Техническое задание

на услуги по предоставлению сервисов для обеспечения деятельности объектов государственной информационной системы в сфере здравоохранения (ГИСЗ РА) Республики Алтай в 2024 году

1. **Сервис сопровождения и технической поддержки средств защиты информации.**

1. **Подсервис активации сервиса технической поддержки продуктов ViPNet**

В рамках сервиса должны быть предоставлены сертификаты активации сервиса технической поддержки продуктов ViPNet (сеть № 1721).

Продукты ViPNet, на которые распространяется техническое сопровождение (шт.):

- программное обеспечение ViPNet Administrator 4.x (КС2) – 1;

- программно-аппаратный комплекс ViPNet Coordinator HW 1000 4.x – 6;

- программно-аппаратный комплекс ViPNet Coordinator HW 1000С 4.x – 2;

- программно-аппаратный комплекс ViPNet IDS NS1000 3.x – 2.

Уровень сопровождения «Стандартный» сервиса технической поддержки продуктов ViPNet включает в себя:

- Рекомендации по процессу установки продукта в объеме эксплуатационной документации;

- Рекомендации по настройке продукта в объеме эксплуатационной документации;

- Исполнитель предоставляет обновление (hotfix), устраняющее дефекты, выявленные в продукте;

- Исполнитель предоставляет обновление (hotfix), а также все изменения, производимые в рамках минорной (MINOR) версии ПРОДУКТА (service pack).

Прием обращений и консультирование осуществляется в режиме - 5 дней в неделю, 8 часов (по электронной почте).

Гарантированное время реакции на обращение определяется приоритетностью обращения:

П1- Критический: не более 8 рабочих часов;

П2- Средний: не более 12 рабочих часов;

П3-Низкий: не более 48 рабочих часов.

В рамках подсервиса должен быть предоставлен сертификат активации сервиса обновления баз решающих правил ПАК ViPNet IDS 1000 на срок 1 год, в количестве – 2 шт.

1. **Подсервис передачи прав на средство анализа защищенности**

В рамках подсервиса Заказчику должно быть переданы права сроком действия не менее 1 года на использование средства анализа защищенности на 32 IP адреса в количестве 1 шт, права на использование средства анализа защищенности на дополнительные IP адреса в количестве 18 шт.

В состав комплекта программного обеспечения должны входить:

- лицензия на право использования ПО;

-установочный комплект на ПО;

- копия сертификата соответствия ФСТЭК России, внесенного в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00, удостоверяющего соответствие ПО требованиям по безопасности информации, установленном в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК Росcии, 2018) – по 4 уровню доверия и технических условиях НПЭШ.00606-01, при выполнении указаний по эксплуатации, приведенных в формуляре НПЭШ.00606-01 30.

1. **Место предоставления сервиса**

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование Получателя | Наименование подсервиса | Кол-во, шт. |
| 1 | КУЗ РА "МИАЦ" | Подсервис активации сервиса технической поддержки и обновления продуктов ViPNet | 1 |
| 2 | КУЗ РА "МИАЦ" | Подсервис передачи прав на средство анализа защищенности | 1 |

1. **Сервис по передаче прав на средство антивирусной защиты информации**

В рамках сервиса должно быть осуществлено продление существующего у заказчика антивирусного программного обеспечения:

Неисключительное право на использование ПО Dr.Web Desktop Security Suite\* (LBW-BC-12M-1148-B3-FSTНеисключительное право на использование ПО Dr.Web Server Security Suite\* (LBS-AC-12M-70-B3-FS).

Программное обеспечение (программный продукт) передается с целью создания системы антивирусной защиты (далее - Система).

**Наименование:** Система антивирусной защиты (далее - Система)

1. **Общие требования**
	1. Участники конкурса на использование антивирусного программного продукта должны иметь статус официального партнера компании производителя, что является подтверждением их квалификации и прав на поставку антивирусных продуктов и/или лицензий. При заключении контракта необходимо предоставить копии документов, подтверждающих статус официального партнера компании производителя.
	2. Участник должен принять во внимание, что ссылка на наименование продукции носит описательный, а не обязательный характер. В случае если Участником предлагаются эквивалент требуемого Заказчиком ПО, то в составе своей конкурсной заявки он должен в обязательном порядке предоставить следующую информацию:
		1. в Техническом предложении – подробное техническое описание предлагаемого к поставке эквивалента, с указанием полного соответствия (или превосходящего) всем техническим характеристикам, указанным в данной спецификации, заверенное у производителя предлагаемого программного продукта

Отсутствие в составе конкурсной заявки подробного технического описания аналогов продукции и/или письма о согласовании может являться причиной отклонения конкурсной заявки Участника.

