

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Услуги по эксплуатационно-техническому обслуживанию серверного оборудования и подсистемы обеспечения информационной безопасности аппаратно-программного комплекса «Безопасный город»

Перечень используемых определений и сокращений

Перечни используемых в настоящем документе сокращений и определений представлены в Таблице № 1 и Таблице № 2 соответственно.

Таблица № 1. Перечень сокращений

АПК Аппаратно-программный комплекс

АРМ Автоматизированное рабочее место

ЕДДС Единая дежурно-диспетчерская служба муниципального образования

АСО ЛВС Активное сетевое оборудование локальной вычислительной сети

ВМ Виртуальная машина

ИБП Источник бесперебойного питания

КТС Комплекс технических средств

КСА Комплекс средств автоматизации

МО Муниципальное образование

МСК Московское время

ОПО Общее программное обеспечение

ОС Операционная система

ЦОД Центр обработки данных

ОПО Общее программное обеспечение

ПО Программное обеспечение

СПД Сеть передачи данных

СПО Специализированное программное обеспечение

СТП Служба технической поддержки Исполнителя – подразделение Исполнителя, осуществляющее выполнение работ по обеспечению исполнения условий Договора

СХД Система хранения данных

ЗИП Запасные части, инструменты и принадлежности

ТЗ Техническое задание

Запрос Официальное письмо

НСД Несанкционированный доступ

ПОИБ Подсистема обеспечения информационной безопасности

СрЗИ Средства защиты информации

УИВ Участник информационного взаимодействия АПК «Безопасный город»

ФСБ России Федеральная служба безопасности Российской Федерации

ФСТЭК России Федеральная служба по техническому и экспортному контролю

Таблица № 2. Перечень определений

Гарантийный ремонт Ремонт, выполняемый в авторизованном сервисном центре производителя оборудования или осуществляемый поставщиком оборудования в

соответствии с условиями гарантии на оборудование

Заказчик Лицо, заинтересованное в выполнении исполнителем работ, оказании им

услуг или приобретении у продавца какого-либо продукта

Заявка Обращение Пользователя в техническую поддержку Исполнителя

Исполнитель Лицо (физическое или юридическое), подрядившееся выполнить для

Заказчика определенную работу или оказать услуги к оговоренному сроку за определенную оплату

Виртуальный

сервер Программная эмуляция физического сервера

КТС Оборудование, перечисленное в п. 4.5 к ТТ

Инцидент Событие, связанное с невозможностью использования обслуживаемого компонента по его назначению согласно документации, либо с функционированием обслуживаемого компонента в режиме, отличном от штатного согласно эксплуатационной документации

Компонент Целостная составная часть Инфраструктуры, включающая оборудование, его комплектующие и ОПО, конструктивно входящие в оборудование.

Видеокамеры и рабочие места не относятся к компонентам

Обращение Обращение пользователя в СТП по вопросам, связанным с оказанием Услуг

Операция Действие, которое необходимо выполнить в рамках оказания Услуги

Представитель

Заказчика Ответственное лицо со стороны Заказчика

Решение запроса Предоставление Заказчику исчерпывающих рекомендаций (инструкций) по

решению задач, описанных в Запросе

Решение инцидента Выработка любого временного или постоянного решения, позволяющего восстановить работоспособность обслуживаемого компонента или

восстановить возможность его использования по назначению

Соглашение Соглашение об уровне качества Услуг (Приложение 3 к ТЗ)

Уровень обслуживания Совокупность требований к обслуживанию Инфраструктуры, определяющих выполнение Исполнителем принятых на себя обязательств в соответствии с

Договором

Сроки оказания услуг: с 27.04.2026 по 31.12.2026 г.

Место оказания услуг: г. Брянск, ул. Бондаренко, д. 8.

4. Требования к Исполнителю:

4.1. Наличие у Исполнителя действующей лицензии ФСБ РФ на осуществление разработки, производства, распространения 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 пунктом 1 части 1 статьи 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» с указанием как минимум следующих выполняемых работ и оказываемых услуг, предусмотренных Перечнем выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющимся приложением к Положению, утвержденному Постановлением Правительства Российской Федерации от 16.04.2012 г. N 313:

Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем (пункт 13 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному Постановлением Правительства Российской Федерации от 16.04.2012 г. N 313);

4.2. Наличие у Исполнителя действующей лицензии на деятельность по технической защите конфиденциальной информации, в части работ, предусмотренных подпунктом «б» части 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого Постановлением Правительства РФ от 3.02.2012 № 79, в соответствии с пунктом 5 части 1 статьи 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» и Постановлением Правительства РФ от 3.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»);

4.3. Наличие у Исполнителя действующей лицензии Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации в соответствии с пунктом 5 части 1 статьи 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», распространяющейся как минимум на следующие виды работ и услуг, предусмотренные Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным Постановлением Правительства РФ от 03.02.2012 № 79:

Услуги по установке, монтажу, наладке, испытаниям, ремонту 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 эффективности защиты информации) (подпункт «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного Постановлением Правительства РФ от 03.02.2012 № 79);

4.4. Исполнитель должен являться аккредитованным центром государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА). Участником предоставляется информация, подтверждающая факт аккредитации Национальным координационным центром по компьютерным инцидентам (копия документа о сотрудничестве (взаимодействии) в области обнаружения, предупреждения и ликвидации последствий компьютерных атак с Федеральной службой безопасности Российской Федерации (Национальным координационным центром по компьютерным инцидентам) или предоставляется информация о записи на официальном сайте с перечнем центров ГосСОПКА).

4.5. Наличие у Исполнителя сертификатов, действующих весь период проведения технического обслуживания:

- Сертификаты СРК КиберБэкап;
- Сертификаты СХД QSAN;
- Сертификаты АСО ЛВС ELTEX.

5. Требования к объему и содержанию услуг:

Объем услуг:

Исполнитель должен:

оказать услуги по эксплуатационно-техническому обслуживанию серверного оборудования аппаратно-программного комплекса «Безопасный город» в соответствии с Приложением №1 настоящего ТЗ;

оказать услуги по эксплуатационно-техническому обслуживанию подсистемы обеспечения информационной безопасности аппаратно-программного комплекса «Безопасный город» в соответствии с Приложением №2 ТЗ.

5.2 Способ предоставления услуги:

Услуга по эксплуатационно-техническому обслуживанию серверного оборудования и подсистемы обеспечения информационной безопасности аппаратно-программного комплекса «Безопасный город» на территории Брянской области оказывается преимущественно посредством удаленного доступа.

Цель оказания услуг: Целью оказания Услуг является обеспечение бесперебойного функционирования элементов КТС аппаратно-программного комплекса «Безопасный город» на территории Брянской области, предназначенной для решения комплекса задач обеспечения общественной безопасности и правопорядка посредством своевременной идентификации и реагирования на

потенциальные угрозы общественной безопасности и нарушений правопорядка, а также подсистемы обеспечения информационной безопасности.

Достижение цели обеспечивается решением следующих задач Исполнителем:

- осуществление технической поддержки КТС, с целью обеспечения бесперебойного функционирования аппаратно-программного комплекса «Безопасный город» на территории Брянской области;
- осуществление технической поддержки средств защиты информации с целью обеспечения бесперебойного функционирования вычислительной инфраструктуры;
- обеспечение непрерывности процессов сбора, обработки и хранения информации в КТС АПК «Безопасный город» на территории Брянской области;
- обеспечение мониторинга работоспособности серверного оборудования;
- осуществление технической поддержки подсистемы обеспечения информационной безопасности, с целью обеспечения бесперебойной работы серверного оборудования, сервисов СПО, сетевой связанности компонентов Системы между собой;
- оказание консультаций Пользователям.

СОСТАВ ДОКУМЕНТАЦИИ

В состав комплекта документации на КТС АПК «Безопасный город» входят документы, список которых приведён в Таблице № 3.

Таблица № 3 Список документации

№п/п	Документ	Способ передачи документов
1	Сетевые имена компонентов КТС АПК «Безопасный город»	нарочно
2	Перечень QR - кодов оборудования (инвентарные номера)	нарочно
3	Реестр оборудования КТС АПК «Безопасный город»	нарочно

Заказчик в течение 5 (Пяти) рабочих дней с даты получения запроса от Исполнителя направляет Исполнителю официальное письмо с запрашиваемыми документами, список которых приведён в Таблице № 3.

