первичную установку справочно-ключевой информации, сформированной в центре управления защищенной сетью.
17. 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.

18. Иметь в своем составе ПО для осуществления защищенных почтовых услуг с возможностями аутентификации отправителя и получателя, квитирования (доставлено, прочитано), электронной подписи (далее – ЭП).
19. Иметь в своем составе ПО для реализации дополнительных сервисов: защищенный чат, защищенная конференция, защищенный обмен файлами.
20. Обеспечивать замкнутость среды функционирования ПК.
21. Автоматически обрабатывать обновления, полученные из ПК управления VPN-сетью.
22. Должен функционировать под управлением следующих ОС:

- Microsoft Windows 8.1 (32/64-разрядная);
- Microsoft Windows 10 (32/64-разрядная);
- Microsoft Windows Server 2012 (64-разрядная);
- Microsoft Windows Server 2012 R2 (64-разрядная);
- Microsoft Windows Server 2016 (64-разрядная);
- Astra Linux Special Edition «Смоленск»;
- Astra Linux Common Edition «Орел»;
- ГосЛинукс IC5;
- РЕД ОС 7.2;
- Альт Рабочая станция 8;
- Альт Рабочая станция 8 СП;
- Альт Рабочая станция 9;

- ЛОТОС (редакция для серверов и рабочих станций);
- РОСА «КОБАЛЬТ» (пользовательская редакция);
- EMIAS OS 1.0, Ubuntu 18.04.2 LTS;
- Debian 9.9;
- CentOS 7.1;
- CentOS 7.5;
- CentOS 8;
- ОС Android версий 6.x, 7.x, 8.x, 9.x, 10.x, 11.x, 12.x;
- iOS 12.4 и выше;
- iPadOS 13 и выше;
- macOS версии 10.15, 11, 12, 13.

23. Должен поддерживать работу в следующих виртуальных средах:

- Microsoft Hyper-V;
- VMWare Workstation;
- VMWare Player;
- VMWare vSphere ESXi.

24. Обеспечивать шифрование IP-трафика, файлов и почтовых сообщений в режиме гаммирования с обратной связью, а также имитозащита информации выполняются в соответствии с ГОСТ 28147-89.
25. Обеспечивать создание ЭП, проверку ЭП, создание ключей ЭП и ключей проверки ЭП осуществляются в соответствии с алгоритмом ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
26. ПК VPN-клиент должен реализовывать функции средства ЭП (создание ЭП, проверка ЭП, создание ключа ЭП, создание ключа проверки ЭП) согласно Федеральному закону от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
27. Должен соответствовать требованиям ФСБ России к устройствам типа межсетевые экраны по 4 классу защищённости.
28. Должен соответствовать требованиям ФСБ России к шифровальным (криптографическим) средствам по классу не ниже КС3

4.6.Требования к средствам управления политиками безопасности:

В качестве средства управления политиками безопасности (сетевыми фильтрами) VPN-узлов должен использоваться программный комплекс (далее – ПК управления политиками безопасности VPN-узлов), удовлетворяющий следующим требованиям:

1. ПК управления политиками безопасности VPN-узлов должен входить в состав защищенной VPN-сети.
2. ПК управления политиками безопасности VPN-узлов должен быть совместим с VPN-узлами.
3. ПК управления политиками безопасности VPN-узлов должен централизованно управлять политиками безопасности VPN-узлов.
4. ПК управления политиками безопасности VPN-узлов должен поддерживать прозрачную работу через различные NAT-устройства.

ПК управления политиками безопасности VPN-узлов должен выполнять следующие функции:

1. Работа (создание, редактирование, удаление) с группами (подразделениями, объединениями) защищенных узлов:

- VPN-узлов;
- IP-адресов;
- протоколов;
- интерфейсов;

- расписаний.

2. Работа (создание, редактирование, удаление) шаблонов политик безопасности.
3. Применение шаблона политики безопасности как на отдельный VPN-узел, так и на группу VPN-узлов.
4. Просмотр журнала отправки, получения и применения политик безопасности.
5. Online нотификация об отправке, получения и применения политик безопасности.
6. Управление учетными записями (создание, редактирование, удаление) пользователей.
7. Определение роли или ролей для учетных записей:

- управление пользователям;
- управление ролями пользователей;
- управление группами (подразделениями, объединениями и т.п.);
- управление шаблонами политик безопасности;
- назначение шаблонов политик безопасности;
- отправка политик безопасности;
- аудит.