* 1. Все компоненты Системы должны принадлежать одной торговой марке с единой службой технической поддержки на русском языке. Техническая поддержка должна предоставляться непосредственно производителем поставляемых программных продуктов.
	2. Поставляемые средства защиты должны представлять масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети заказчика.
	3. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке.
	4. Все антивирусные средства, функционирующие под операционной системой типа Windows, включая средства управления, должны обладать контекстной справочной системой на русском языке.
	5. Участник конкурса должен предоставить единый серийный номер для всех поставляемых по условиям конкурса продуктов.
	6. Поставляемый серийный номер должен иметь возможность отложенной активации. Срок действия лицензионных ключевых файлов на все поставляемые по условиям конкурса программные продукты должен начинаться с момента активации серийного номера.
	7. Система лицензирования не должна иметь привязку к используемому на защищаемых объектах аппаратному обеспечению. Система должна позволять перенос лицензий с одних защищаемых объектов (в том числе рабочих станций и серверов) на иные без необходимости перепривязки или получения дополнительных лицензий
	8. Антивирусные средства должны включать:
* программные средства защиты рабочих станций;
* программные средства защиты файловых серверов;
* программные средства централизованного управления, мониторинга и обновления;
* обновляемые базы данных сигнатур вредоносных программ всех типов и атак;
* эксплуатационную документацию на русском языке.
1. **Требования к программным средствам**
	1. **Общие требования к системе антивирусной защиты**
		1. Программные средства Системы должны обеспечивать определение угроз следующих типов:
			1. классических вирусов;
			2. троянских программ;
			3. руткитов;
			4. сетевых червей;
			5. рекламных программ;
			6. программ автодозвона на платные сайты;
			7. потенциально опасных приложений;
			8. прочих вредоносных программ.
		2. Антивирусная защита должна обеспечивать:
			1. обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п.;
			2. обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками;
			3. обнаружение вирусов внутри контейнеров и архивных файлов формата ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (включая NRG, образы с нестандартным форматом сектора и не имеющие сигнатур), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER с зашифрованными контейнерами и т.д. без ограничений на уровень вложенности проверяемых объектов;
			4. обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME);
			5. обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т.д.);
			6. антивирусную проверку файлов и объектов, имеющих формат Smart Install Maker (SIM); DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); INNO SETUP (5.3.9 и выше); SETUP FACTORY (линейки 7,8); XENOCODE; TARMA INSTALL (линейка 3); XZ (UNIX); COMPRESS; SQUAHFS; CHILKAT ZIP; пакеты LHA (AWARD BIOS);
			7. антивирусную проверку в самораспаковывающихся архивах: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy;
			8. проверку исполняемых файлов, упакованных следующими упаковщиками: PELOCK, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, а также почтовых файлов Mozilla Thunderbird- вне зависимости от их размера;
			9. разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF;
			10. защиту от вредоносных программ, принадлежащих семействам вредоносных программ, информация о которых имеется в антивирусных базах, созданных после занесения соответствующей информации в антивирусные базы и еще не попавших на анализ в антивирусные лаборатории - как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;
			11. обнаружение вредоносных объектов в HTML- и PDF-документах, включая обфусцированные эксплойты в JavaScript, находящиеся в документах данных типов. Возможность извлечения и анализа «невидимых» IFRAME-элементов. Возможность извлечения для проверки скриптов любой сложности и снятие с них защиты;
			12. обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA);
			13. обнаружение угроз, направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля
			14. обнаружение вредоносных объектов в DEX-файлах (Android).
		3. Используемое антивирусное ядро:
			1. не должно допускать снижение скорости проверки при увеличении размера антивирусных баз;
			2. в связи с возможностью исчерпания ресурсов ОС (в том числе места на диске, памяти) в ходе обработки специальным образом сформированных архивов автоматически выбирать уровень анализа упакованных объектов, а также механизм уменьшения размера промежуточных файлов. При выборе уровня анализа должен учитываться уровень загрузки системы
			3. в целях ускорения проверки архивов и упакованных файлов должно обеспечивать опознание вредоносных программ без запуска распаковщика;
			4. должно обеспечивать защиту от так называемых «почтовых бомб»;
			5. должно обеспечивать работу с файлами размером как менее, так и больше 2 ГБ;
			6. должно поддерживать работу с дисками с LBA-адресацией;
			7. в целях исключения «утечки» оперативной памяти должно использовать механизм распределения динамической памяти уровня антивирусного ядра.
	2. **Требования к системе управления антивирусной защитой (далее - Сервер управления)**
		1. Система управления должна быть построена по клиент-серверной архитектуре с возможностью построения иерархической системы серверов – с возможностью использования в системе антивирусного управления как главных, так подчиненных серверов.
		2. Система управления должна быть реализована на основе Web-интерфейса, поддерживающего Web-браузеры, используемые как в корпоративной сети, так и Web-браузеры, используемые на устройствах и компьютерах, имеющих доступ к сервисам управления антивирусной защитой извне корпоративной сети - в том числе Mozilla Firefox или Internet Explorer. Управление через данные браузеры должно быть доступно с любых ОС, имеющих возможность их установки и запуска.
		3. Система должна включать поддержку кластерного протокола, с помощью которого координируются действия над агентами защиты с разных антивирусных серверов
		4. Система управления должна быть доступной с любой операционной системы, поддерживающей браузеры Mozilla Firefox или Internet Explorer (в том числе с ОС Microsoft Windows и ОС типа UNIX (Linux, FreeBSD, Solaris)), без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения как на стороне сервера управления, так и на стороне администратора Системы. Контроль работы Системы должен быть также возможен консоли управления, функционирующей на мобильных устройствах iPhone
		5. В целях безопасности все ПО, входящее в состав антивирусного сервера (в том числе необходимое для доступа с помощью браузера) должно поставляться в виде единого дистрибутива и принадлежать одной торговой марке.
		6. Система управления должна включать систему управления лицензиями, позволяющую распределять между серверами в рамках иерархической сети необходимое количество лицензий
		7. Установка антивирусного сервера Системы, сертифицированного на соответствие требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна быть возможна на:
			1. Microsoft Windows Server 2003;
			2. Microsoft Windows Server 2008;
			3. Microsoft Windows 7;
			4. Microsoft Windows 10;
			5. Microsoft Windows Server 2012;
			6. Microsoft Windows Server 2016;
			7. FreeBSD 10;
			8. Debian GNU/Linux 7;
			9. RedHat Enterprise Linux 6;
			10. Ubuntu 14;
			11. CentOS 6;
			12. CentOS 7;
			13. AstraLinux 1.6.
		8. Система управления должна иметь возможность:
			1. просмотра и сравнения состава аппаратно-программного обеспечения на станциях антивирусной сети
			2. контроля неактивных станций антивирусной сети
			3. просмотра сессий пользователей антивирусной сети
			4. замены системного DNS
			5. использования как внутренней СУБД (поставляемой в составе дистрибутива антивирусного сервера), так и внешней (устанавливаемой отдельно до или после развертывания антивирусного сервера). При использовании внешней СУБД Система должна иметь возможность работы с ней как без установки дополнительное ПО (с СУБД MS SQL, Oracle), так и с помощью драйверов ODBC для операционных систем Windows и Linux (в том числе с СУБД PostgreSQL). Система должна иметь возможность замены типа используемой СУБД после установки серверной части – без необходимости переустановки серверной части Системы
			6. управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов
			7. экспорта и импорта базы данных антивирусного сервера в XML-файл.
			8. создания иерархической сети антивирусных серверов. В случае реализации иерархической сети Система должна иметь возможность:
				1. объединения информации от нескольких серверов на одном.
				2. распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть.
				3. обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий
				4. контроля отсутствия связанных серверов в расписании антивирусного сервера.
			9. построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне;
			10. установки антивирусных агентов в сети, не использующей единого пароля доступа к рабочим станциям;
			11. централизованной настройки параметров защиты, уникальных для различных групп, в том числе для рабочих станций, находящихся в режиме off-line.
			12. централизованного сбора и просмотра статистической информации и создания отчетов о состоянии антивирусной защиты и их консолидации;
			13. интеграции в системы управления и информационные системы с помощью встроенного в систему API
			14. наличия множественных путей уведомления пользователей и администраторов путем посылки почтового сообщения, звукового оповещения, всплывающего окна, записи в журнал событий, SNMP-trap;
			15. оповещения о возникновении эпидемий (множественных инфекций)
			16. оповещения о наличии обновлений сервера
			17. отправки информационных сообщений пользователям по сети в режиме реального времени через Web-интерфейс Системы;
			18. обеспечения связи антивирусного сервера и клиентских частей через встроенный модуль в случае, когда они расположены в различных сетях, работающих по протоколам TCP/IP (в т.ч. IPv6), между которыми отсутствует маршрутизация пакетов
			19. самостоятельного написания обработчиков событий на языке Lua, а также выполнения произвольных Lua-скриптов с помощью средств системы управления.
		9. В случае интеграции с внешними подсистемами с помощью встроенного Web API, должна иметься возможность аудита действий, произведенных с помощью функций данного Web API
		10. Вне зависимости от типа антивирусного агента и защищаемой системы, Система должна обеспечивать реализацию следующих функциональных возможностей
			1. экспорта, импорта и распространения конфигураций групп, станций антивирусной сети или компонентов антивирусной защиты на другие группы, станции и компоненты, в том числе в целях изменения политик, применения их к определенным группам
			2. скачивания конфигурационных файлов с настройками подключения антивирусных агентов для ОС Android, Mac OS X и ОС семейства UNIX
			3. восстановления рабочих станций, случайно удаленных из системы защиты;
			4. централизованного обновления антивирусных баз на всех защищенных рабочих станциях, в том числе мобильных и находящихся в режиме off-line. Доставки обновлений на рабочие места пользователей как по расписанию, так сразу после их получения;
			5. обновления программных средств и антивирусных баз из разных источников, доставляемые как автоматически по каналам связи в пределах антивирусной сети, так и на отчуждаемых машинных носителях информации – путем ручной синхронизации информации между серверами и рабочими станциями
			6. обновления программных средств и антивирусных баз с помощью мобильного сервера обновлений, представляющего собой Сервер управления, развернутый на flash-диске;
			7. управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений
			8. контроля результатов обновления антивирусного ПО на станциях антивирусной сети.
			9. организации межсерверного обмена согласно расписанию
			10. ограничения канала связи по группам
			11. наличия возможности групповых обновлений
			12. обновлений по защищенному каналу с использованием SSL-сертификатов
			13. организации отложенного обновления
			14. проверки обновлений на выбранных администратором компьютерах/группах перед распространением их на все клиентские компьютеры
			15. автоматического перехода установленного ПО на более новые версии, в том числе с возможностью выбора обновляемых компонентов;
		11. Программные средства управления для всех защищаемых ресурсов, реализованных на платформах ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:
			1. централизованной удаленной установки и деинсталляции программных средств, антивирусных баз и антивирусного ядра на защищаемые узлы сети – в том числе на станции, находящиеся в разных доменах.
			2. создания инсталляционных пакетов для конкретных защищаемых рабочих станций;
			3. выбора и настройки устанавливаемых компонентов до начала установки антивирусного пакета на клиентские части;
		12. Система должна обладать специальной политикой для мобильных пользователей (ноутбуки), при применении которой, мобильные пользователи должны иметь возможность редактирования настроек антивирусного пакета и обновления через Интернет при отсутствии доступа к антивирусному серверу. Применение политики должно происходить через Web-интерфейс, без необходимости использования файлов конфигурации типа \*.xml.
		13. Система управления должна поддерживать возможность:
			1. создания точки восстановления перед установкой антивирусного пакета на защищаемые рабочие станции и сервера;
			2. восстановления удаленных станций.
		14. Система должна поддерживать множественную возможность установки своих компонентов на защищаемые рабочие станции – в том числе с помощью:
			1. прямого их указания в системе управления в результате сканирования локальной сети, Microsoft Active Directory,
			2. политик Microsoft Active Directory
			3. установки с помощью дистрибутива, содержащего все компоненты защиты
			4. рассылки инсталляционных файлов из системы управления по электронной почте
			5. возможностей службы распределенной файловой системы (DFS).
		15. Система должна поддерживать возможность настройки правил автоматического распределения станций по пользовательским группам, а также возможность изменения первичной группы при автоматическом подтверждении доступа станций к антивирусному серверу
		16. Система управления должна обладать возможностью встроенного автоматического резервного копирования критически важных данных и конфигурации антивирусного сервера по заранее заданному расписанию, а также опцию восстановления сервера из резервной копии без использования файлов конфигурации типа \*.xml.
		17. Система должна иметь возможность минимизации трафика:
			1. за счет применения специальных алгоритмов сжатия;
			2. ограничения трафика по пропускной способности и по времени в определенных IP-подсетях.
		18. Система должна иметь возможность интеграции с платформой Microsoft® Network Access Protection (NAP), обеспечивающей автоматическую систему реагирования на инциденты безопасности.
		19. Система должна иметь возможность выбора уровня подробности протоколирования своих компонентов. cистема управления должна иметь возможность загрузки архивированных файлов журнала работы всех антивирусных серверов иерархической сети
		20. В целях ограничения использования серверного пространства должна иметься возможность ротации файлов журнала антивирусного сервера по времени (час, день, неделя)
		21. Система управления должна обеспечивать защиту от несанкционированного доступа. Авторизация должна обеспечиваться парой логин/пароль.
		22. Администраторы Системы должны иметь возможность авторизации с помощью ActiveDirectory, LDAP, RADIUS, PAM. Система управления должна иметь возможность предварительного тестирования настроек авторизации внешних администраторов Active Directory, LDAP и RADIUS
		23. Система должна иметь журнал аудита действий администраторов Системы, позволяющий просматривать журнал событий и изменений, осуществленных администраторами при помощи системы управления.
		24. Система должна обеспечивать:
			1. возможность экспорта выбранных файлов из карантина рабочей станции и/или файлового сервера на антивирусный сервер для дальнейшего анализа;
			2. возможность задания групповых политик в зависимости от группы IP-адресов.
			3. возможность просмотра новостей безопасности, в том числе информирующих об актуальных угрозах
		25. В случае включения какого-либо компонента Системы в единую систему управления антивирусной защиты локальной сети:
			1. обновления компонента Системы должны происходить через сервер обновления системы управления антивирусной защиты;
			2. статистика работы компонентов Системы должна:
				1. собираться на сервере системы управления антивирусной защиты;
				2. быть доступной с любой операционной системы, поддерживающей браузеры Mozilla Firefox, Internet Explorer, Safari, Opera без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения за исключением устанавливаемого автоматически с антивирусного сервера модуля, необходимого для отображения статистики.
				3. Иметь возможность экспорта в формат PDF
				4. Иметь возможность отправки по по электронной почте согласно расписанию работы антивирусного сервера
		26. Система должна обеспечивать реализацию следующих функциональных возможностей по обновлению:
			1. получения ежедневных обновлений вирусных баз не менее 10 раз в сутки независимо от того, рабочий, либо выходной день, что должно подтверждаться созданным Системой отчетом (файлом протокола). Система также должна поддерживать возможность получения экстренных обновлений, связанных с выходом новых типов вредоносного ПО, а также возможность мгновенного распространения этих обновлений;
			2. возможность множественности путей обновления, в том числе по каналам связи и на съемных электронных носителях информации;
			3. возможность обновления через прокси-серверы, в том числе прокси-серверы MS ISA/TMG.
			4. проверка целостности и подлинности обновлений средствами электронной цифровой подписи.
			5. обновления компонентов и вирусных баз по защищенному каналу, с использованием протокола HTTPS.
		27. В случае размещения антивирусных серверов во внутренней сети без доступа к сети Интернет получение обновлений должно быть возможно с помощью специальной утилиты автономной загрузки репозитория;
		28. Система должна иметь возможность перезагрузки защищаемой станции через систему управления
		29. Система должна иметь возможность шифрования трафика между серверами и защищаемыми рабочими станциями в целях предотвращения утечки конфиденциальной информации.
	3. **Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows**
		1. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
			1. осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях.
		2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов:
		3. Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствие требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна обеспечивать защиту рабочих станций под управлением операционных систем:
			1. Microsoft Windows XP Professional;
			2. Microsoft Windows 7;
			3. Microsoft Windows 8.1;
			4. Microsoft Windows 10.
		4. Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.
		5. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур.
		6. Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов.
		7. В случае наличия системы централизованного управления права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля.
		8. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав.
		9. В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
		10. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.
		11. Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:
			1. поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
			2. непрерывное фоновое сканирование в целях нейтрализации активных угроз
			3. проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;
			4. проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
			5. блокировку опасных макросов VBA в реальном времени;
			6. защиту от вредоносных сценариев, загружаемых с Web-страниц;
			7. защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана;
			8. проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО;
			9. защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных носителей информации, локальным файлам и каталогам, сайтам в сети Интернет;
			10. ограничения доступа к сети Интернет или к компьютеру в определенный момент времени по расписанию
			11. помещение найденных зараженных файлов в специальное место на жестком диске -«карантин»;
			12. просмотр местоположения станций и серверов на карте, если заданы географические координаты станции
			13. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
			14. запуск задач по расписанию и/или сразу после загрузки операционной системы;
			15. возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке.
		12. Система защиты рабочих станций должна обеспечивать проверку протоколов:
		13. HTTP;
		14. IMAP, SMTP, POP3 независимо от используемого почтового клиента;
		15. NNTP (только проверка на вирусы), независимо от почтового клиента.
		16. Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством:
		17. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
		18. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.
		19. В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
		20. Система должна обеспечивать защиту от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) с помощью превентивной защиты, отслеживающей попытки внедрения вредоносных файлов
		21. В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.
	4. **Требования к программным средствам антивирусной защиты рабочих станций и домашних компьютеров под управлением ОС семейства Microsoft Windows, не входящих в систему централизованного управления**
		1. Программные средства системы защиты (далее Системы) должны обеспечивать реализацию следующих функциональных возможностей:
			1. осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях;
			2. создание резервных копий папок, указанных пользователем, а также восстановление данных из хранилища - в том числе самим пользователем.
		2. Система используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствие требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна обеспечивать защиту рабочих станций под управлением операционных систем:
			1. Microsoft Windows XP;
			2. Microsoft Windows 7;
			3. Microsoft Windows 8.1;
			4. Microsoft Windows 10.
		3. В целях противодействия вредоносным программам, блокирующим запуск известного ПО - для установки системы защиты не должна требоваться установка стороннего инсталлятора - включая Microsoft Windows Installer, либо использование служб, дополнительных к ранее используемым.
		4. В связи с необходимостью автоматизации развертывания системы защиты установка должна быть возможна в том числе в режиме командной строки - указанием необходимых параметров установки. В том числе установки в фоновом режиме, необходимости перезагрузки и состава устанавливаемых компонент;
		5. В связи с возможными ограничениями канала доступа в сеть Интернет установка системы защиты должна быть возможной без доступа в сеть Интернет - дистрибутив должен содержать все компоненты системы защиты, а также базы данных признаков вредоносных программ и вредоносных ресурсов сети Интернет, доступ к которым может регулироваться системой защиты.
		6. Для работы системы защиты не должны использоваться внешние библиотеки, а также среда .Net Framework, целостность которых не находится под контролем системы самозащиты и компрометация которых может привести к ошибкам отображения информации системы защиты или иным проблемам, связанным с интерфейсом системы защиты
		7. С целью противодействия вредоносным программам, запущенным на компьютере, система установки должна быть интегрирована с антируткитом - обнаружение и удаление угроз должно быть доступно во время установки.
		8. Система установки должна поддерживать импорт настроек, содержания карантина и хранилища резервных копий папок, сохраненных после удаления ранее установленного антивируса - в случае наличия совместимости версий.
		9. Дистрибутив, использованный для установки, должен после завершения установки использоваться для автоматического восстановления работы сервисов. В целях поддержания дистрибутива в актуальном состоянии должно быть реализовано инкрементированное обновление установочного пакета. В целях исключения неправомерного доступа к дистрибутиву в целях удаления или изменения доступ должен контролироваться системой самозащиты антивирусной Системы.
		10. Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.
		11. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур.
		12. Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов.
		13. В случае наличия системы централизованного управления права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля.
		14. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав.
		15. Обновление системы защиты должно быть возможно (по выбору администратора системы защиты) с серверов компании поставщика системы защиты, размещенных в сети Интернет, локальной или сетевой папки, компьютеров локальной сети, на которых установлена аналогичная система защиты и создано зеркало обновлений;
		16. В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
		17. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.
		18. По умолчанию система защиты должна работать в так называемом пользовательском (ограниченном) режиме. Пользователю системы, не являющемуся администратором защиты, не должны быть доступны настройки компонентов системы защиты, а также возможность отключения системы защиты. При работе в данном режиме в интерфейсе системы защиты не должны показываться пункт меню или иконка, нажатие на которые открывает окно или раздел интерфейса с настройками системы защиты. Администратор должен иметь возможность ограничить доступ к настройкам с помощью пароля;
		19. Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:
			1. поиск и удаление вредоносных программ всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
			2. обнаружение вредоносных программ, не обнаруживаемых средствами антивирусного ядра, с помощью превентивной защиты, отслеживающей поведение запущенных процессов, а также вредоносных объектов, внедренных в запущенные процессы;
			3. проверки ссылок на видоизменение, скрипты и фреймы;
			4. проверки файлов по ссылкам до скачивания из сети Интернет на локальный компьютер;
			5. проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;
			6. выявления вредоносных объектов в HTML- и PDF-документах;
			7. выявления и анализа «невидимых» IFRAME-элементов на страницах сайтов и HTML-документах;
			8. проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
			9. блокировку опасных макросов VBA в реальном времени;
			10. блокировку перехода по внешним ссылкам в социальных сетях;
			11. защиту от вредоносных сценариев, загружаемых с Web-страниц;
			12. защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана;
			13. проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО;
			14. защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных носителей информации, локальным файлам и каталогам, сайтам в сети Интернет;
			15. помещение найденных зараженных файлов, а также резервных копий объектов, к которым были применены действия, отличные от «Поместить в карантин», в специальное место на жестком диске -«карантин»;
			16. просмотр местоположения станций и серверов на карте, если заданы географические координаты станции;
			17. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
			18. запуск задач по расписанию и/или сразу после загрузки операционной системы;
			19. возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке
			20. защиту возникновения претензий от правообладателей контента путем использования специальной базы данных признаков ресурсов, доступ к которым ограничен по требованию правообладателей.
		20. Администратор системы должен иметь возможность:
			1. настройки правил защиты от намеренных/непреднамеренных действий посредством блокировки доступа к локальным и сетевым ресурсам (локальным файлам и каталогам, сайтам в сети Интернет) для конкретных пользователей;
			2. копировать настройки между учетными записями пользователей;
			3. запрещать возможность отправки заданий на печать;
			4. запрещать возможность передачи данных по сети;
			5. запрещать возможностьизменения системного времени и часового пояса;
			6. отключать ранее заданные ограничения для конкретной учетной записи;
			7. назначать месторасположения карантина при обнаружении зараженных файлов на съемных носителей;
			8. используя возможности менеджера карантина, осуществлять повторную проверку объектов, помещенных в карантин;
			9. иметь возможность очистки карантина для отдельного диска.
		21. Система защиты рабочих станций должна обеспечивать проверку протоколов:
			1. HTTP независимо от используемого браузера или иного приложения, получающего трафик;
			2. IMAP, SMTP, POP3 независимо от используемого почтового клиента;
			3. NNTP (только проверка на вирусы), независимо от почтового клиента.
		22. Система защиты рабочих станций должна обеспечивать проверку почтовых сообщений, передаваемых по протоколу MAPI для Microsoft Outlook 2000 (Outlook 9)/2002 (Outlook 10 или Outlook XP)/2003 (Outlook 11)/2007/2010/2013.
		23. Система защиты рабочих станций должна автоматически обеспечивать проверку трафика передаваемого по поддерживаемым системой защиты протоколам:
			1. вне зависимости от порта, через который передается трафик - без необходимости указания списка проверяемых портов для конкретных протоколов;
			2. включая проверку трафика, передаваемого по зашифрованному соединению SSL.
		24. Система защиты рабочих станций должна обеспечивать фильтрацию трафика в мгновенных сообщениях Mail.Ru Agent, ICQ, Jabber, QIP, Pidgin и другие, включая антивирусную проверку пересылаемых вложений, а также автоматическое удаление из сообщений ссылок, ведущих на вредоносные и фишинговые сайты.
		25. Система защиты рабочих станций должна обеспечивать фильтрацию выдачи результатов поисковых систем Google, Yandex, Yahoo!, Bing, Rambler с показом только безопасных с точки зрения поисковых систем и системы защиты ресурсов.
		26. Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством:
			1. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
			2. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы;
			3. непрерывного фонового сканирования и нейтрализации активных угроз. В том числе в критических областях Windows, оперативной памяти, запущенных процессах, MBR/VBR дисков, BIOS;
			4. проверки ссылок и файлов с помощью репутационного сервиса облачной защиты - в том числе с помощью базы данных алгоритмов работы вредоносных программ.
		27. В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
		28. С целью защиты от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) Система должна:
			1. обеспечивать защиту критически важных частей системы (в том числе папок и ветвей реестра) от модификаций вредоносными программами, в том числе блокировать попытки:
				1. изменения вредоносными программами загрузочных областей диска;
				2. изменения нежелательным образом пользовательских файлов (в том числе действия троянцев-шифровальщиков) ;
				3. изменения файла HOSTS;
				4. добавления новых задач в логику работы операционной системы;
				5. изменения правил запуска ранее установленных программ;
				6. измения параметров работы системных служб, в том числе процесса создания резервных копий файлов;
				7. загрузки новых или неизвестных драйверов без ведома пользователя, установки новых виртуальных устройств, загрузки в браузер вредоносных плагинов, в том числе блокировщиков браузера;
				8. автозапуска вредоносных программ;
				9. получения низкоуровневого доступа к диску;
				10. регистрации вредоносных программ в реестре для последующего запуска;
				11. отключения безопасного режима Windows путем блокировки изменения реестра;
				12. сокрытия присутствия троянской программы в контролируемой системе в виде руткита.
			2. блокировать попытки установления каналов связи между вредоносным ПО, ранее установленным на компьютер и удаленными серверами злоумышленников;