5.5. Общие требования к порядку оказанию Услуг

Оказание Услуг должно осуществляться в соответствии со следующими Приложениями к ТЗ:

Приложение №1: «Требования по оказанию услуг сопровождения серверного оборудования аппаратно-программного комплекса «Безопасный город»;

Приложение №2: «Требования по оказанию услуг сопровождения подсистемы обеспечения информационной безопасности аппаратно-программного комплекса «Безопасный город»

Приложение № 3: «Соглашение об уровне качества Услуг»;

Приложение № 4: «Регламент оказания Услуг»;

Приложение № 5: «Регламент мониторинга компонентов КТС»;

Приложение № 6: «Регламент обработки обращений в СУТП и консультаций пользователей»;

Приложение № 7: «Данные о сотрудниках Исполнителя для предоставления доступа к местам оказания Услуг»

Исполнитель в течение 3 (Трёх) рабочих дней с даты заключения Договора направляет Заказчику официальным письмом сведения о сотрудниках Исполнителя для предоставления им доступа к местам оказания Услуг по форме Приложения № 7 к ТЗ;

Для оказания Услуг Заказчик в течение 2 (Двух) рабочих дней с даты получения от Исполнителя информации обеспечивает Исполнителю доступ к оборудованию КТС АПК «Безопасный город».

В течение 10 (Десяти) рабочих дней с даты заключения Договора Исполнитель обязан организовать за свой счет и своими силами удаленный доступ к обслуживаемому оборудованию КТС, по схеме, согласованной с заказчиком, посредством подключения к сети VipNet.

Криптографическая защита передаваемых данных по каналу связи должна осуществляться в соответствии с ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры».

Средства криптографической защиты, используемые для защиты канала связи, должны быть сертифицированы ФСБ России.

Перечень оказываемых Услуг

В состав оказываемых Услуг по поддержанию в исправном состоянии элементов оборудования комплекса технических средств и подсистемы обеспечения информационной безопасности АПК «Безопасный город» должны входить виды Услуг, список которых приведён в Таблице № 4.

Таблица № 4. Перечень Услуг

№ п/п	Перечень Услуг	Периодичность оказания Услуг	Требования
1.	Обработка обращений пользователей КТС	По запросу;	В соответствии с Регламентом (Приложение №4) и в соответствии с таблицей 5, таблицей 6 Приложения №1; Приложение № 1, №4 к ТЗ;
2.	Восстановление работоспособности компонентов КТС при возникновении Инцидентов	По запросу;	По результатам мониторинга в соответствии с Регламентом мониторинга компонентов (Приложение №5); В соответствии с Приложением № 1 к ТЗ и в соответствии с таблицей 5, таблицей 6; Приложение № 1, №5 к ТЗ;
3.	Регламентное обслуживание компонентов КТС	В соответствии с	Регламентом (Приложение №4) и в соответствии с таблицей 5, 6 Приложения №1; Приложение №1, №4 к ТЗ;
4.	Мониторинг доступности и производительности компонентов КТС	Периодически	в соответствии с Регламентом мониторинга компонентов КТС (Приложение №5); В соответствии с Приложением № 1 к ТЗ и в соответствии с таблицей 4.2; Приложение №1, №5 к ТЗ;
5.	Обработка обращений пользователей ПОИБ	По запросу;	

В соответствии с Регламентом (Приложение №4) в соответствии с Приложением №2 Приложение №2, №4 к ТЗ;

6. Восстановление работоспособности компонентов КТС при возникновении Инцидентов По запросу;

По результатам мониторинга в соответствии с Регламентом мониторинга компонентов (Приложение №5);

В соответствии с Приложением № 2 к ТЗ. Приложение № 2, №5 к ТЗ;

7. Регламентное обслуживание компонентов КТС В соответствии с Регламентом (Приложение №4) и в соответствии с Приложением №2; Приложение №2, №4 к ТЗ;

8. Мониторинг доступности и производительности компонентов КТС Периодически в соответствии с Регламентом мониторинга компонентов КТС (Приложение №5);

В соответствии с Приложением № 2 к ТЗ. Приложение №2, №5 к ТЗ;

10 Поддержание средств защиты информации актуальной версии и в работоспособном состоянии По запросу;

В соответствии с Регламентом (Приложение №4) в соответствии с Приложением №2 Приложение №2, №4 к ТЗ;

Требования к конфиденциальности

В соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» Исполнитель обязан:

- обеспечить конфиденциальность сведений, касающихся предмета Договора, ходе его исполнения, полученных результатов, а также сведений ограниченного доступа, которые могут стать ему известны в ходе исполнения Договора (далее – конфиденциальная информация) в течение 2 лет с даты заключения Договора;

- использовать доступ к информационным ресурсам Заказчика только в целях оказания Услуг, не копировать, не размножать и не распространять в любой форме любые материалы, содержащиеся на рабочих местах, серверах и прочих средствах хранения информации Заказчика без предварительного письменного разрешения Заказчика;

- принять все необходимые меры для защиты конфиденциальной информации;

- не передавать конфиденциальную информацию третьим лицам без предварительного письменного разрешения Заказчика.

ТРЕБОВАНИЯ ПО ОКАЗАНИЮ УСЛУГ ТЕХНИЧЕСКОГО СОПРОВОЖДЕНИЯ СЕРВЕРНОГО ОБОРУДОВАНИЯ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА «БЕЗОПАСНЫЙ ГОРОД»

Место оказания услуги: ЦОД КТС АПК «Безопасный город» Брянской области, расположенный по адресу: Брянская область, г. Брянск, ул. Бондаренко, д.8.

• Назначение Системы

Комплекс технических средств АПК «Безопасный город» Брянской области предназначен для решения комплексных задач в части обеспечения общественной безопасности, правопорядка и безопасности среды обитания за счет существенного улучшения координации деятельности сил и служб, ответственных за решение этих задач, путем внедрения комплексной информационной системы, обеспечивающей прогнозирование, мониторинг, предупреждение и ликвидацию возможных угроз, а также контроль устранения последствий чрезвычайных ситуаций и правонарушений с интеграцией под ее управлением действий информационно-управляющих подсистем дежурных, диспетчерских, муниципальных служб для их оперативного взаимодействия.

КТС АПК «Безопасный город» Брянской области предназначен для обеспечения:

- комплексной обработки оперативной информации о чрезвычайных ситуациях и информационного обмена между различными подсистемами и звеньями РСЧС, передачи органами повседневного управления необходимых указаний силам и средствам ликвидации чрезвычайных ситуаций;

- мониторинга места нахождения транспортных средств;

- мониторинга состояния окружающей среды;

- автоматизированного контроля радиационной обстановки и метеопараметров;

- мониторинга пожароопасной обстановки, визуальный контроль обстановки на территории Брянской области;

- видеонаблюдения в местах массового скопления и проживания людей, а также на социально значимых объектах инфраструктуры Брянской области;

- процессов сбора и обработки видеoinформации;

- поиска и розыска транспортных средств на основании данных фотовидеофиксации;

- хранения видеoinформации с камер видеонаблюдения, расположенных на территории Брянской области;

- доступа уполномоченных лиц и ведомств к сохраненной информации

• Сведения об оборудовании и сервисах, входящих в состав комплекса технических средств АПК «Безопасный город»

Количественные характеристики существующего комплекса технических средств и сервисов АПК «Безопасный город» приведены в Таблицах №5, №6.

Таблица №5 Количественные характеристики существующего комплекса технических средств АПК «Безопасный город» Брянской области

№ п/п	Наименование Комплекса	Наименование технических средств	Наименование компонента	кол-во имеющегося оборудования
1	Комплекс технических средств АПК «Безопасный город»	Технические средства АПК «Безопасный город»	Гипервизоры	23
2			Выделенные серверы	19
3			Виртуальные машины	121
4			СХД	5
5			Коммутаторы MLAG	8
6			Коммутаторы Stack NSF	4
7			Межсетевой экран	2
8			ИБП	6

Таблица №6 Сведения о техническом обеспечении комплекса технических средств

№ п/п	Функциональное назначение	Наименование оборудования	Количество	Гарантия
1.	Гипервизоры	SYS-1029U-TRTP2	23	нет
2.	Выделенные серверы	Supermicro SYS-1029P-WTR, Гравитон C2101И	19	нет
3.	Виртуальные машины		121	нет
4.	СХД	XN8024-D	2	нет
		XCubeSAN XS5226-D, XCubeSAN XS5212-D	3	нет
5.	Коммутаторы MLAG	MES3324, MES3348	8	нет
6.	Коммутаторы Stack NSF	MES5448	4	нет
7.	Межсетевой экран	МСЭ DIONIS 5000	2	нет
8.	ИБП	СИП380А10КД.9-33/БПССК05	6	нет

- Порядок регламентного обслуживания компонентов КТС АПК «Безопасный город»

Регламентное обслуживание компонентов КТС АПК «Безопасный город» осуществляется в соответствии с требованиями Таблицы №7 Приложения №1.

Таблица № 7. Порядок обслуживания компонентов КТС

№№ п/п	Типы операций	Периодичность	Отчет по работам
1.	Регламентное обслуживание компонентов КТС	В соответствии с установленными требованиями (Таблица № 13 Приложения №3)	По факту возникновения инцидента занесение инцидента в журнал

В рамках оказания услуги по регламентному обслуживанию компонентов КТС АПК «Безопасный город» Исполнитель должен выполнять установленный перечень операций (Таблица №8 Приложения №1).