8. Определение расписания действия шаблонов политик безопасности.
9. Работа (создание, редактирование, удаление) со следующими типами сетевых фильтров:

- локальные;
- транзитные;
- туннелируемые;
- защищенные;
- трансляция сетевых адресов.

10. Просмотр результирующей политики безопасности на VPN-узле или на группе VPN-узлов.

Сохранение и печать результирующей политики безопасности на VPN-узле или на группе VPN-узлов

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ

Выполнение работ в соответствии с настоящим Техническим заданием должно осуществляться поэтапно, включая следующие этапы:

Таблица № 2

№ этапа	Наименование Работ	Содержание Работ	Отчетные материалы	Сроки выполнения	Стоимость Этапа
1	Предоставление неисключительных прав (лицензий) на систему	Передача оборудования (ПАК) и предоставление неисключительных прав (лицензий) на ПО	-Акт приема-передачи оборудования; -Акт приема-передачи неисключительных прав (лицензий); - Лицензионное (Сублицензионное) соглашение;	14 рабочих дней с даты заключения договора	30 % от суммы контракта
2	Разработка проекта и актуализация эксплуатационной документации на систему	- Сбор исходных данных, необходимых для разработки и актуализации эксплуатационной документации на систему; - Разработка проекта и актуализация эксплуатационной документации на систему	Комплект документов: - Программа и методика предварительных испытаний системы; - Программа опытной эксплуатации системы;	24 рабочих дня с даты окончания этапа 1	10 % от суммы контракта

			- Программа и методика приемочных испытаний системы; - Руководство администратора системы; - Руководство по установке и настройке системы; - Процедуры аварийного восстановления - Руководство пользователя системы		
3	Пуско-наладочные работы системы	Проведение пуско-наладочных работ по установке и настройке системы на площадке Заказчика, указанной в п. 2	Комплект документов: - Акт выполненных работ по установке и настройке системы.	14 рабочих дней с даты окончания этапа 2	20% от суммы контракта
4	Проведение испытаний системы	- Проведение предварительных испытаний системы на площадке Заказчика, указанной в п. 2; - Проведение опытной эксплуатации системы на площадке Заказчика, указанной в п.2;	Комплект документов: - Протокол предварительных испытаний;	30 рабочих дней с даты окончания этапа 3	10 % от суммы контракта

		- Проведение приемочных испытаний системы на площадке Заказчика, указанной в п.2;	- Акт передачи в опытную эксплуатацию системы; - Журнал опытной эксплуатации - Отчет о проведении опытной эксплуатации системы; - Акт завершения опытной эксплуатации системы; - Протокол приемочных испытаний; - Проект Акта приемки системы в промышленную эксплуатацию;		
5	Оформление закрывающих документов	Выставление в адрес Заказчика закрывающих документов	Комплект документов: - Акт сдачи-приемки выполненных работ - Счет на оплату	14 рабочих дней с даты окончания этапа 5	30% от суммы контракта

5.1.Требования к проведению испытаний ПО СКЗИ.

Приемка работ по внедрению ПАК СКЗИ должна осуществляться на основании испытаний. Должны быть проведены следующие виды испытаний:
- предварительные испытания;
- опытная эксплуатация;
- приемочные испытания.

По результатам выполнения Работ Исполнитель должен предоставить отчетные документы, перечень которых приведен таблице 3 настоящего ТЗ.

5.2.Предварительные испытания.

Датой начала проведения предварительных испытаний ПАК СКЗИ должна быть дата, следующая после даты завершения пуско-наладочных работ ПАК СКЗИ. После завершения пуско-наладочных работ Заказчик назначает сроки проведения предварительных испытаний и направляет Исполнителю соответствующее уведомление.
Замечания, выявляемые в ходе проведения предварительных испытаний, должны фиксироваться участниками предварительных испытаний в Протоколе предварительных испытаний.
Участниками предварительных испытаний после выполнения, указанных в Программе и методике предварительных испытаний сценариев проверки, выставляется в Протоколе предварительных испытаний одна из оценок:
– «Принято»;
– «Принято с замечаниями»;
– «Не принято».