			3. с помощью превентивной защиты, отслеживающей работу всех процессов системы в поисках действий, характерных для процессов вредоносных программ и не позволяющей вредоносным объектам внедриться в процессы других программ или каким-либо способом разместить вредоносные файлы в защищаемой системе, выявлять и прекращать работу вредоносных, подозрительных или ненадежных сценариев и процессов;
			4. обеспечивать защиту от эксплойтов (программ, эксплуатирующих как уже известные, так и еще неизвестные уязвимости) путем внедрения специального модуля защиты в контролируемые процессы;
			5. ограничивать время работы конкретного сотрудника на защищаемом компьютере - с целью исключения доступа у компьютеру в остальное время неопределенного круга лиц. Система ограничения доступа должна позволять:
				1. задавать время работы на компьютере для выходных и будних дней для каждого сотрудника, а также ограничения по доступу в сеть Интернет;
				2. задавать суммарное время работы на компьютере для конкретного сотрудника;
				3. автоматически блокировать доступ к защищаемому компьютеру в ночное время.
			6. ограничивать доступ к определенным ресурсам сети Интернет - согласно белым и черным спискам ресурсов сети, предопределенным группам ресурсов;
			7. ограничивать доступ к определенным файлам и папкам - с указанием типа доступа объектам (блокировать доступ или разрешать только чтение);
			8. обеспечивать возможность использования на защищаемом компьютере только устройств, входящих список разрешенных. Администратор Системы должен иметь возможность:
				1. контроля доступа к таким типам устройств, как дисковые накопители, приводы DVD/CD-ROM, клавиатуры, компьютерные мыши, сетевые карты, игровые устройства, USB-устройства;
				2. импорта и экспорта правил использования устройств (в том числе с помощью функционала управления удаленными компьютерами антивирусной сети), а также формирования правил блокировки шин и классов устройств, создания списка разрешенных устройств для заблокированных шин и классов устройств;
				3. задать уровень доступа к устройству осуществляется в форме полного запрета доступа всем процессам операционной системы или в форме интерактивного режима, в котором пользователю выводится оповещение о попытке доступа к устройству. Для устройств. с файловой системой администратор Системы должен иметь возможность задать тип доступа - разрешать полный доступ к устройству или доступ только на чтение.
			9. обеспечивать возможность полного запрета использования USB-устройств и CD/DVD-приводов;
			10. обеспечивать создание резервных копий папок, указанных пользователем, а также восстановление данных из хранилища как системой защиты, так и самим пользователем в любой момент времени.
		29. модуль превентивной защиты должен:
			1. поддерживать возможность создания профилей - групп настроек, применяемых пользователем или администратором защищаемой системы - как для системы превентивной защиты в целом, так и для конкретных приложений с целью исключения потенциальных конфликтов при их работе.
		30. система создания резервных копий папок должна поддерживать возможность:
			1. выбора защищаемых каталогов;
			2. выбора диска для хранения защищаемых копий;
			3. настройки расписаний копирования;
			4. создания защищенных копий по требованию.
		31. С целью ускорения проверки Система должна поддерживать возможность исключения из проверки различными компонентами системы защиты:
			1. данных, передаваемых по защищенным протоколам (в том числе HTTPS), а также трафика доверенных приложений (имеющих валидную цифровую подпись) ;
			2. файлов и папок;
			3. ресурсов сети Интернет;
			4. почтовых адресов;
			5. доверенных программ;
		32. С целью ускорения проверки Брандмауэр (файрвол) должен поддерживать **базу** доверенных приложений, а также позволять создавать правила работы для приложений.
		33. В случае отсутствия централизованного управления системой защиты Система защиты рабочей станции должна поддерживать возможность удаленного управления Системами защиты, установленными на компьютерах в пределах одной локальной сети.
		34. Подсистема показа статистики Системы защиты должна:
			1. отображать время возникновения (детектирования) угроз;
			2. списки запрещенных сайтов, доступ к которым был запрошен с защищаемого компьютера.
		35. Подсистема статистики должна иметь возможность отображения только необходимых для анализа сообщений - в том числе создания выборки сообщений отдельных компонентов системы защиты, сообщений с определенными кодами
		36. В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.
	5. **Требования к программным средствам антивирусной защиты рабочих станций Linux**
		1. Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
		2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.
		3. Система, используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствие требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна обеспечивать защиту ресурсов рабочих станций функционирующих под управлением операционных систем:
			1. Debian GNU/Linux 7;
			2. RedHat Enterprise Linux 6;
			3. Ubuntu 14;
			4. CentOS 6;
			5. CentOS 7;
			6. AstraLinux 1.6.
		4. Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью универсального пакета для UNIX систем, независимого от типа и версии используемой операционной системы, репозитория или пакета, рассчитанного на работу с используемым в ОС менеджером пакетов
		5. Установка и обновление Системы должны быть возможны как через средства командной строки, так и с помощью графического инсталлятора.
		6. Система установки должна включать возможность автоматической установки модулей, необходимых для компонентов Системы.
		7. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности работы. При этом, в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках имеющихся у них прав.
		8. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением заданных файловых областей.
		9. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
			1. поиск и удаление вирусов всех известных типов в файлах;
			2. антивирусного сканирования ресурсов сервера как по команде администратора, так и по расписанию, заключающегося в однократной полной или выборочной проверке на наличие угроз объектов;
			3. помещения найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа;
			4. автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
			5. запуска задач по расписанию и/или сразу после загрузки операционной системы;
			6. настройки расписания сканирования с указанием параметров запуска.
		10. Управление программой должно осуществляться как непосредственно через конфигурационные файлы, так и через графический интерфейс, реализованный для операционных систем типа Linux. Система управления должна поддерживать возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, действий по отношению к вредоносным объектам различных типов.
		11. Администратор системы должен иметь возможность:
			1. Определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;
			2. определять типы проверяемых файлов, в том числе с использованием масок;
			3. задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения;
			4. управлять детализацией протоколов антивирусной проверки;
			5. просматривать информацию об используемом ключевом файле и его владельце;
			6. запускать периодическую проверку в приоритетном или в фоновом режиме;
	6. **Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows**
		1. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
			1. Осуществление антивирусной защиты на серверах, включая защиту от руткит-технологий.
		2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.
		3. Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствие требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна обеспечивать защиту серверов под управлением операционных систем:
			1. Microsoft Windows Server 2003;
			2. Microsoft Windows Server 2008;
			3. Microsoft Windows Server 2012;
			4. Microsoft Windows Server 2016.
		4. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
		5. Антивирусное программное обеспечение должно по умолчанию иметь оптимальные настройки с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках имеющихся у них прав.
		6. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением системы.
		7. В Системе должна быть реализована возможность выбора приоритета сканирования, а также остановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
		8. Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
		9. Система должна обеспечивать:
			1. поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
			2. проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
			3. блокировку опасных макросов VBA в реальном времени;
			4. защиту от вредоносных сценариев, загружаемых с веб-страниц;
			5. помещение найденных зараженных файлов в специальное место на жестком диске —«карантин»;
			6. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
			7. запуск задач по расписанию и/или сразу после загрузки операционной системы.
		10. Система защиты серверов под управлением семейства ОС Microsoft Windows должна обеспечивать реализацию следующих функциональных возможностей:
			1. проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов посредством:
				1. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
				2. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.
		11. В Системе должна быть реализована самозащита для всех ее объектов, в том числе критических файлов, процессов, окон, ключей и прочего, от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
	7. **Требования к программным средствам антивирусной защиты файловых серверов UNIX**
		1. Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
		2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных файлов всех типов.
		3. Система, используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствие требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна обеспечивать защиту ресурсов серверов, использующих Samba версий 3.0.x - 3.6.x, и функционирующих под управлением операционных систем:
			1. FreeBSD 10.3;
			2. Debian GNU/Linux 7;
			3. RedHat Enterprise Linux 6;
			4. Ubuntu 14;
			5. CentOS 6;
			6. CentOS 7;
			7. AstraLinux 1.6.
		4. Интеграция Системы с Samba должна осуществляться с помощью модуля VFS (Virtual File System).
		5. В случае использования версий Samba, отличных от вышеперечисленных, либо Samba для 64-битных платформ семейства Linux должна существовать возможность компиляции модулей интеграции из исходных кодов.
		6. Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью универсального пакета для UNIX систем, независимого от типа и версии используемой операционной системы, репозитория или пакета рассчитанного на работу с используемым в ОС менеджером пакетов
		7. Установка и обновление Системы должны быть возможны как через средства командной строки, так и с помощью графического инсталлятора.
		8. Система установки системы должна включать возможность автоматической установки модулей, необходимых для установки необходимых компонентов.
		9. Компоненты системы должны иметь возможность управления использованием серверных ресурсов при выполнении сканирования файлового пространства.
		10. В Системе должна быть реализована возможность задания приоритета антивирусного сканирования.
		11. Система должна поддерживать возможность порождения нескольких одновременно действующих процессов проверки.
		12. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы настройки. При этом, в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователем в рамках имеющихся у них прав.
		13. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением заданных файловых областей.
		14. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
			1. поиск и удаление вирусов всех известных типов в файлах;
			2. антивирусного сканирования ресурсов сервера, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде администратора, так и по расписанию;
			3. антивирусной проверке «на лету» файлов, загружаемых как на сервер, так и с него;
			4. помещения найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа;
			5. автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
			6. запуска задач по расписанию и/или сразу после загрузки операционной системы;
			7. настройки расписания сканирования с указанием параметров запуска.
		15. Управление программой должно осуществляться как с помощью веб-интерфейса, так и непосредственно через конфигурационные файлы. Система управления должна поддерживать возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, и действий по отношению к вредоносным объектам различных типов.
		16. Администратор системы должен иметь возможность:
			1. определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;
			2. определять типы проверяемых файлов, в том числе с использованием масок;
			3. задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения.
			4. управлять детализацией протоколов антивирусной проверки;
			5. просматривать результаты антивирусной проверки;
			6. просматривать информацию об используемом ключевом файле и его владельце;
			7. запускать периодическую проверку в приоритетном или в фоновом режиме;
			8. использовать альтернативные языковые файлы**.**
	8. **Требования по комплектности поставки**
		1. В состав Системы должны входить:
			1. программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания;
			2. программные средства защиты пользователей от нежелательных массовых почтовых рассылок – спама;
			3. программные средства централизованного управления, мониторинга и обновления;
			4. обновляемые базы данных сигнатур всевозможных вредоносных программ.
		2. Комплект поставки должен содержать:
			1. необходимый набор серийных номеров либо ключевых файлов;
			2. дистрибутив Системы;
			3. файлы эксплуатационной документации в формате pdf (Adobe Acrobat Reader), в том числе руководство пользователя (администратора). Поставляемая документация должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.
		3. В соответствии с требованиями заказчика комплект поставки ПО должен содержать дистрибутивы продуктов, сертифицированные ФСТЭК России на соответствие требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28) по Профилю защиты средств антивирусной защиты типа «А» второго класса защиты, Профилю защиты средств антивирусной защиты типа «Б» второго класса защиты, Профилю защиты средств антивирусной защиты типа «В» второго класса защиты», Профилю защиты средств антивирусной защиты типа «Г» второго класса защиты.
		Комплект поставки, сертифицированный ФСТЭК России, должен содержать:
		DVD-диск в фирменном конверте, содержащий верифицированные дистрибутивы сертифицированных продуктов
		документацию и материалы в формате PDF для настройки поставляемого программного обеспечения в соответствии с сертифицированными параметрами, приведенными в технической документации;
		формуляр с голографической наклейкой, содержащий эталонные значения контрольных сумм сертифицированных продуктов;
		лицензионный сертификат, удостоверяющий законное приобретение программного изделия;
		заверенную копию сертификата соответствия ФСТЭК России.
	9. **Требования по технической поддержке Системы**
		1. Техническая поддержка должна предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет.
		2. Техническая поддержка должна включать возможность написания специального ПО, предназначенного для устранения последствий воздействия вредоносного ПО на зараженную систему. В том числе утилит расшифровки файлов, если данная операция является возможной
		3. Техническая поддержка должна обеспечивать возможность получения специалистами и пользователями Заказчика информационной помощи по установке Системы и ее компонентов, в том числе:
			1. ответов на вопросы, а также получение инструкций относительно процесса установки и применения программного обеспечения;
			2. ответов на вопросы о наличии проблем в работе программного обеспечения, а также помощи в определение того, является ли данная проблема результатом сбоя программного обеспечения, ошибок настройки или же она вызвана проблемами, связанными с внешними условиями существования или установкой программного обеспечения.
		4. Web-сайт производителя Системы должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов производителя.