Таблица №8. Перечень операций по регламентному обслуживанию компонентов КТС АПК «Безопасный город»

Обеспечивающие системы			
№	Подсистема	Проверка	Периодичность
1	AD/DNS	проверка синхронизации PDC/SDC	Ежемесячно
		проверка получения DNS внешние ресурсы PDC/SDC	Ежемесячно
		проверка синхронизации NTP PDC/SDC	Ежемесячно
2	Мониторинг (ЦОД)	проверка истории сработок/проблем	Ежедневно
		проверка проблем в работе КТС ЦОД	Ежедневно
		проверка проблем в работе гостевых ОС и выделенных серверов	Ежедневно
		проверка проблем в работе Подсистемы Виртуализации	Ежедневно
		проверка параметров работы оборудования	Еженедельно
		проверка параметров работы ВМ и выделенных серверов	Еженедельно
		проверка состояния и нагрузки на каналы связи	Еженедельно
3	СРК	проверка отработки вакуума СУБД системы Мониторинга	Еженедельно
		проверка работоспособности и ошибок подсистемы мониторинга и его компонент	Еженедельно
		проверка ошибок резервного копирования (еженедельные копии)	Еженедельно
4	Виртуализация	проверка ошибок резервного копирования (ежемесячные копии)	Ежемесячно
		проверка состояния агентов резервного копирования	Еженедельно
		проверка состояния и объемов хранилищ Резервных копий	Еженедельно
4	Виртуализация	проверка состояния узлов виртуализации	Еженедельно
		проверка состояния кластеров	Еженедельно
		проверка состояния кластерных и локальных хранилищ	Еженедельно
		проверка состояния виртуальных коммутаторов и сетей	Еженедельно
		проверка состояния/работоспособности НА	Еженедельно
		проверка журналов событий	Еженедельно
Комплекс технических средств			
№	Подсистема	Проверка	Периодичность
1	СХД	проверка ошибок	Еженедельно
		проверка логов событий	Еженедельно
		проверка консистентности Pool/Lun	Еженедельно
		проверка наличия дисков HS	Еженедельно
		проверка журналов доступа	Еженедельно
2	АСО ЛВС	проверка ошибок	Еженедельно
		проверка логов событий	Еженедельно
		проверка состояния основных компонент	Еженедельно
3	Серверы	выполнение резервной копии	Еженедельно
		проверка ошибок	Еженедельно
		проверка логов событий	Еженедельно

		проверка состояния основных компонент	Еженедельно
		проверка журналов доступа	Еженедельно
		проверка ошибок	Еженедельно
		проверка логов событий	Еженедельно
4	ИБП	проверка характеристик входного и выходного напряжения	Еженедельно
		проверка состояния батарейных модулей (при наличии такой возможности)	Еженедельно
		проверка журналов доступа	Еженедельно

Приложение № 2

ТРЕБОВАНИЯ ПО ОКАЗАНИЮ УСЛУГ ТЕХНИЧЕСКОГО СОПРОВОЖДЕНИЯ ПОДСИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА «БЕЗОПАСНЫЙ ГОРОД»

Место оказания услуги: Брянская область, г. Брянск, ул. Бондаренко, д.8.

Назначение ПОИБ: Подсистема обеспечения информационной безопасности предназначена для бесперебойного функционирования КТС АПК «Безопасный город» с учетом существующих угроз информационной безопасности.

Состав технических средств подсистемы обеспечения информационной безопасности: В составе АПК «Безопасный город» функционируют 27 объектов информатизации, на которых развернуто 42 автоматизированных рабочих места и 43 сервера.

Объектами информатизации являются ЦОД (комплекс средств автоматизации «Региональная платформа», система мониторинга окружающей среды, система мониторинга транспортных средств, система видеонаблюдения) и 26 участников информационного взаимодействия АПК «Безопасный город» на территории Брянской области.

Перечень УИВ, а также подробный перечень используемых СрЗИ ПОИБ АПК «Безопасный город» предоставляется Исполнителю Заказчиком по письменному запросу.

1. Требования к контролю параметров обслуживаемого оборудования и ПО

а. Мониторинг оборудования узлов доступа и программного обеспечения

Исполнитель осуществляет мониторинг параметров оборудования и ПО, используя имеющиеся средства Заказчика (ViPNet IDS NS2000, ViPNet IDS HS, ViPNet TIAS) в соответствии с параметрами, приведенными в таблице №9.

Таблица №9

Объект контроля	Контролируемый параметр
1	2
ЦОД (КСА «Региональная платформа»), г. Брянск, улица Бондаренко, дом 8	
Криптомаршрутизатор ViPNet Coordinator HW1000D 4.x	1. доступность сетевых интерфейсов
	2. состояние кластера
	3. журнал сетевых пакетов
	4. журнал событий
Криптомаршрутизатор ViPNet Coordinator HW5000 4.x	5. доступность сетевых интерфейсов
	6. состояние кластера
	7. журнал сетевых пакетов
	8. журнал событий
Система обнаружения вторжений ViPNet IDS NS2000 3.x	9. доступность сетевых интерфейсов
	10. актуальность баз решающих правил
	11. атаки среднего и высокого уровня
	12. журнал диагностики устройства
	13. журнал событий
Средство обнаружения угроз и расследования сетевых инцидентов ViPNet TIAS 2000 3.x	14. доступность сетевых интерфейсов
	15. актуальность баз решающих правил
	16. атаки среднего и высокого уровня
	17. журнал диагностики устройства
	18. журнал событий
Система обнаружения вторжений уровня хоста ПО COB ViPNet IDS HS 1.x	19. актуальность баз решающих правил
	20. атаки среднего и высокого уровня
	21. журнал диагностики устройства
	22. журнал событий
ПО ViPNet Administrator (Центр управления	23. доступность узла

сетью и удостоверяющий и ключевой центр)	24.	журнал событий
ПО ViPNet Client for Windows 4 (КСЗ)	25.	доступность узла
	26.	журнал событий
ПО ViPNet Client 4U for Android (КС1)	27.	доступность узла
	28.	журнал событий
ПО ViPNet Policy Manager 4.x	29.	доступность узла
	30.	журнал событий
ПАК Dionis DPS-5000	31.	доступность сетевых интерфейсов
	32.	состояние кластера
	33.	журнал сетевых пакетов
	34.	журнал событий
ПО СЗИ Secret Net Studio	35.	доступность узла
	36.	журнал событий
ПО СЗИ Secret Net Studio LSP	37.	доступность узла
	38.	журнал событий
ПАК "Соболь" Версия 3.2, PCI-E, серт. ФСБ	39.	доступность узла
	40.	журнал событий
ПАК "Соболь" Версия 4, PCI-E, серт. ФСТЭК	41.	доступность узла
	42.	журнал событий
ПАК "Соболь" Версия 4, M2, серт. ФСТЭК и ФСБ	43.	доступность узла
	44.	журнал событий
СДЗ Dallas Lock, M2, серт. ФСТЭК	45.	доступность узла
	46.	журнал событий
ПО Kaspersky Endpoint Security для бизнеса Стандартный	47.	журнал событий
ПО RedCheck, редакция Professional	48.	журнал событий
Узлы УИВ (участников информационного взаимодействия)		
Криптомаршрутизатор ViPNet Coordinator HW1000D 4.x	49.	доступность сетевых интерфейсов
	50.	журнал сетевых пакетов
	51.	журнал событий
Криптомаршрутизатор ViPNet Coordinator HW100 С 4.x	52.	доступность сетевых интерфейсов
	53.	журнал сетевых пакетов
	54.	журнал событий
ПАК "Соболь" Версия 4, PCI-E, серт. ФСТЭК	55.	доступность узла
	56.	журнал событий
ПО СЗИ Secret Net Studio	57.	доступность узла
	58.	журнал событий

В случае обнаружения инцидента или риска его возникновения, Исполнитель информирует Заказчика об обнаруженной проблеме и приступает к её устранению в соответствии с регламентом оказания услуг (Приложение 6 к Описанию объекта закупки).

в. Требования к сопровождению жизненного цикла оборудования и программного обеспечения

В процессе оказания услуг Исполнитель обеспечивает поддержку актуальности программного обеспечения средств защиты информации. Необходимые лицензии для получения доступа к соответствующему программному обеспечению предоставляются Заказчиком.

Поддержка актуальности включает в себя следующие мероприятия:

1. настройка, корректировка правил, предоставление доступа – по заявкам Заказчика;
2. обновление прошивок и микропрограмм – по мере выхода обновлений соответствующего программного обеспечения и по согласованию с Заказчиком;
3. обновление сигнатур атак, антивирусных баз – по мере выхода соответствующих обновлений;
4. диагностика отказов средств защиты информации;
5. устранение нестабильностей в работе средств защиты информации;

6. резервное копирование конфигураций оборудования и программного обеспечения средств защиты информации – согласно рабочему регламенту (регламент резервного копирования предоставляется Заказчиком).