Предварительные испытания проводятся путем поочередного выполнения проверок, каждая из которых состоит из ряда действий. Состав и содержание проверок должны быть приведены в Программе и методике предварительных испытаний.
В случае если в Протоколе предварительных испытаний, есть сценарии с оценкой «Не принято», то предварительные испытания считаются не пройденными. В этом случае Исполнитель после завершения предварительных испытаний должен устранить все выявленные сбои, ошибки и недостатки, после чего уведомить Заказчика о готовности к проведению повторных предварительных испытаний.
Повторные предварительные испытания проводятся в объеме сценариев, получивших оценку «Не принято» в Протоколе предварительных испытаний. Повторные предварительные испытания осуществляются в порядке, описанном выше.
Предварительные испытания считаются завершенными не успешно в случае, если они проводились повторно более трех раз.
Предварительные испытания считаются завершенными успешно и обеспечена готовность ПАК СКЗИ к опытной эксплуатации, если Протокол предварительных испытаний не содержит оценки «Не принято».
По результатам проведения предварительных испытаний оформляется Протокол предварительных испытаний и согласовывается Исполнителем и Заказчиком.
После подписания Протокола предварительных испытаний Исполнитель должен передать Заказчику два подписанных экземпляра Акта приемки в опытную эксплуатацию. После чего Заказчик подписывает Акты и передает 1 (один) экземпляр Заказчику.
Датой завершения предварительных испытаний должна быть дата подписания Заказчиком Акта приемки в опытную эксплуатацию.

Во время проведения предварительных испытаний должны выполняться требования техники безопасности, противопожарной безопасности, промышленной санитарии и эргономики.

5.3.Опытная эксплуатация.

Датой начала проведения опытной эксплуатации ПАК СКЗИ должна быть дата, следующая после даты подписания Акта приемки в опытную эксплуатацию. После подписания Заказчиком и Исполнителем Акта приемки в опытную эксплуатацию Заказчик назначает сроки проведения опытной эксплуатации и направляет Исполнителю соответствующее уведомление.
Замечания, выявляемые в ходе проведения опытной эксплуатации, должны фиксироваться участниками опытной эксплуатации в Журнале опытной эксплуатации. В Журнал опытной эксплуатации заносят сведения о продолжительности функционирования, отказах, сбоях, аварийных ситуациях, изменениях параметров ПАК СКЗИ, проводимых корректировках в документации ПАК СКЗИ.
В случае успешного прохождения опытной эксплуатации, Исполнитель должен передать для подписания Заказчику подписанные Исполнителем 2 (два) экземпляра Акта завершения опытной эксплуатации. После чего Заказчик подписывает Акты и передает 1 (один) экземпляр Исполнителю. Датой завершения опытной эксплуатации должна быть дата подписания Заказчиком Акта завершения опытной эксплуатации.

5.4.Приемочные испытания.

Датой начала проведения приемочных испытаний ПАК СКЗИ должна быть дата, следующая после даты подписания Акта завершения опытной эксплуатации.
После подписания Заказчиком и Исполнителем Акта завершения опытной эксплуатации Заказчик назначает сроки проведения приемочных испытаний и направляет Исполнителю соответствующее уведомление.
Замечания, выявляемые в ходе проведения приемочных испытаний, должны фиксироваться участниками приемочных испытаний в Протоколе приемочных испытаний.
Участниками приемочных испытаний после выполнения, указанных в Программе и методике приемочных испытаний сценариев проверки, выставляется в Протоколе приемочных испытаний одна из оценок:
– «Принято»;
– «Принято с замечаниями»;
– «Не принято».
Приемочные испытания проводятся путем поочередного выполнения проверок, каждая из которых состоит из ряда действий. Состав и содержание проверок должны быть приведены в Программе и методике приемочных испытаний.
В случае если в Протоколе приемочных испытаний, есть сценарии с оценкой «Не принято», то приемочные испытания считаются не пройденными. В этом случае Исполнитель после завершения приемочных испытаний должен устранить все выявленные сбои, ошибки и недостатки, после чего уведомить Заказчика о готовности к проведению повторных приемочных испытаний. Повторные приемочные испытания проводятся в объеме сценариев, получивших оценку «Не принято» в Протоколе приемочных испытаний. Повторные приемочные испытания осуществляются в порядке, описанном