**Место предоставления сервиса.**

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование Получателя | Кол-во лицензий ПК, шт. | Кол-во лицензий сервер, шт. |
| 1 | БУЗ РА "Кожно-венерологический диспансер" | 21 | 0 |
| 2 | БУЗ РА "Перинатальный центр" | 65 | 0 |
| 3 | КУЗ РА "Медицинский информационно-аналитический центр" | 0 | 70 |
| 4 | БУЗ РА "Центр медицины катастроф" | 15 | 0 |
| 5 | БУЗ РА "Центр по профилактике и борьбе со СПИД" | 32 | 0 |
| 6 | КУЗ РА "Бюро судебно-медицинской экспертизы" | 1 | 0 |
| 7 | КУЗ РА "Врачебно-физкультурный диспансер" | 11 | 0 |
| 8 | КУЗ РА "Противотуберкулёзный диспансер" | 28 | 0 |
| 9 | КУЗ РА "Психиатрическая больница" | 20 | 0 |
| 10 | БУЗ РА "Центр общественного здоровья и медицинской профилактики" | 6 | 0 |
| 11 | БУЗ РА "Кош-Агачская РБ" | 74 | 0 |
| 12 | БУЗ РА "Майминская РБ" | 168 | 0 |
| 13 | БУЗ РА "Онгудайская РБ" | 94 | 0 |
| 14 | БУЗ РА "Турочакская РБ" | 75 | 0 |
| 15 | БУЗ РА "Улаганская больница" | 94 | 0 |
| 16 | БУЗ РА "Усть-Канская РБ" | 95 | 0 |
| 17 | БУЗ РА "Усть-Коксинская РБ" | 78 | 0 |
| 18 | БУЗ РА "Чемальская РБ" | 55 | 0 |
| 19 | БУЗ РА "Чойская РБ" | 58 | 0 |
| 20 | БУЗ РА "Шебалинская РБ" | 114 | 0 |
| 21 | АУЗ РА "Республиканская стоматологическая поликлиника" | 32 | 0 |
| 22 | АУЗ РА "Стоматологическая поликлиника № 2" | 12 | 0 |
|   | Итого | 1148 | 70 |

1. **Сервис обеспечения информационной безопасности объекта информатизации - Центр обработки данных ГИСЗ РА**
2. **Подсервис системы обеспечения сетевой безопасности.**

В рамках подсервиса должны быть переданы права на Подписку Security Updates на 1 год для UserGate до 50 пользователей с сертификатом ФСТЭК (кластер из 2 нод) в количестве 1 шт.

В рамках подсервиса должны быть переданы права на Подписку Security Updates на 1 год для UserGate до 50 пользователей с сертификатом ФСТЭК в количестве 1 шт.

Подписка должна включать в себя:

обновление UserGate OS.

1. **Подсервис активации сервиса технической поддержки средств защиты информации**

В рамках подсервиса заказчику должны быть предоставлены следующие ключи технической поддержки:

Ключ активации сервиса прямой технической поддержки уровня "Расширенный" для СЗИ Secret Net LSP в количестве 34 шт.

Ключ активации сервиса прямой технической поддержки уровня "Расширенный" для СЗИ Secret Net Studio в количестве 11 шт.

Ключ активации сервиса прямой технической поддержки уровня "Расширенный" для ПАК "Соболь в количестве 18 шт.

Техническая поддержка должна включать:

|  |  |
| --- | --- |
| Характеристика | Показатель |
| Срок действия | 1 год |
| Работа над критичными инцидентами в режиме | 24 х 7 |
| Способ получения консультаций | Телефон, электронная почта, веб-портал |
| Приоритет обслуживания | Высокий |
| Консультирование по дополнительномуфункционалу продукта | Наличие |
| Самостоятельная регистрация и контрольобращений через веб-портал | Наличие |
| Работа над инцидентами в режиме 8х5 (рабочиедни МСК 10:00–18:00) | Наличие |
| Консультирование по установке и использованиюпродукта | Наличие |
| Информирование о доступных обновленияхпродукта по запросу | Наличие |
| Доступ к пакетам обновлений продукта при наличии непрерывной технической поддержки | Наличие |
| Доступ к базе знаний | Наличие |
| Гарантированное время реакции (время передачи инцидента в работу) | критичный – не более 30 минсущественный – не более 45 миннекритичный – не более 1 часа |

1. **Место предоставления сервиса:**

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование Получателя | Наименование подсервиса | Кол-во, шт. |
| 1 | КУЗ РА "МИАЦ" | Подсервис системы обеспечения сетевой безопасности | 1 |
| 2 | КУЗ РА "МИАЦ" | Подсервис активации сервиса технической поддержки средств защиты информации | 1 |

1. **Сервис обеспечения доступности участнику Центра обработки данных ГИСЗ РА**
2. **Подсервис активации сервиса технической поддержки средств защиты информации**
* В рамках подсервиса заказчику должны включать набор услуг технической поддержки – 694 шт.:
* Приём обращений и консультирование по электронной почте с 9:00 до 18:00;
* Приём обращений и консультирование по телефону горячей линии с 9:00 до 18:00;
* Рекомендации по процессу установки продукта в объеме эксплуатационной документации;
* Рекомендации по настройке продукта в объеме эксплуатационной документации;
* Ключ активации сервиса технической поддержки Dallas Lock Linux (СЗИ НСД, СКН) (1 год на 1 рабочую станцию/сервер, основной пакет) 74114-6679-1845 (до 31.12.2024 г.), 694 шт.
* Dallas Lock Linux. Сертифицированный комплект для установки - 1шт.
1. **Подсервис активации сервиса активации сервиса совместной технической поддержки ПК ПМДЗ ViPNet SafeBoot на срок 1 год, уровень – Расширенный**

В рамках подсервиса заказчику должны включать набор услуг технической поддержки – 694 шт.:

• Приём обращений и консультирование по электронной почте с 9:00 до 18:00;

• Приём обращений и консультирование по телефону горячей линии с 9:00 до 18:00;

• Рекомендации по процессу установки продукта в объеме эксплуатационной документации;

• Рекомендации по настройке продукта в объеме эксплуатационной документации;

• Предоставление обновления (hotfix), устраняющего дефекты, выявленные в продукте;

• Предоставление обновления (hotfix), а также всех изменений, производимых в рамках минорной (MINOR) версии ПРОДУКТА (service pack);

• Предоставление новой версии (изменение мажорной (MAJOR) версии, поколения) ПРОДУКТА без взимания дополнительной платы (для ПАК — только программные компоненты);

Восстановление работоспособности (ремонт) вышедшего из строя оборудования (аппаратной платформы ПАК) из состава Продуктов Пользователя в соответствии с гарантийными обязательствами АО «ИнфоТеКС».

* Установочный комплект ПК ПМДЗ ViPNet SafeBoot с сертификационными документами - 1 шт.
1. **Подсервис проведения регламентных работ**

Все нижеперечисленное оборудование и программное обеспечение располагается в ЦОД по адресуг. Горно-Алтайск, пр-т Коммунистический, д. 140.