2. Требования к документированию

Все работы по техническому обслуживанию средств защиты информации, входящих в состав ПОИБ АПК «Безопасный город» должны быть регламентированы и документированы Исполнителем.

Исполнитель должен поддерживать в актуальном состоянии документацию, переданную ему Заказчиком.

3. Требования к составу услуг, проводимому в рамках обслуживания

Ниже указан минимальный состав услуг, которые должны быть оказаны Исполнителем в соответствии с требованиями настоящего Описания объекта закупки. Данный перечень услуг может быть расширен по согласованию между Заказчиком и Исполнителем.

а. Мероприятия общего плана

1 Обследование АПК «Безопасный город» в части используемых средств и систем обеспечения информационной безопасности, документирование текущей информации о состоянии СЗИ и СКЗИ, формирование предложений по оптимизации настроек и конфигурации, формирование предложений по унификации используемых средств защиты информации.

2 Поддержание существующей эксплуатационной документации в актуальном состоянии, внесение изменений при добавлении нового оборудования или программного обеспечения в состав обслуживаемой подсистемы. Эксплуатационная документация предоставляется Заказчиком.

3 Формирование предложений по модернизации обслуживаемой ПОИБ в случае изменения требований законодательства или контролирующих органов. Данные предложения могут быть оформлены как в виде отдельного уведомления в произвольной форме.

4 Взаимодействие с подрядчиками в случае необходимости взаимодействия обслуживаемой подсистемы с иными информационными системами.

б. Мероприятия, проводимые в штатном режиме эксплуатации

1. Корректировка настроек обслуживаемых средств защиты информации в случае такой необходимости, взаимодействие с представителями иных обслуживающих (или проводящих работы на обслуживаемом объекте) организаций.

2. Формирование и поддержание в актуальном состоянии правил межсетевого экранирования как в отношении отдельных узлов, так и в отношении обслуживаемой системы защиты в целом.

3. Плановая и внеплановая смена ключевого материала на обслуживаемых СКЗИ.

4. Генерация ключевых дистрибутивов для новых узлов СКЗИ, задание необходимых связей между узлами.

5. Учет СКЗИ в журналах Заказчика.

6. Установка и поддержание межсетевого взаимодействия с другими сетями ViPNet.

7. Периодическое тестирование работоспособности используемых СЗИ и СКЗИ.

8. Периодическая оценка защищенности информационных ресурсов, защищаемых обслуживаемой подсистемой ИБ.

9. Периодическое обновление баз решающие правил используемых средств обнаружения вторжений.

10. Постоянный контроль состояния обслуживаемых узлов, формирование превентивных мероприятий по предотвращению перехода системы в аварийный режим.

11. Информирование Заказчика и его представителей о состоянии обслуживаемой системы.

12. Консультации представителей Заказчика по вопросам эксплуатации применяемых средств защиты информации.

с. Мероприятия, проводимые в аварийном режиме эксплуатации

– Настройка и установка резервного оборудования в случае выхода из строя, на время диагностики или ремонта основного оборудования.

– Формирование и применение необходимых настроек обслуживаемых СЗИ и СКЗИ для локализации аварийного участка системы, восстановление штатного режима работы системы защиты.

– Информирование ответственных лиц Заказчика в случае возникновения инцидентов информационной безопасности, принятие мер, направленных на ликвидацию выявленного инцидента.

– Активное участие в расследовании инцидентов, связанных с информационной

безопасностью в обслуживаемой системе.

6. Требования к мониторингу информационной безопасности

Для организации услуг по мониторингу событий информационной безопасности и локализации инцидентов информационной безопасности на объектах ПОИБ АПК БГ, используются средства обнаружения вторжений и анализа событий информационной безопасности. В рамках данных требований Исполнителем должны быть оказаны следующие услуги:

6.1. Эксплуатация технических средств обнаружения вторжений и средств анализа событий и выявления инцидентов:

- выявление ошибок в технических средствах (передача информации разработчику);
- настройку средства обнаружения вторжений и анализа событий информационной безопасности на отправку событий информационной безопасности;
- подключение средств обнаружения вторжений, имеющихся у Заказчика, к механизму автоматического обновления баз решающих правил;
- направление в НКЦКИ предложений по совершенствованию указанных средств.

6.2. Анализ событий информационной безопасности:

- анализ событий информационной безопасности, поступающих от различных источников.

6.3. Регистрация компьютерных инцидентов и атак:

- регистрация инцидента/подозрения на инцидент путём создания заявки на его обработку (карточки инцидента);
- предоставление первичных рекомендаций Заказчику по ликвидации последствий инцидента.

6.4. Прием обращений о возможных инцидентах:

- приём обращений о возможных компьютерных инцидентах с использованием средств взаимодействия с персоналом и пользователями информационных систем.

6.5. Взаимодействие с группой реагирования Заказчика:

- предоставление рекомендаций Заказчику по реагированию и расследование причин возникновения инцидентов.

6.6. Инвентаризация информационных ресурсов:

- не реже одного раза в ходе исполнения Договора с помощью программно-технических средств, установленных у Заказчика;
- не реже одного раза в ходе исполнения Договора с помощью сертифицированных программно-технических средств, установленных у Заказчика.

6.7. Аудит защищенности информационных ресурсов:

- не реже одного раза в ходе исполнения Договора проверка защищённости внешнего периметра от внешнего нарушителя, которая включает в себя: сбор информации; поиск уязвимостей (недостатков) сетевых сервисов, ОС, конфигураций оборудования; разработка рекомендаций по устранению выявленных уязвимостей (недостатков);
- не реже одного раза в ходе исполнения Договора: изучение топологии сети; поиск внутренних веб-интерфейсов; анализ антивирусной защиты и настроек безопасности; анализ доступов; анализ логирования действий; анализ учетных записей; анализ политики паролей; сканирование портов внутренних IP-адресов.

6.8. Информационное взаимодействие с системой ГосСОПКА:

- взаимодействие с НКЦКИ;
- предоставление сведений о состоянии защищённости информационных ресурсов;
- предоставление сведений о компьютерных инцидентах;
- предоставление Заказчику бюллетеней ИБ (информации об угрозах и трендах).

6.9. Подготовка и предоставление аналитических данных:

- предоставление отчетов по выявленным инцидентам;
- предоставление ежемесячных отчетов, включая информацию по статистике собранных событий, о типах зарегистрированных инцидентов (подозрений на инциденты) ИБ, о статусах выявленных инцидентов ИБ и мерах обработки (реагирования);
- формирование предложений по повышению уровня защищенности информационных ресурсов.

Приложение № 3

СОГЛАШЕНИЕ ОБ УРОВНЕ КАЧЕСТВА УСЛУГ

Термины и сокращения

Термины и сокращения, используемые в настоящем документе (далее – Соглашение) приведены в Таблице №10. Иные термины и сокращения установлены Договором и ТЗ.

Таблица №10. Перечень терминов и сокращений

Термин	Определение
Время реакции на обращение (время реакции)	Период времени от момента регистрации обращения до наступления одного из следующих событий: принятия заявки в работу и подтверждения типа обращения; запрос дополнительной информации по обращению у заявителя. Время реакции соответствует периоду времени от присвоения заявке статуса «Зарегистрировано» до присвоения статуса «В работе»
Время регистрации обращения (время регистрации)	Момент времени, отраженный в обращении как время его регистрации в СУТП. Соответствует времени присвоения статуса «Зарегистрировано»
Время решения обращения (время решения)	Момент времени, отраженный в заявке как время его решения в СУТП, соответствует моменту присвоения заявке статуса «Выполнено»
Длительность решения	Время, фактически затраченное Исполнителем на обработку обращения. Период времени от присвоения заявке статуса «Зарегистрировано» до присвоения статуса «Выполнено». Время, в течение которого заявка находится в статусе «Приостановлено», не входит в длительность решения
Заявка	Зарегистрированное в СУТП Обращение Пользователя
Инициатор обращения Обращение	Пользователь, обратившийся в СТП в рамках оказания Услуг по Договору Обращение пользователя в СТП по вопросам, связанным с оказанием Услуг
ОПО	Общее программное обеспечение КТС АПК «Безопасный город».
Время доступности функции, (рабочее время)	Период времени, в течение которого должно обеспечиваться исполнение функции СТП
Режим доступности функции (режим работы)	График рабочего времени, в течение которого осуществляется исполнение функций СТП, состоящий из количества рабочих часов и количества рабочих дней. Возможные варианты: 8x5 – 8 рабочих часов 5 рабочих дней в неделю, пн. -пт. с 8:00-17:00 (МСК); Время, находящееся за пределами, указанного режима, а также время, выпадающее на нерабочие и праздничные дни, установленные законодательством РФ, является нерабочим.
СУТП	Система управления технической поддержкой Исполнителя – программное обеспечение, в котором производится отражение фактов регистрации и обработки Обращений. Предоставляется Исполнителем
Тип обращения	Признак, по которому производится классификация обращений в СУТП, в зависимости от оказываемых Услуг

Приоритеты обработки Инцидентов

При регистрации обращений с типом «Инцидент» в СУТП назначается приоритет в зависимости от влияния отказа или сбоя на функционирование компонентов Системы (Таблица №11 Соглашения).