выше. Приемочные испытания считаются завершенными не успешно в случае, если они проводились повторно более 3 (трех) раз.
Приемочные испытания считаются завершенными успешно и ПАК СКЗИ готов к промышленной эксплуатации, если Протокол приемочных испытаний не содержит оценку «Не принято».
По результатам проведения приемочных испытаний оформляется Протокол приемочных испытаний и согласовывается Исполнителем и Заказчиком. После подписания Протокола приемочных испытаний Исполнитель должен передать Заказчику 2 (два) подписанных экземпляра Акта приемки в промышленную эксплуатацию. После чего Заказчик подписывает Акты и передает 1 (один) экземпляр Исполнителю.
Датой завершения приемочных испытаний должна быть дата подписания Заказчиком Акта приемки в промышленную эксплуатацию.
Во время проведения предварительных испытаний должны выполняться требования техники безопасности, противопожарной безопасности, промышленной санитарии и эргономики.

6. ТРЕБОВАНИЯ К ДОКУМЕНТАЦИИ

Перечень комплектов и видов документов, подлежащих разработке в рамках работ по внедрению Системы представлен в Таблице № 3. Требования к содержанию документов представлены в Приложении №2 к Техническому заданию.

Таблица № 3

№ п/п	Наименование отчетных документов	Требования к структуре, содержанию и оформлению документов
1.	Ведомость эксплуатационных документов	На бумажном носителе (1 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
2.	Общее описание системы ПАК СКЗИ	На бумажном носителе (1 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
3.	Программа и методика предварительных испытаний системы ПАК СКЗИ	На бумажном носителе (1 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
4.	Программа опытной эксплуатации системы ПАК СКЗИ	На бумажном носителе (2 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
5.	Программа и методика приемочных испытаний системы ПАК СКЗИ	На бумажном носителе (1 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
6.	Руководство администратора системы ПАК СКЗИ	На бумажном носителе (1 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
7.	Руководство по установке и настройке системы ПАК СКЗИ	На бумажном носителе (1 экз.) и в электронном виде (текстовая часть в

№ п/п	Наименование отчетных документов	Требования к структуре, содержанию и оформлению документов
		формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
8.	Принципиальная схема функционирования системы серверной виртуализации	На бумажном носителе (2 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
9.	Руководство пользователя системы ПАК СКЗИ	На бумажном носителе (2 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
10.	Протокол предварительных испытаний	На бумажном носителе (2 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
11.	Акт передачи в опытную эксплуатацию ПАК СКЗИ	На бумажном носителе (1 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
12.	Журнал опытной эксплуатации ПАК СКЗИ	На бумажном носителе (2 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
13.	Отчет о проведении опытной эксплуатации ПАК СКЗИ	На бумажном носителе (2 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
14.	Акт завершения опытной эксплуатации ПАК СКЗИ	На бумажном носителе (2 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*, графическая часть в формате Microsoft Visio*).
15.	Протокол приемочных испытаний ПАК СКЗИ	На бумажном носителе (2 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*)
16.	Проект Акта приемки ПАК СКЗИ в промышленную эксплуатацию	На бумажном носителе (2 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*)
17.	Акт сдачи-приемки выполненных работ	На бумажном носителе (2 экз.) и в электронном виде (текстовая часть в формате Microsoft Word*)

Вся разработанная документация должна быть выполнена на русском языке.

7. ПОРЯДОК ОПЛАТЫ

Оплата работ осуществляется на позднее 7 (семи) рабочих дней с даты приемки товаров и услуг в соответствии с этапами работ, указанными в п.5 Таблица 2 и Федеральным законом от 18 июля 2011 №223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»