В рамках подсервиса Заказчику должны быть оказаны следующие услуги:

1. **Регламентное обслуживание активного сетевого оборудования**
	1. **Обслуживание коммутаторов ядра:**

- визуальный осмотр оборудования;

- сверка наличия инвентарных и серийных номеров с инвентарной ведомостью;

- проверка доступа через консоль;

- проверка удаленного доступа через web-интерфейс и ssh;

- резервное копирование настроек;

- контроль кабельных соединений, в том числе подключения всех сетевых интерфейсов в соответствии с кабельным журналом;

- проверка работы стеков/кластеров;

- проверка информации о наличии критических и рекомендуемых обновлений по аппаратным компонентам системы (прошивка/OS);

- проверка работы основного и резервного блоков питания;

- проверка работы LACP;

- анализ нагрузки на процессор, сетевые интерфейсы за прошедший период.

* 1. **Обслуживание коммутаторов доступа:**

- визуальный осмотр оборудования;

- сверка наличия инвентарных и серийных номеров с инвентарной ведомостью;

- проверка доступа через консоль;

- проверка удаленного доступа через web-интерфейс и ssh;

- резервное копирование настроек;

- контроль кабельных соединений, в том числе подключения всех сетевых интерфейсов в соответствии с кабельным журналом;

- проверка работы стеков/кластеров;

- проверка информации о наличии критических и рекомендуемых обновлений по аппаратным компонентам системы (прошивка/OS);

- проверка работы основного и резервного блоков питания;

- проверка работы LACP;

- анализ нагрузки на процессор, сетевые интерфейсы за прошедший период.

1. **Регламентное техническое обслуживание кластеров ПК СВ Брест**
	1. **Обслуживание фронтальной машины и вычислительных нод:**

- визуальный осмотр оборудования;

- сверка наличия инвентарных и серийных номеров с инвентарной ведомостью;

- проверка индикации об ошибках;

- проверка параметров в подсистеме мониторинга и диагностики;

- подключение к iDRAC, просмотр состояния компонентов сервера, проверка журнала логов (на ошибки, предупреждения);

- резервное копирование настроек;

- проверка информации по дискам в RAID массивах;

- контроль кабельных соединений;

- проверка информации о наличии критических и рекомендуемых обновлений по аппаратным компонентам системы (микрокод);

- проверка работы основного и резервного блока питания;

- проверка работы LACP;

- анализ нагрузки на сервер за прошедший период, сравнение с предыдущими периодами;

- проверка конфигурации оборудования и соответствия данным, указанным в документах на оборудование;

- смена пароля на iDRAC;

- проверка наличия СДЗ.

* 1. **Обслуживание сервера хранения данных:**

- визуальный осмотр оборудования;

- сверка наличия инвентарных и серийных номеров с инвентарной ведомостью;

- подключение к Web-консоли, просмотр состояния компонентов СХД и дисков, проверка журнала логов (на ошибки, предупреждения);

- резервное копирование настроек;

- проверка объема доступного места в пулах;

- проверка информации по дискам в RAID массивах;

- контроль кабельных соединений;

- проверка информации о наличии критических и рекомендуемых обновлений по аппаратным компонентам системы (микрокод);

- проверка работы основного и резервного блока питания;

- анализ нагрузки на СХД, массивы, сетевые интерфейсы за прошедший период, сравнение с предыдущими периодами, анализ использования аппаратных компонентов и анализ динамики изменения остатка свободного места по пулам;

- проверка конфигурации оборудования и соответствия данным, указанным в документах на оборудование;

- смена пароля на Web-консоль.

* 1. **Обслуживание гипервизора:**

- проверка подключения к фронтальной машине ПК СВ Брест;

- проверка входа в web-интерфейс OpenNebula;

- смена пароля администратора;

- проверка доступности вычислительных нод;

- проверка наличия ошибок подключения к вычислительным нодам;

- проверка доступности разделов IMAGE и STORAGE на СХД;

- проверка миграции виртуальных машин;

- проверка автостарта виртуальных машин;

- создание актуальных снапшотов ВМ;

- удаление не актуальных снапшотов;

- просмотр журнала ВМ на наличие ошибок.

1. **Регламентное обслуживание сети ViPNet**
	1. **Обслуживание ViPNet Administrator:**

- сверка наличия инвентарных и серийных номеров с инвентарной ведомостью;

- проверка наличия и контроль работоспособности СЗИ от НСД, СДЗ и антивируса;

- контроль кабельных соединений;

-контроль настроек ПО ЦУС, УКЦ;

- создание резервной копии конфигурации;

- проверка сроков действия сертификатов пользователей;

- проверка логической конфигурации защищенной сети.

- обеспечение межсетевого взаимодействия сети 1721 с сетями Название владельца сети, номер сети, в том числе:

* настройка маршрутизаци;
* создание и обмен доверенным способом межсетевым мастер-ключом;
* выбор сетевые узлы, которые будет участвовать в межсетевом взаимодействии;
* приемка ответного экспорта от доверенной сети;
* проверка доступности узлов доверенной сети;
* проверка доступность ресурсов.
	1. **Обновление Администратора**

- Создание резервной копии настроек и базы данных ЦУС и УКЦ;

- Обновление серверной и клиентской части ЦУС;

- Задать и проверить настройки подключения к SQL-серверу;

- Обновление УКЦ;

- Проверка работоспособности УКЦ и ЦУС;

- Демонстрация работоспособности заказчику.

* 1. **Обслуживание ПАК ViPNet Coordinator:**

- визуальный осмотр оборудования;

- сверка наличия инвентарных и серийных номеров с инвентарной ведомостью;

- контроль кабельных соединений, в том числе подключения всех сетевых интерфейсов в соответствии с кабельным журналом;

- проверка доступа через консоль;

- проверка удаленного доступа через web-интерфейс и ssh;

- проверка правил межсетевого экрана с эталонной конфигурацией;

- проверка работы failover;

- проверка работы LACP;

- анализ нагрузки на процессор, сетевые интерфейсы за прошедший период.

* 1. **Обновление ПО ПАК ViPNet Coordinator HW1000 4.x до крайней сертифицированной версии:**

- Создание экспорта справочно-ключевой информации и настроек обновляемого программно-аппаратного комплекса;

- Запись флэш накопителя с новой сертифицированной версией;

- Обновление программно-аппаратного комплекса;

- Проверка корректности обновления программно-аппаратного комплекса;

- Проверка доступности сетевых ресурсов;

- Демонстрация работоспособности обновленного программно-аппаратного комплекса заказчику.

* 1. **Обновление ПО ПАК ViPNet Coordinator HW1000 C 4.x до крайней сертифицированной версии:**

- Создание экспорта справочно-ключевой информации и настроек обновляемого программно-аппаратного комплекса;

- Запись флэш накопителя с новой сертифицированной версией;

- Обновление программно-аппаратного комплекса;

- Проверка корректности обновления программно-аппаратного комплекса;

- Проверка доступности сетевых ресурсов;

- Демонстрация работоспособности обновленного программно-аппаратного комплекса заказчику.

* 1. **Обновление ПО ПАК ViPNet IDS NS1000 3.x до крайней сертифицированной версии:**

- Загрузка на флэш-накопитель актуальной сертифицированной версии ПО;

- Обновление с флэш-накопителя ПО на ПАК ViPNet IDS NS;

- Смена пароля локального администратор;

- Настройка времени, даты и часового пояса;

- Настройка управляющего интерфейса;

- Настройка шлюза по умолчанию;

- Настройка интерфейсов для захвата трафика;

- Подключение к веб-интерфейсу и смена пароля администратора;

- Установка и активация лицензии;

- Загрузка актуальных баз разрешающих правил;

- Загрузка базы Malware detection;

- Настройка защищаемой сети (после предоставления адресов заказчиком);

- Демонстрация работоспособности.

* 1. **Регламентное обслуживание СОВ ViPNet IDS:**

- визуальный осмотр оборудования;

- сверка наличия инвентарных и серийных номеров с инвентарной ведомостью;

- контроль кабельных соединений, в том числе подключения всех сетевых интерфейсов в соответствии с кабельным журналом;

- подключение к Web-консоли, просмотр состояния компонентов, проверка журнала логов (на ошибки, предупреждения);

- проверка настройки параметров обработки трафика защищаемой сети;

- контроль работоспособности ViPNet IDS через самотестирование;

- создание резервной копии конфигурации ViPNet IDS;

- обновление сигнатур атак систем обнаружения вторжений (атак) из базы решающих правил производителя;

- смена пароля администратора на web-интерфейс.

1. **Регламентное обслуживание межсетевых экранов UserGate**

- визуальный осмотр оборудования;

- сверка наличия инвентарных и серийных номеров с инвентарной ведомостью;

- проверка удаленного доступа через web-интерфейс;

- резервное копирование настроек;

- контроль кабельных соединений, в том числе подключения всех сетевых интерфейсов в соответствии с кабельным журналом;

- проверка работы кластера;

- проверка работы LACP;

- проверка срока действия лицензии;

- проверка правил межсетевого экрана с эталонной конфигурацией;

- анализ нагрузки на процессор, сетевые интерфейсы за прошедший период.

1. **Регламентное обслуживание сервера управления антивируса Dr.Web:**

- проверка подключения к web-интерфейсу;

- проверка срока действий лицензий;

- проверка доступности обновлений антивирусных баз;

- проверка актуальности версии ПО;

- проверка состояния агентов;

- проверка наличия ошибок;

- проверка клиентских событий;

- проверка наличия ошибок;

- проверка клиентских событий;

- проверка наличия сетевых атак;

- проверка наличия вирусной активности;

- создание резервной копии;

- проверка корректности и работоспособности создаваемых резервных копий.

1. **Подсервис по сопровождению подсистемы информационной безопасности ЦОД**

Все нижеперечисленное оборудование и программное обеспечение располагается в ЦОД по адресуг. Горно-Алтайск, пр-т Коммунистический, д. 140.