Таблица №11. Приоритеты Инцидентов и плановое время исполнения

№ п/п	Приоритет инцидентов	Описание	Плановое время исполнения
1.	Приоритет № 1 (Высокий)	Критичная ошибка/проблема, приводящая к неработоспособности системы в целом или большей ее части	2 (два) рабочих дня
2.	Приоритет № 2 (Средний)	Ошибка/проблема, приводящая к неработоспособности части сервисов	7 (семь) рабочих дней
3.	Приоритет № 3 (Низкий)	Ошибка/проблема, не влияющая на работу системы в целом (единичные пользователи и/или сервисы)	14 (четырнадцать) рабочих дней

Плановое время исполнения, указанное в Таблице №11 Соглашения, обеспечивается только при наличии у Заказчика необходимых ЗИП на складе, а также квалифицированного сотрудника в месте размещения компонентов Системы, способного, в случае необходимости, оперативно выполнить работы, по извлечению/установке вышедших из строя компонентов Системы.

Контрольные сроки решения (выполнения) обращений

Исполнитель должен производить обработку обращений в соответствии с установленными контрольными сроками на выполнение операций (Таблица № 12 Соглашения).

Таблица 12 – Время реагирования на инцидент

№ п/п	Приоритет	Время реакции
1.	Высокий	не более 1 (одного) часа (в рабочие часы с 08:00 до 17:00 (МСК))
2.	Средний	не более 4 (четырёх) часов (в рабочие часы с 08:00 до 17:00 (МСК))
3.	Низкий	не более 8 (восьми) часов (в рабочие часы с 08:00 до 17:00 (МСК))

Периодичность проведения работ компонентов КТС и ПОИБ АПК «Безопасный город»

Исполнитель должен обеспечить периодичность проведения работ КТС и ПОИБ АПК «Безопасный город» в соответствии с установленными параметрами (Таблица № 13 Соглашения).

Таблица № 13. Режимы работы компонентов КТС АПК «Безопасный город»

№ п/п	Параметр	Периодичность
	Разрешенное время (окно) проведения плановых регламентных работ	08:00-17:00 часов (время московское)
	Порядок проведения плановых и регламентных работ	В соответствии с: 1. Регламентом оказания услуг (Приложение №4 к ТЗ)
	Корректировка настроек обслуживаемых узлов в случае такой необходимости, взаимодействие с представителями иных обслуживающих (или проводящих работы на обслуживаемом объекте) организаций	По мере поступления заявок Заказчика
	Формирование и поддержание в актуальном состоянии правил межсетевое экранирования как в отношении отдельных узлов, так и в отношении обслуживаемой системы защиты в целом	По мере поступления заявок Заказчика
	Очистка оборудования от пыли и грязи, внешних поверхностей оборудования, организация оборудования в телекоммуникационной стойке (шкафу)	Проводится на месте установки оборудования, материалы и инструмент – Исполнителя, периодичность проведения – 1 раз в квартал
	Плановая и внеплановая смена ключевого	По мере поступления заявок Заказчика или по

материала на обслуживаемых СКЗИ	мере выявления скомпрометированного узла
Генерация ключевых дистрибутивов для новых узлов СКЗИ, задание необходимых связей между узлами	По мере поступления заявок Заказчика
Учет СКЗИ	По мере проведения соответствующих работ
Установка и поддержание межсетевого взаимодействия	По мере поступления заявок Заказчика
Периодическое тестирование работоспособности используемых СЗИ и СКЗИ	Раз в квартал
Периодическая оценка защищенности информационных ресурсов, защищаемых обслуживаемой системой защиты информации с формированием отчета	Раз в квартал
Периодическое обновление баз, решающих правил используемых средств обнаружения вторжений	Раз в месяц, по мере выхода соответствующих обновлений
Диагностика работоспособности, локализация и устранение неисправностей, тестирование работоспособности	По мере поступления заявок Заказчика
Контроль состояния обслуживаемых узлов, формирование превентивных мероприятий по предотвращению перехода системы в аварийный режим	Постоянно
Информирование Заказчика и его представителей о состоянии обслуживаемой системы	По мере проведения соответствующих работ, по запросу Заказчика
Консультации представителей Заказчика по вопросам эксплуатации применяемых средств защиты информации	По мере поступления заявок Заказчика
Установка обновлений ПО средств защиты информации	По мере поступления заявок Заказчика и по мере выпуска производителем соответствующего программного обеспечения
Резервное копирование настроек конфигурации	Раз в месяц. Производится после внесения изменений в конфигурацию

Методика оценки качества оказания Услуг

Для оценки качества оказания Услуг Заказчиком применяются метрики качества в соответствии с Таблицей № 14 Соглашения.

Таблица № 14. Метрики качества оказания Услуг

№№ п/п	Метрика	Параметр, от которого зависит метрика	Объем нарушений	Значение метрики	Вес метрики, Р
1.	Нарушение сроков обработки обращений	Суммарное время нарушений сроков всех обращений, обработанных с нарушением срока (Таблица № 10 Соглашения)	от 0ч. до 3ч.(включительно)	1	0,3
			более 3ч. до 5ч.(включительно)	0,5	
			более 5ч.	0	
2.	Количество нарушений сроков обработки обращений типа «Инцидент»	Количество зафиксированных случаев нарушения сроков обработки обращений типа «Инцидент»	от 0ед. до 2ед. (включительно)	1	0,3
			более 2ед. до 4 ед. (включительно)	0,5	
			более 4ед.	0	
3.	Количество нарушений сроков обработки обращений типа «Обслуживание»	Количество зафиксированных случаев нарушения сроков обработки обращений типа «Обслуживание» по всем обращениям данного типа, обработанным с нарушением срока.	от 0ед. до 2ед. (включительно)	1	0,2
			более 2ед. до 4ед.(включительн о)	0,5	
			более 4 ед.	0	

Итоговый показатель качества технической поддержки (QoS) рассчитывается по формуле:

$$QoS = \sum P_i Q_i,$$

где

i – номер метрики;

P_i – вес i -й метрики (в соответствии с Таблицей № 15);

Q_i – значение i -й метрики (в соответствии с Таблицей № 15).

Итоговый вывод о качестве технической поддержки формулируется в соответствии с критериями Таблицы № 16.

Таблица № 15. Оценка качества оказанных Услуг

Итоговая оценка	Критерии оценки	Документ, на основании которого производится оценка
Услуги оказаны надлежащим образом	Значение QoS составляет от 0,95 (включительно) до 1 (включительно)	Журнал оказания Услуг; Отчет о качестве оказания Услуг за отчетный период; Отчет по обслуживанию АПК «Безопасный город».
Услуги оказаны ненадлежащим образом*	Значение QoS составляет от 0,75 (включительно) до 0,95	
Существенное нарушение условий Договора*	Значение QoS составляет менее 0,75	

*Каждое нарушение установленных критериев является отдельным нарушением условий Договора.

РЕГЛАМЕНТ ОКАЗАНИЯ УСЛУГ

– Общие положения

Настоящий Регламент устанавливает требования к порядку оказания Услуг по поддержанию в исправном состоянии КТС и ПОИБ АПК «Безопасный город» Брянской области.

Регламент разработан с целью:

- определения перечня компонентов, подлежащих обслуживанию;
- определения процедуры обслуживания компонентов;
- определения перечня компонентов, подлежащих регламентному обслуживанию;
- определения процедуры регламентного обслуживания компонентов;
- определения процедуры восстановления компонентов КТС и ПОИБ;
- определения процедуры восстановления работоспособности технических средств оказания Услуг;
- определения формы отчета по оказанным Услугам.

Под регламентным обслуживанием понимаются профилактические мероприятия, выполняемые специалистом Исполнителя в соответствии с Приложением № 3 к ТЗ.

Контрольные сроки решения (выполнения) обращений по Услугам выполнения запросов на обслуживание и восстановление компонентов приведены в Приложении № 3 к ТЗ «Соглашение об уровне качества Услуг».

– Требования к услугам

– Услуга «Поддержание в исправном состоянии»

В процессе оказания услуги Исполнитель должен обеспечить выполнение следующих операций:

Таблица № 16. Перечень операций по поддержанию оборудования в исправном состоянии

№ п/п	Перечень операций	Периодичность	Отчетные документы, в которых отражается выполнение операции
1	Устранение Инцидента	По запросу; По результатам модуля мониторинга	Журнал оказания Услуг

На техническое обслуживание Исполнителем принимается исправное оборудование, указанное в Приложениях №1 и №2 к ТЗ.