Приложение №1
к Техническому заданию

Спецификация программного обеспечения

Артикул	Наименование	Количество
SC-31-KC3-4.X	Передача права на использование ПО ViPNet Administrator 4.x (KC3)	1
SC-31-KC3-4.X-T-G2	Сертификат активации сервиса прямой технической поддержки ПО ViPNet Administrator 4.x (KC3) на срок 1 год, уровень - Расширенный	1
SC-29-KC3-4.X	Передача права на использование ПО ViPNet Client for Windows 4.x (KC3)	205
SC-29-KC3-4.X-T-G2	Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client for Windows 4.x (KC3) на срок 1 год, уровень - Расширенный	205
SC-29-Client-4U-LIN-KC3	Передача права на использование ПО ViPNet Client 4U for Linux (KC3)	10
SC-29-Client-4U-LIN-KC3-T-G2	Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client 4U for Linux (KC3) на срок 1 год, уровень - Расширенный	10
SC-29-Client-2.X-MacOS	Передача права на использование ПО ViPNet Client for MacOS 2.x	1
SC-29-Client-2.X-MacOS-T-G2	Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client for MacOS 2.x на срок 1 год, уровень - Премиальный	1
SC-191-KC1-2.X	Передача права на использование ПО ViPNet Client for iOS 2.x (KC1)	24
SC-191-KC1-2.X-T-G2	Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client for iOS 2.x (KC1) на срок 1 год, уровень - Расширенный	24
SC-195-Client-4U-Andr-KC1	Передача права на использование ПО ViPNet Client 4U for Android (KC1)	32
SC-195-Client-4U-Andr-KC1-T-G2	Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client 4U for Android (KC1) на срок 1 год, уровень - Расширенный	32
SC-100-PM-4.X	Передача права на использование ПО ViPNet Policy Manager 4.x	1
SC-100-PM-4.X-T-G2	Сертификат активации сервиса прямой технической поддержки	1

	ПО ViPNet Policy Manager 4.x на срок 1 год, уровень - Расширенный	
HC-119-1000D-4.X	ПАК ViPNet Coordinator HW1000 D 4.x	2
HC-119-1000D-4.X-T-G2	Сертификат активации сервиса прямой технической поддержки ПАК ViPNet Coordinator HW1000 D 4.x на срок 1 год, уровень - Расширенный	2
USB Key	Аппаратный Ключ Аутентификации, имеющий специальную сертифицированную защиту как на аппаратном, так и на программном уровнях.	205

Общие требования к поставляемому ПО:

1. Срок предоставления ПО в течение 14 (Четырнадцати) рабочих дней с даты заключения Сторонами Договора.
2. Условия использования программного обеспечения должны предусматривать предоставление Сублицензиату права использования программного обеспечения способами, указанными в ст. 1280 Гражданского кодекса Российской Федерации с момента начала использования программного обеспечения Сублицензиатом и до момента продажи или иного отчуждения Сублицензиатом соответствующего оборудования или программного обеспечения. Сублицензиат должен быть освобождён от обязанности предоставлять Правообладателю и (или) Лицензиату, иным третьим лицам отчёты об использовании программного обеспечения.
3. Программное обеспечение должно быть поставлено в наименовании, в количестве и в сроки, предусмотренные Договором.

Приложение № 2
к Техническому заданию

Требования к содержанию документов

Наименование документов	Содержание документа
Общее описание системы	Должно содержать следующую информацию: назначение ПАК СКЗИ; описание ПАК СКЗИ; описание взаимосвязей ПАК СКЗИ с другими системами;
Программа и методика испытаний	Должна содержать по каждой функции/операции Системы следующую информацию: • тестируемая функция; • действия пользователей; • реакция ПАК СКЗИ; • пояснения Исполнителя. • Также программа определяет сроки тестирования, содержит форму протокола испытаний ПАК СКЗИ
Руководство пользователя	Руководство пользователей (отдельное для каждой роли) должно включать следующую информацию: • для кого написано руководство; • инициирующие события (какие документы, изображения и (или) события являются основанием для начала действия пользователя); • путь к необходимой информации или форме (пункт меню в интерфейсе пользователя); • краткий перечень действий пользователя (для напоминания пользователю); • описание действий пользователя с заполнением обязательных полей и указанием критериев выбора значений в каждом поле; • другая информация. В руководствах могут быть приведены снимки экранных форм ПАК СКЗИ.
Руководство администратора	Руководство администратора должно включать следующую информацию: для кого написано руководство (роль); подключение нового пользователя (инструкция по подключению типовых рабочих мест); обслуживание ПАК (необходимые регламентные операции системы); операции администрирования системы; описание процедуры резервного копирования; инструкция по установке, удалению и обновлению ПАК СКЗИ. В руководствах должны быть приведены снимки экранных форм ПАК СКЗИ.
Процедуры аварийного восстановления работы системы.	Пошаговое руководство восстановления работы всей системы при выходе из строя как ПАК, так и ПО.