1. В рамках подсервиса Заказчику должны быть оказаны услуги по сопровождению системы информационной безопасности и консультации по работе оборудования, перечисленного в Таблице 4 настоящего ТЗ:

Таблица 4

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование оборудования** | **Количество** |
| 1 | Коммутатор доступа Huawei S5735-S24T4X | 16 |
| 2 | Коммутатор ядра Huawei 6730-H48X6C | 4 |
| 3 | Межсетевой экран UserGate D200 | 3 |
| 4 | ПАК ViPNet Coordinator HW1000  | 8 |
| 5 | ПАК ViPNet IDS NS1000  | 2 |
| 6 | Коммутатор Eltex MES5316A | 2 |
| 7 | СХД Infortred ESDS 2012RC | 1 |
| 8 | Сервер Progres-R | 1 |
| 9 | Сервер Depo Storm 3450A2 | 2 |
| 10 | СХД Dell ME-4012 | 1 |
| 11 | Сервер Dell R-440 | 2 |
| 12 | Сервер Dell R-940 | 2 |
| 13 | Сервер Dell R-640 | 3 |
| 14 | СХД Dell ME 4012 | 1 |

2. Техническое сопровождение включает в себя выполнение заявок и выезды по местонахождению оборудования с целью устранения сбоев, осуществления перенастройки оборудования и ПО, перечисленного в Таблице 5:

Таблица 5

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование заявки** | **Выполняемый перечень работ** |
| 1 | Заявка на активное сетевое оборудование | Одна заявка соответствует одной единице оборудования или программного обеспечения.Возможные типы заявок:* 1. Настройка параметров системы безопасности: создание новых учетных записей;
	2. Настройка параметров системы безопасности: настройка привилегий учетным записям;
	3. Настройка параметров системы безопасности: настройка пароля для консоли;
	4. Настройка параметров системы безопасности: настройка пароля для ssh.
	5. Настройка системного времени (ntp);
	6. Настройка интерфейсов стекирования;
	7. Конфигурирование сетевых интерфейсов: настройка интерфейса управления;
	8. Конфигурирование сетевых интерфейсов: настройка шлюза по умолчанию;
	9. Конфигурирование сетевых интерфейсов:настройка работы порта в режиме access;
	10. Конфигурирование сетевых интерфейсов: настройка работы порта в режиме trunk;
	11. Конфигурирование сетевых интерфейсов: настройка скорости передачи данных на сетевых интерфейсах;
	12. Конфигурирование сетевых интерфейсов:настройка агрегирования сетевых интерфейсов;
	13. Конфигурирование сетевых интерфейсов:настройка MTU сетевых интерфейсов;
	14. Конфигурирование сетевых интерфейсов:настройка Private VLAN;
	15. Конфигурирование сетевых интерфейсов: настройка контроля широковещательного шторма;
	16. Резервное копирование: создание резервной копии настроек сетевого оборудования;
	17. Резервное копирование: восстановление настроек из резервной копии.
 |
| 2 | Заявка на ПК СВ Брест | Одна заявка соответствует одной единице оборудования или программного обеспечения.Возможные типы заявок:2.1 Создание виртуальной сети;2.2 Настройка виртуальной сети с добавлением VLAN;2.3 Загрузка образа операционной системы \*.iso в среду виртуализации;2.4 Создание виртуального диска;2.5 Создание шаблона виртуальной машины;2.6 Создание виртуальной машины из шаблона;2.7 Добавление дополнительного сетевого интерфейса к ВМ;2.8 Добавление дополнительного виртуального диска;2.9 Изменение характеристик ВМ (количество ЦП, ОЗУ);2.10 Установка qemu-guest-agent в гостевой ОС;2.11 Создание снапшотов ВМ;2.12 Восстановления ВМ из снапшота. |
| 3 | Заявка на серверное оборудование и систему хранения данных | Одна заявка соответствует одной единице оборудования или программного обеспечения.Возможные типы заявок:3.1 Обновление BIOS серверного оборудования;3.2 Обновление IPMI, iDrac серверного оборудования;3.3 Настройка IP-адреса управления IPMI и iDrac на серверном оборудовании;3.4 Настройка учетных записей на серверном оборудовании;3.5 Настройка SNMP и syslog на серверном оборудовании;3.6 Создание RAID-массива на серверном оборудовании;3.7 Настройка IP-адреса управления на системе хранения данных;3.8 Настройка учетных записей на системе хранения данных;3.9 Настройка SNMP и syslog на системе хранения данных;3.10 Создание и модификация RAID-массива системы хранения данных. |
| 4 | Заявка на МЭ UserGate | Одна заявка соответствует одной единице оборудования или программного обеспечения.Возможные типы заявок:4.1 Настройка учетных записей;4.2 Загрузка лицензии;4.3 Экспорт\импорт настроек устройства;4.4 Настройка управления доступом к консоли управления UserGate.4.5 Настройки сети: настройка зон;4.6 Настройки сети: настройка интерфейсов (интерфейс VLAN, bond, bridge);4.7 Настройки сети: настройка маршрутизации;4.8 Настройки сети: настройка DHCP;4.9 Настройки сети: настройка DNS.4.10 Настройка политик сети: настройка правил межсетевого экранирования;4.11 Настройка политик сети: настройка NAT (NAT, DNAT, Порт-форвардинг);4.12 Настройка политик сети: балансировка нагрузки;4.13 Настройка политик сети: настройка пропускной способности;4.14 Настройка политик безопасности и модуля СОВ;4.15 Резервное копирование конфигурации усройств. |
| 5 | Заявка на Сеть ViPNet | Одна заявка соответствует одной единице оборудования или программного обеспечения.Возможные типы заявок:6.1 Отправка на сетевые узлы обновлений справочников и ключей.6.2 Резервное копирование и восстановление данных программы ViPNet 6.3 Настройка параметров сетевых узлов: создание сетевого узла (ViPNet Coordinator);6.4 Настройка параметров сетевых узлов: удаление сетевого узла (ViPNet Coordinator);6.5 Настройка параметров сетевых узлов: изменение связей между сетевыми узлами;6.6 Настройка параметров сетевых узлов: настройка списков DNS- и WINS-серверов;6.7 Настройка параметров сетевых узлов: настройка списка защищенных DNS-серверов и доменных зон;6.8 Настройка параметров сетевых узлов: настройка параметров подключения к внешней сети;6.9 Настройка параметров сетевых узлов: изменение списка групп, в которые входит сетевой узел;6.10 Настройка параметров пользователей: создание пользователя и настройка его параметров;6.11 Настройка параметров пользователей: работа с группами пользователей.6.12 Межсетевое взаимодействие: организация межсетевого взаимодействия;6.13 Межсетевое взаимодействие: связи с объектами доверенных сетей;6.14 Межсетевое взаимодействие: изменение шлюзового координатора своей сети;6.15 Межсетевое взаимодействие: передача межсетевой информации;6.16 Межсетевое взаимодействие: обработка межсетевой информации;6.17 Межсетевое взаимодействие: разрыв межсетевого взаимодействия.6.18 Настройка ПАК ViPNet Coordinator: переинициализация программно-аппаратных комплексов;6.19 Настройка ПАК ViPNet Coordinator: настройка параметров сетевого подключения координатора;6.20 Настройка ПАК ViPNet Coordinator: настройка сетевых интерфейсов Ethernet;6.21 Настройка ПАК ViPNet Coordinator: настройка маршрутизации;6.22 Настройка ПАК ViPNet Coordinator: настройка сетевых фильтров;6.23 Настройка ПАК ViPNet Coordinator: настройка правил трансляции;6.24 Настройка ПАК ViPNet Coordinator: создание резервных копий настроек;6.25 Настройка ПАК ViPNet Coordinator: восстановление настроек из резервной копии. |

3. Прием и оформление заявок от Заказчика осуществляется Исполнителем в режиме 8/5. Для приема заявок Исполнитель должен предоставить Заказчику доступ к порталу приема заявок:

Этапы обработки заявок:

− прием запросов от Заказчика;

− идентификация, классификация, сбор и проверка данных по запросу;

− маршрутизация обращений в рабочие группы специалистов;

− решение инцидентов;

− доведение информации о решении инцидентов до Заказчика.

Регистрация заявок производится средствами порталу приема заявок Исполнителя. При этом средствами портала приема заявок контролируется срок исполнения заявок.

При обращении в службу технической поддержки Исполнителя с запросом на заявку необходимо зафиксировать:

− инициатора обращения, контактные данные;

− объект информатизации;

− обслуживаемая подсистема информационной безопасности;

− время и временной интервал возникновения проблемы;

− описание проблемы (дополнительно: лог-файлы, скриншоты; фотографии).

4. Количество заявок на техническое сопровождение должно быть не более 90 шт. в течение срока действия контракта. В случае невозможности удаленного исполнения заявки, исполнитель должен выполнить выезд по местонахождению оборудования. Количество выездов в период действия контракта должно быть не более 7.

1. **Место предоставления сервиса:**

Таблица 6

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование Получателя | Коэффициент распределения |
| 1 | БУЗ РА "Республиканская больница" | 0,274 |
| 2 | КУЗ РА "Врачебно-физкультурный диспансер" | 0,016 |
| 3 | БУЗ РА "Кожно-венерологический диспансер" | 0,016 |
| 4 | БУЗ РА "Перинатальный центр" | 0,019 |
| 5 | КУЗ РА "Противотуберкулезный диспансер" | 0,017 |
| 6 | КУЗ РА "Психиатрическая больница" | 0,017 |
| 7 | КУЗ РА "Бюро судебно-медицинской экспертизы" | 0,001 |
| 8 | БУЗ РА "Центр медицины катастроф" | 0,003 |
| 9 | БУЗ РА "Центр медицинской профилактики" | 0,009 |
| 10 | БУЗ РА "Центр по профилактике и борьбе со СПИД" | 0,024 |
| 11 | БУЗ РА "Майминская районная больница" | 0,072 |
| 12 | БУЗ РА "Чойская районная больница" | 0,030 |
| 13 | БУЗ РА "Турочакская районная больница" | 0,065 |
| 14 | БУЗ РА "Шебалинская районная больница" | 0,092 |
| 15 | БУЗ РА "Онгудайская районная больница" | 0,053 |
| 16 | БУЗ РА "Кош-Агачская районная больница" | 0,059 |
| 17 | БУЗ РА "Улаганская районная больница" | 0,048 |
| 18 | БУЗ РА "Усть-Канская районная больница" | 0,052 |
| 19 | БУЗ РА "Усть-Коксинская районная больница" | 0,079 |
| 20 | БУЗ РА "Чемальская районная больница" | 0,039 |
| 21 | АУЗ РА "Республиканская стоматологическая поликлиника" | 0,012 |
| 22 | АУЗ РА "Стоматологическая поликлиника №2" | 0,003 |