В случае обнаружения неисправности оборудования и/или в случае отсутствия оборудования по адресу его размещения Исполнитель официальным письмом направляет отчет об обследовании в произвольной форме сообщая Заказчику об обнаруженных неисправностях (или отсутствии) оборудования в день обнаружения данных фактов с конкретными рекомендациями по их устранению.

Мероприятия по регламентному обслуживанию выполняются в соответствии с Таблицей № 13 Соглашения.

По результатам выполненных работ необходимо сделать запись в Журнале оказания Услуг.

- Требования к выполнению операции по настройке компонентов

В рамках выполнения операции Исполнитель осуществляет изменения в настройках компонентов, в соответствии с Заявкой или по результатам работы модуля мониторинга.

А также:

- диагностику и определение неисправностей;
- восстановление работоспособности Системы после проведения квалифицированным сотрудником Заказчика работ по замене и/или ремонту вышедших из строя компонентов Системы, при наличии необходимых ЗИП на складе;

▪ Требования к выполнению операции по изменению конфигурации компонентов АПК «Безопасный город»

В рамках выполнения операции Исполнитель должен осуществлять изменения в конфигурации компонентов КТС (Таблица №5, №6 ТЗ):

- изменение аппаратной конфигурации компонентов КТС в случае возникшей аварии Системы, повлекшей за собой замену компонентов Системы на аналогичные, при наличии необходимых ЗИП на складе;

- изменение аппаратной конфигурации компонентов ПОИБ в случае возникшей аварии Системы, повлекшей за собой замену компонентов Системы на аналогичные, при наличии необходимых ЗИП на складе (Приложение №2);

- изменение программной конфигурации компонентов ПОИБ в случае функционального сбоя Системы или несанкционированного доступа в Систему третьими лицами.

- Услуга «Восстановление работоспособности компонентов КТС и ПОИБ при возникновении Инцидентов»

▪ Требования к операции по устранению Инцидента

В рамках выполнения операции специалист Исполнителя проводит дистанционную (удаленную) диагностику отказа (неисправности) компонента. При необходимости специалист Исполнителя связывается с уполномоченным представителем Заказчика для получения дополнительной информации.

В случае успешного восстановления работоспособности дистанционно сотрудник Исполнителя вносит в Заявку СУТП информацию о действиях по восстановлению работоспособности компонента АПК «Безопасный город», дате их выполнения и фамилию сотрудника Исполнителя.

На компонентах АПК «Безопасный город» восстановление работоспособности производится дистанционно сотрудником Исполнителя.

В зависимости от результатов проведенной диагностики сотрудник Исполнителя выполняет действия в соответствии с Регламентом оказания Услуг (Приложение №4).

• Устранение Инцидента в случае программного сбоя

Устранение Инцидента осуществляется восстановлением ОПО и/или настроек ОПО, микрокодов и/или настроек микрокодов из резервной копии.

• Устранение Инцидента в случае аппаратного сбоя

В случае аппаратного сбоя специалистами Заказчика обеспечивается полное восстановление работоспособности Системы, путем ремонта или замены компонентов Системы, при наличии необходимых ЗИП на складе.

- Контроль результатов

Контроль результатов устранения инцидентов осуществляется записью в Журнале оказания Услуг.

- Требования к отчетности

- Требования к ежемесячной отчетности

Исполнитель ежемесячно, до 5 числа месяца, следующего за отчетным (за декабрь отчет предоставляется не позднее 20 декабря), предоставляет Заказчику отчет по техническому обслуживанию оборудования и программного обеспечения КТС и ПОИБ АПК «Безопасный город» в электронном виде на электронном носителе информации (CD или DVD-диск), в формате, совместимым с MS Office, с рекомендациями по своевременному предупреждению проблем функционирования средств защиты информации. К отчету Исполнитель прилагает Акт приема-передачи сопроводительной документации.

Состав отчёта:

- 1 перечень изменений в структуре КТС и ПОИБ АПК «Безопасный город», с указанием дат;
- 2 перечень заменённых комплектующих наименований устройств, в которых проведена замена, перечень заменённых устройств;
- 3 журнал регистрации письменных и устных обращений;
- 4 журнал регистрации выявленных попыток НСД к ресурсам АПК «Безопасный город» с указанием принятых мероприятий;
- 5 рекомендации по устранению эпизодически возникающих проблем (если такие проблемы возникают);
- 6 предложение по оптимизации используемых компонентов КТС и ПОИБ (в случае необходимости).

- Требования к ежеквартальной отчетности

Исполнитель ежеквартально, до 5 числа квартала, следующего за отчетным кварталом (за 4 квартал отчет предоставляется не позднее 20 декабря), предоставляет Заказчику отчет об оценке защищенности АПК «Безопасный город» в электронном виде на электронном носителе информации (CD или DVD-диск), в формате, совместимом с MS Office, с рекомендациями, необходимыми для закрытия выявленных уязвимостей. К отчету Исполнитель прилагает Акт приема-передачи сопроводительной документации.

Состав отчета:

1. результаты оценки защищенности, перечень выявленных уязвимостей;
2. перечень рекомендуемых мероприятий по закрытию выявленных уязвимостей.

– Требования к отчетности, предоставляемой по окончании работ

По окончании исполнения государственного Договора, Исполнитель предоставляет Заказчику на электронном носителе информации (CD или DVD-диск) в формате, совместимом с MS Office, следующую документацию:

1. отчет об обследовании ГИС АПК «Безопасный город» в части используемых средств и систем обеспечения информационной безопасности;
 2. технический паспорт на КТС и ПОИБ;
 3. учетные данные на элементы КТС и ПОИБ;
 4. актуальную IP-адресацию системы КТС и ПОИБ;
- документы, подготовленные за последний отчетный период, а также итоговый Акт приема-передачи сопроводительной документации.

– Взаимодействие Заказчика и Исполнителя

Для выполнения работ по обслуживанию КТС и ПОИБ АПК «Безопасный город» Заказчик обеспечивает Исполнителя всей необходимой для выполнения этих работ документацией (в том числе, логинами, паролями, IP-адресами доступа и т.п.). При проведении работ Исполнитель может изменять переданные ему данные аутентификации только по согласованию с Заказчиком.

Заказчик обеспечивает беспрепятственный доступ сотрудников Исполнителя на объекты Заказчика ко всем необходимым компонентам, размещенным в помещениях на объектах Заказчика.

– Требования к обеспечению лицензионной и патентной чистоты

Ответственность за лицензионную чистоту уже используемого ПО лежит на Заказчике.

Установка и использование Исполнителем нелицензионного программного обеспечения не допускается, ответственность за нарушения данного требования лежит на Исполнителе.

– Требования к обеспечению безопасности и конфиденциальности

При оказании Услуг Исполнитель обязуется:

- не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся на объектах автоматизации;
- не осуществлять несанкционированный доступ к информационным ресурсам объектов автоматизации;
- не проводить незаконное копирование информации, циркулирующей или хранящейся на объектах автоматизации;
- не предпринимать манипулирование информацией, циркулирующей или хранящейся на объектах информатизации (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);
- не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;
- не внедрять на объекты автоматизации программы-вирусы (загрузочные, файловые и др.);
- не устанавливать программные и аппаратные закладные устройства в технические средства объектов автоматизации;
- не устанавливать в технические средства объектов автоматизации программное обеспечение, зараженное вирусами.

– Требования к персоналу Исполнителя

Специалисты Исполнителя, находящиеся на территории Заказчика, подчиняются всем правилам и распорядку, принятым в организации Заказчика.

Персонал Исполнителя должен пройти обучение и подтвердить квалификацию, необходимую для выполнения работ по сопровождению КТС, СЗИ и СКЗИ, входящих в состав обслуживаемых узлов доступа. В частности, персонал Исполнителя должен подтвердить квалификацию персонала, предоставив Заказчику копии действующих дипломов/сертификатов/свидетельств по следующим направлениям:

5. администрирование СХД – не менее 1 чел.;
6. сетевая инфраструктура на базе ELTEX – не менее 1 чел.;
7. администрирование системы защиты информации ViPNet – не менее 1 чел.;
8. программно-аппаратные комплексы ViPNet HW версия 4 – не менее 1 чел.;
9. программно-аппаратный комплекс ViPNet IDS – не менее 1 чел.

Приложение 5

РЕГЛАМЕНТ МОНИТОРИНГА КОМПОНЕНТОВ КТС АПК «БЕЗОПАСНЫЙ ГОРОД»

- Общие положения

Настоящий Регламент устанавливает основные требования к организации мониторинга производительности и доступности компонентов КТС.

Регламент разработан с целью:

- определения общих требований к мониторингу компонентов КТС;
- определения перечня компонентов КТС, подлежащих мониторингу;
- определения процедуры мониторинга компонентов КТС.

- Требования к Услуге мониторинга доступности и производительности компонентов КТС

Модуль мониторинга должен использоваться в следующих целях:

- повышение эксплуатационной готовности КТС АПК «Безопасный город» за счет мониторинга состояния компонентов КТС;

- предотвращение аварийных ситуаций за счет механизмов раннего выявления событий, потенциально приводящих к отказам в работе компонентов КТС;

- визуального отслеживания состояния компонентов КТС на основании информации, получаемой из модуля мониторинга.

Перечень компонентов и систем КТС и технических средств оказания Услуг, являющихся объектами мониторинга, приведены в Таблице № 4.2 к ТЗ, за исключением телекоммуникационных монтажных шкафов, жестких дисков, запасных частей и принадлежностей.

Модуль мониторинга предоставляется Заказчиком и должен обеспечивать следующие функции:

- контроль Исполнителем доступности сетевых коммутаторов, серверов, СХД по протоколу ICMP/SNMP;

- возможность сигнализации Исполнителю о нарушениях в работе серверов и СХД – превышение нагрузки на процессорах, оперативной памяти, дисковых устройств и сетевых интерфейсов, сбои в работе дисковой подсистемы, состояние системных служб при наличии такой возможности в предоставляемой Заказчиком Системе;

- возможность сигнализации посредством Web-интерфейса Исполнителю при повышении температуры используемого оборудования или отдельных его компонентов от заданных эксплуатационных параметров, указанных в документации производителя по эксплуатации оборудования;

- информирование о недоступности или предельной загрузке каналов связи между компонентами КТС.

o Требования к перечню параметров мониторинга

Рекомендуемый перечень параметров, предоставляемых системой мониторинга Заказчика указан в таблице №16. В рамках технической поддержки Исполнитель используют существующую и настроенную Заказчиком систему мониторинга.

Таблица № 17. Рекомендуемый перечень параметров, предоставляемых системой мониторинга

Заказчика

№п/п	Компонент	Объекты и параметры измерения
1.	Сервер/Виртуальные серверы/СХД	Центральный процессор, CPU: Длина очереди процессора (количество задач на ядро процессора в среднем за пять минут); Процессорное время (время простоя, в процентах); Процессорное время (используемое системой, в процентах); Процессорное время (используемое приложениями, в процентах); Процессорное время (время ожидания операций I/O, в процентах); Температура процессора (градусы Цельсия). Мониторинг состояния процессов (базовые) Наличие процесса в системе Количество запущенных процессов (в любом из состояний) Оперативная память, RAM (дополнительно): Расширенная информация о памяти из /proc/meminfo Дисковая подсистема (базовые): Количество свободно места на разделах (в мегабайтах и процентах) Доступность iSCSI-target (при наличии программной компоненты); Состояние массивов RAID (при наличии программной компоненты); Состояние SMART для HDD (при наличии программной компоненты). Сетевые интерфейсы (базовые): Входящая/исходящая загрузка активных сетевых интерфейсов в байтах/сек или бит/сек Сетевые интерфейсы (дополнительные): Входящая исходящая загрузка активных сетевых интерфейсов в пакетах в секунду
2.	Коммутатор	Центральный процессор, CPU: Процессорное время (в процентах); Температура процессора/окружающей среды (градусы Цельсия) Оперативная память, RAM: Количество использованной RAM (в процентах или мегабайтах). Сетевые интерфейсы: Входящая/исходящая загрузка активных сетевых интерфейсов в байтах/сек или бит/сек; Входящая/исходящая загрузка активных сетевых интерфейсов в пакетах/сек; Скорость порта; Оперативный статус порта

○ Требования и описание Модуля мониторинга доступности и производительности компонентов КТС

Модуль мониторинга должен осуществлять:

- проверку сетевой доступности в соответствии с адресом (IP, URL и т.д.) компонентов и систем;
- проверку значений производительности (загруженности) каждого компонента или Системы;
- отображение состояния доступности и производительности компонентов и систем;
- индикацию нарушения доступности и пороговых значений производительности компонентов и систем.

В модуле мониторинга реализована возможность просмотра параметров и пороговых значений мониторинга для каждого компонента и системы на каждом компоненте КТС в режиме реального времени со следующими временными интервалами: 24 часа, 72 часа, 1 неделя, 1 месяц, 6 месяцев, 1 год в графическом виде.

- Требование к Услуге мониторинга доступности и производительности компонентов КТС

В рамках оказания Услуги по мониторингу доступности и производительности компонентов КТС Исполнитель по запросу предоставляет отчеты Заказчику.

- Контроль результатов

Контроль результатов мониторинга компонентов КТС осуществляется по результатам предоставленных отчетов доступности и производительности компонентов КТС АПК «Безопасный город» и Журнала оказания услуг.

Приложение 6

РЕГЛАМЕНТ ОБРАБОТКИ ОБРАЩЕНИЙ

– Порядок обращений

Для оказания Услуг Исполнитель в течение 5 (пяти) рабочих дней с даты заключения Договора уведомляет заказчика об ответственном лице/сотруднике Исполнителя и предоставляет официальным письмом телефонный номер и электронную почту ответственного лица для приема обращений Пользователей и представителей Заказчика.

– Функции регламента обработки обращений

Регламент обработки обращений должен обеспечивать выполнение функций и задач в соответствии с Таблицей № 17.

Таблица № 18. Функции и задачи регламента обработки обращений

№ п/п	Функция (задача) СТП	Ответственный за функцию регламента обработки обращений
1.	Приём и регистрация обращений	Исполнитель
2.	Классификация обращений	
3.	Оказание Услуг (выполнение операций)	

Режим доступности функций регламента обработки обращений

Предоставление функций должно осуществляться в соответствии с режимом работы и рабочим временем (Таблица № 19).

Таблица № 19. Режимы доступности функций СТП

№ п/п	Функция (задача) СТП	Режим доступности функции (телефон/ эл. почта/ портал)	Время доступности функции
1.	Приём и регистрация обращений	8x5	Пн-пт, с 8:00 до 17:00 (МСК), кроме выходных и праздничных дней)
2.	Классификация обращений		
3.	Оказание Услуг (выполнение операций)		

1.1. Параметры оказания Услуг

Регламент обработки обращений должен включать следующие параметры оказания Услуг (Таблица № 20).

Таблица № 20. Параметры оказания Услуг

№ п/п	Параметр	Значение
1.	Максимальное время ожидания ответа по телефонной линии	30 мин.
2.	Среднее время ожидания ответа по телефонной линии	20 мин.

Порядок обработки обращений

Обработка обращений должна осуществляться в соответствии с Правилами обработки обращений в рамках функций регламента оказания услуг (Таблица № 21).

Таблица № 21. Правила обработки обращений в рамках функций регламента обработки обращений

№ п/п	Функция (задача) СТП	Порядок
1.	Приём и регистрация обращений	Согласно требованиям п. 2.1 Регламента. Приём обращений осуществляется в соответствии с режимом доступности функций (Таблица № 19)

2.	Классификация обращений	В соответствии с требованиями п. 3.2 Регламента
3.	Оказание Услуг	В соответствии с требованиями п. 3.3 Регламента

На всех стадиях обработки обращений должны присваиваться статусы обращений (Таблица № 22).

Таблица № 22. Статусы обработки обращений

№	Наименование статуса	Описание	Последующий статус
1.	Новый	Обращение принято	Зарегистрировано
2.	Зарегистрировано	Обращение зарегистрировано	В работе; Приостановлено; Закрыто (по несоответствию Договору);
3.	В работе	Обращение принято, действия по сути выполнения обращения уже начаты.	Выполнено; Приостановлено
4.	Приостановлено	Работы по обращению приостановлены. Со стороны инициатора обращения требуются дополнительные действия/информация. Обращение должно быть автоматически закрыто, если находится в этом статусе более 15 (Пятнадцати) календарных дней для работ, проводимых на не гарантийном оборудовании. Срок действия приостановки не учитывается в общем сроке обработки обращения.	В работе; Выполнено; Закрыто;
5.	Выполнено	Обращение выполнено. Если по обращению в статусе «Выполнено» не подтверждена информация от Заказчика/Представителя Заказчика о решении данного обращения в течение 15 (Пятнадцати) календарных дней, то сотрудник СТП Исполнителя	Закрыто; В работе;

		должен перевести такое обращение в статус «Закрыто».	
6.	Закрыто	Обращение закрыто. Получено подтверждение Заказчика о выполнении работ по обращению.	-

Порядок приёма и регистрации обращений

Исполнитель должен обеспечивать приём обращений в соответствии с установленными требованиями (Таблица № 23).

Таблица № 23. Порядок приёма обращений в СТП

№№ п/п	Инициатор обращения	Порядок (способы) приема обращений
1	Пользователь	– телефон – электронная почта
2	Ответственный представитель Заказчика	– телефон – электронная почта
3	Модуль мониторинга	– электронная почта

В каждом Обращении должна содержаться следующая информация:

- дата и время регистрации обращения;
- тип Обращения;
- приоритет;
- текущий статус обработки Обращения;
- ФИО Инициатора Обращения;
- контактные данные Инициатора Обращения;
- подробное описание по сути обращения.

В обращениях с типом «Инцидент» указывается, в том числе, следующая информация:

- сетевое имя компонента;
- сетевой адрес компонента;
- тип компонента;
- описание шагов, в результате выполнения которых произошла ошибка/ возникла проблема;
- снимки экрана с сообщением об ошибке (при наличии);
- информация о причинах смены приоритета (при смене приоритета).

Сотрудник Исполнителя проводит первичную классификацию обращения в соответствии с перечнем Услуг и типом обращения (Приложение № 3 к ТЗ).

При необходимости уточнения у инициатора обращения информации, необходимой для обработки Обращения, сотрудник Исполнителя может перевести данное обращение в статус «Приостановлено» с уведомлением Заказчика и инициатора обращения и вернуть его в работу после получения необходимых сведений.

Порядок классификации обращений

В рамках классификации Обращения сотрудник Исполнителя осуществляет проверку и окончательное определение:

- типа Обращения;
- оказываемой Услуги;
- приоритета Инцидента;
- контрольного срока обработки.

Сотрудник Исполнителя, классифицирующий Обращение, осуществляет информирование Инициатора обращения об ориентировочных сроках решения Обращения.

Порядок оказания Услуг

В рамках функций регламента обработки обращений по выполнению операций осуществляются:

- устранение Инцидентов (тип Обращения «Инцидент») в соответствии с установленным приоритетом в соответствии с контрольными сроками (Приложения № 3 к ТЗ);
- выполнение операций (тип Обращения «Обслуживание») в соответствии с контрольными сроками (Приложение №3 к ТЗ), при наличии у Заказчика необходимых компонентов в ЗИП на складе, а также квалифицированного сотрудника в месте размещения компонентов Системы, способного, в случае необходимости, оперативно выполнить работы, по замене вышедших из строя компонентов Системы.

В процессе обработки Обращения может потребоваться дополнительная информация или действия Инициатора, необходимые для решения Обращения – на период запроса указанных данных обработка Обращения приостанавливается: статус обработки обращения может быть изменен на «Приостановлено» с уведомлением Заказчика посредством оповещения по электронной почте.

Порядок приостановки и завершения отсчёта времени решения Заявки

Порядок перевода Заявки в статус завершения («Закрыто»)

Отчет времени выполнения по Заявке завершается при переводе ее в статус «Закрыто». Заявка может быть закрыта по следующим основаниям:

Заявка не соответствует условиям Договора:

Закрытие происходит без выполнения каких-либо работ (операций). Закрыть Заявку может сотрудник Заказчика при выявлении несоответствия указанной в Заявке информации об оборудовании, информационной системе, адресе и типе требуемых Услуг Договору, на основании которого осуществляется оказание Услуг. При выявлении таких несоответствий выполнение Заявки приостанавливается сотрудниками Исполнителя до подтверждения и закрытия Заказчиком. О закрытии Заявки Инициатор информируется письмом по электронной почте.

Заявка неактуальна:

Закрытие происходит по инициативе Инициатора, либо в случае, когда Инициатор в течение длительного времени не предоставляет информацию, необходимую для качественного и полного решения. Закрыть Заявку может сотрудник Заказчика на основании обращения Инициатора, либо по истечении срока ожидания ответа Инициатора. Закрытие происходит без выполнения каких-либо операций. О закрытии Заявки Инициатор информируется письмом по электронной почте.

Переклассификация Заявки:

Закрытие происходит при выявлении несоответствия указанного в Заявке типа Услуг типу Услуг, которые на самом деле необходимо оказать по данному обращению Инициатора. О закрытии Заявки Инициатор информируется письмом по электронной почте, в котором указывается причина закрытия и номер Заявки, вновь открытой для оказания Услуг по Договору.

Заявка решена (Выполнено):

Сотрудник Исполнителя после выполнения всех необходимых по существу Заявки операций переводит Заявку в статус «Выполнено», Инициатору при этом отправляется письмо по электронной почте с просьбой подтвердить выполнение Заявки либо выразить свое несогласие с тем, что Заявка выполнена. Если Инициатор подтверждает оказание Услуг и решение поставленных в его Обращении проблем, то Заявка переходит в статус «Выполнено». Если от Инициатора в ответ на письмо-оповещение отсутствует реакция в течение двух рабочих дней, то через два рабочих дня Заявка автоматически переводится в статус «Закрыта».

Порядок перевода Заявки в статус ожидания (приостановки)

Статус ожидания (приостановка) присваивается Заявке в тех случаях, когда сотрудник Исполнителя, работающий по данной Заявке, по независящим от Исполнителя причинам не может выполнить Заявку. В таких случаях указывается причина перевода в ожидание. При этом Инициатору и Заказчику направляется по электронной почте письмо-оповещение о приостановке выполнения Заявки с указанием причин приостановки. Инициатор имеет возможность отменить приостановку в том случае, если по тем или иным причинам не согласен с приостановкой (никто из сотрудников Исполнителя не обращался за уточнениями, указана неверная причина и т.п.).

Причины, по которым допускается перевод Заявки в статус ожидания (приостановки заявки), максимально допустимый срок приостановки, после которого Заявка выводится из ожидания, а также действия по истечению срока приостановки приведены в Таблице № 24.

Переводить Заявку в состояние ожидания имеют право Заказчик и сотрудники Исполнителя, выполняющие данную Заявку.

Таблица № 24. Причины и сроки перевода заявок в статус ожидания, действия после завершения срока приостановки

№ п/п	Допустимые причины приостановки	Максимальный срок приостановки	Действия после завершения срока приостановки	Возможные причины перевода заявок
1	Ожидание завершения работ, не зависящих от Исполнителя (внешние условия)	1 рабочий день	После истечения срока приостановки Заявке возвращается статус, из которого она перешла в приостановку; исполнителем заявки назначается исполнитель, приостановивший выполнение	Отключение электричества, отсутствие доступа на объект в соответствии с его графиком работы, проведение сотрудниками Заказчика ремонтных работ/замену компонентов Системы в случае выхода их из строя, форс-мажор и прочие внешние обстоятельства, не зависящие от Исполнителя и влияющие на время решения Заявки
2	Выполнение обращения требует проведения работ, связанных с обработкой, копированием большого объема данных	8 рабочих часов	После истечения срока приостановки Заявке возвращается статус, из которого она перешла в приостановку; исполнителем заявки назначается группа, которой принадлежит исполнитель, приостановивший выполнение	Если выполнение Заявки требует проведения работ, связанных с обработкой, копированием большого объема данных (более 50 (пятидесяти) Гбайт) и данные операции превышают согласованное время решения, то: Исполнитель направляет Инициатору и Заказчику сообщение о необходимости и причинах приостановки Заявки; Инициатор ответным письмом по электронной почте подтверждает

				получение информации о приостановке Заявки
3	Ожидание согласования уполномоченного лица Заказчика	8 рабочих часов	После истечения срока приостановки Заявке возвращается статус, из которого она перешла в приостановку; исполнителем заявки назначается группа, которой принадлежит исполнитель, приостановивший выполнение	В тех случаях, когда для выполнения Заявки требуется получение согласования от должностного лица Заказчика, согласно действующим организационно-распорядительным и нормативным документам Заказчика и Исполнителя
4	Отложено по инициативе пользователя/Инициатора	5 рабочих дней	После истечения срока приостановки Заявка закрывается «по неактуальности заявки».	В процессе исполнения Заявки Пользователь/Инициатор обратился с документально подтвержденной просьбой о приостановке выполнения Заявки
5	Ожидание ответа пользователя	1 рабочий день	После истечения срока приостановки Заявке возвращается статус, из которого она перешла в приостановку; исполнителем заявки назначается исполнитель, приостановивший выполнение	В случае, если для решения Заявки требуется дополнительная информация от Пользователя/Инициатора, без которой выполнить Заявку невозможно
8	Ожидание закрытия по несоответствию Договору	1 рабочий день	После истечения срока приостановки Заявке возвращается статус, из которого она перешла в приостановку; исполнителем заявки назначается исполнитель, приостановивший выполнение	При выявлении Исполнителем несоответствия указанной в Заявке информации об оборудовании, адресе и типе Услуг Договору, на основании которого оказываются Услуги

Приложение 7

Данные о сотрудниках Исполнителя для предоставления доступа к местам оказания Услуг

№ п/п	Ф.И.О.	Название организации, место работы	Должность
1	2	3	4