1. **Сервис обеспечения контроля и управления доступом в ЗКСПД с АРМ**

1. Сервис обеспечения контроля и управления доступом (далее «Сервис»), должен быть разработан и построен на следующих основных принципах:

• Сервис должен быть построен на открытом программном коде или относится к Российскому программному обеспечению;

• Сервис должен работать на свободно распространяемой операционной системе (CentOS или аналог) и для системы мониторинга необходимо использовать компоненты свободно распространяемого программного обеспечения;

• в качестве хранилища данных Сервис должен использовать распространенные системы управления базами данных (MySQL, PostgreSQL и т.д ).;

• Сервис должен обеспечивать автоматический сбор данных от объектов, имеющих верифицированный доступ в ЗКСПД и обладать гибкими возможностями по работе с пороговыми значениями для контролируемых параметров;

• Сервис должен быть масштабируемый как в отношении числа подключаемых объектов, так и в отношении расширения функциональности и информативности собственно подсистемы;

• Сервис должен иметь возможность включения в систему территориально распределенных объектов без ущерба общей функциональности и производительности;

• Сервис должен иметь возможность автоматического обнаружения объектов при попытке получения доступа к ЗКСПД;

• Сервис должен иметь возможность автоматического и ручного режимов отключения конкретного АРМ от доступа в ЗКСПД;

• Сервис должен иметь возможность электронного журналирования всех объектов, имеющих доступ в ЗКСПД и зарегистрированных в системе;

• Сервис должен иметь возможность автоматического уведомления настраиваемого списка лиц о попытках получения доступа незарегистрированным в системе Сервиса объектам;

• Сервис должен иметь три пользовательских WEB интерфейса с единой системой авторизации:

• Мониторинговый интерфейс для руководителей и сотрудников Министерства здравоохранения Республики Алтай и КУЗ РА «МИАЦ» с наиболее значимой агрегированной информацией;

• Пользовательский интерфейс для Руководителя МО с наиболее значимой агрегированной информацией

• Административный интерфейс для подготовленных сотрудников, назначенных Приказом Руководителя МО Системных администраторов (далее «Администратор»).

Требования к Заказчику Сервиса:

- Заказчик обязан предоставить место в существующих телекоммуникационных шкафах МО для установки коммутационного оборудования Исполнителя обеспечивающего функционирование Сервиса. Кол-во устанавливаемого оборудования определяется в результате обследования МО, указанных в Таблице 7.

Требования к единой системе авторизации пользователей Сервиса:

Требования к регистрации АРМ и устройств (объектов) в системе Сервиса:

1. Регистрация объекта в системе:

1.1. Администратор открывает заявку в системе, в заявке указывает исчерпывающие данные по подключаемому в сеть АРМ пользователя:

1.1.1. Ф.И.О. основного пользователя;

1.1.2. Должность основного пользователя;

1.1.3. MAC адрес устройства;

1.1.4. Тип устройства (выбор из раскрывающегося списка);

1.1.5. Адрес места установки устройства (Адрес, этаж, кабинет, доп. информация (например – лабораторный корпус));

1.1.6. Коммутатор системы (ближайший по СКС).

1.2. Администратор открывает заявку в системе, в заявке указывает исчерпывающие данные по подключаемому в сеть общему устройству (например, сетевой принтер):

1.2.1. MAC адрес устройства;

1.2.2. Тип устройства (выбор из раскрывающегося списка);

1.2.3. Адрес места установки устройства (Адрес, этаж, кабинет, доп. информация (например – лабораторный корпус));

1.2.4. Коммутатор системы (ближайший по СКС).

1.3. Созданная заявка в автоматическом режиме направляется на утверждение Руководителю МО, Руководитель МО отклоняет или утверждает заявку.

1.4. Утверждённая заявка попадает в систему, далее автоматически присваивается свободный порт на выбранном Администратором коммутаторе.

1.5. Администратору приходит в интерфейсе системы и дублируется на эл. почту сообщение о требовании включить указанное устройство в сеть в течение суток, либо порт деактивируется и высвобождается для подключения других устройств. Если включаемое устройство является АРМом, в предупреждении указывается требование установить на АРМ клиента системы мониторинга, в противном случае при включении устройства в сеть и отсутствии клиента на АРМ, порт деактивируется и высвобождается для подключения других устройств. В системе предусмотрена возможность удаления поданной заявки для деактивации порта ранее чем через сутки.

1.6. При соблюдении условий указанных в п.1.5. порт активируется и устройство встаёт в систему мониторинга, получает доступ в ЗКСПД.

1.7. Для внесения изменений в существующую систему Администратор может подать заявку и изменить данные устройства, кроме MAC адреса устройства, такая заявка в обязательном порядке в автоматическом режиме направляется на утверждение Руководителю МО на согласование, при положительном решении изменения в системе регистрируются автоматически.

Требования к отчетности Сервиса

В рамках выполнения функций построения отчетности Сервис должен обеспечивать возможность построения следующих типов отчетов:

• на основе данных любого показателя одного объекта или группы объектов мониторинга;

• отчет на основе данных событийной обработки;

• отчет с возможностью фильтрации и последующей группировки представляемых событий по дате, классу, степени критичности;

• возможность формирования аналитических отчетов на основании собираемой системой информации.

• отчеты должны предоставляться по запросу Заказчика в онлайн режиме, но не чаще, чем один раз сутки.

• система отчётности должна иметь возможность формирования и вывода на экран тепловой карты (графическое представление данных, где индивидуальные значения в таблице отображаются при помощи цвета) содержащей данные о кол-ве АРМ и устройств, находящихся в режиме онлайн в заданный период времени.

Требования к режимам функционирования системы

В штатном режиме система мониторинга должна функционировать 24 часа в сутки, 7 дней в неделю, с заданными показателями надежности и с плановыми перерывами для проведения регламентного или разового обслуживания.

Исполнитель осуществляет техническую поддержку работы Сервиса и непрерывно обеспечивает пригодность Сервиса к промышленной эксплуатации, включая:

- проведение аналитики зарегистрированных заявок на доработки Сервиса;

- консультационную поддержку;

- диагностику работоспособности Сервиса;

- поиск и устранение проблем в случае невозможности работы Сервиса в промышленном режиме;

- восстановление работоспособности Сервиса при сбоях.

Таблица 7. Место оказания и количественные показатели сервиса.

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование Получателя | Коэффициент распределения |
| 1 | БУЗ РА "Кожно-венерологический диспансер" | 0,016 |
| 2 | БУЗ РА "Перинатальный центр" | 0,050 |
| 3 | БУЗ РА "Республиканская больница" | 0,295 |
| 4 | БУЗ РА "Центр медицины катастроф" | 0,012 |
| 5 | БУЗ РА "Центр по профилактике и борьбе со СПИД" | 0,025 |
| 6 | КУЗ РА "Бюро судебно-медицинской экспертизы" | 0,001 |
| 7 | КУЗ РА "Врачебно-физкультурный диспансер" | 0,008 |
| 8 | КУЗ РА "Противотуберкулёзный диспансер" | 0,022 |
| 9 | КУЗ РА "Психиатрическая больница" | 0,015 |
| 10 | БУЗ РА "Центр общественного здоровья и медицинской профилактики" | 0,005 |
| 11 | БУЗ РА "Кош-Агачская РБ" | 0,045 |
| 12 | БУЗ РА "Майминская РБ" | 0,098 |
| 13 | БУЗ РА "Онгудайская РБ" | 0,048 |
| 14 | БУЗ РА "Турочакская РБ" | 0,045 |
| 15 | БУЗ РА "Улаганская больница" | 0,065 |
| 16 | БУЗ РА "Усть-Канская РБ" | 0,047 |
| 17 | БУЗ РА "Усть-Коксинская РБ" | 0,037 |
| 18 | БУЗ РА "Чемальская РБ" | 0,033 |
| 19 | БУЗ РА "Чойская РБ" | 0,034 |
| 20 | БУЗ РА "Шебалинская РБ" | 0,065 |
| 21 | АУЗ РА "Республиканская стоматологическая поликлиника" | 0,025 |
| 22 | АУЗ РА "Стоматологическая поликлиника № 2" | 0,009 |

1. **Сервис подключения медицинских организаций к ЗКСПД**
2. Технические требования к цифровым каналам связи.

Технические характеристики каналов должны соответствовать требованиям, изложенным в Рекомендациях МСЭ-Т, Нормах на электрические параметры цифровых каналов и трактов магистральной и внутризоновой первичных сетей, утвержденных Приказом Министерства связи России № 92 от 10.08.1996. Ввод кабеля в здание и монтаж по зданию осуществляется в соответствии с требованиями TIA/EIA-569.

Функционирование каналов должно обеспечиваться 7 дней в неделю, 24 часа в сутки.

Необходимо обеспечить следующие параметры производительности и отказоустойчивости (Таблица 8):

Таблица 8. Параметры производительности и отказоустойчивости

| Параметр | Значение |
| --- | --- |
| Количество одновременно подключенных пользователей | не менее 10 тысяч |
| Время отклика, при полной нагрузке | не более 3 секунд |
| Показатель доступности | 0,997 (режим 365\*24, останов на профилактические работы не более 2 часов в месяц) |
| Время восстановления по аварии (Полный отказ информационной системы в результате технической или эксплуатационной аварии) | не более 24 часов |
| Время восстановления по сбою (Выход из строя одного из резервированных или дублирующих элементов или одного из нескольких элементов одинаковой функциональности) | не более 4 часов |
| Время восстановления по ошибке (Программные и аппаратные неисправности, не влияющие на работу Информационной системы в целом) | по согласованию |

Уровень доступности рассчитывается следующим образом:

где, A – доступность выполнения работ в отчетном периоде;

Ts – время предоставления сервиса за отчетный период, часов;

Td – время недоступности сервиса за отчетный период, часов.

Под отчетным периодом понимается календарный месяц.

В случае если уровень доступности выполнения работ составляет менее 99,97%. Заказчик имеет право требовать от Исполнителя компенсации в соответствии с Таблицей 9. Неполный час округляется следующим образом: 30 мин и более округляется в большую сторону, 29 минут и менее округляется в меньшую сторону.

Таблица 9. Компенсация за отсутствие доступности выполнения работ

|  |  |
| --- | --- |
| Замеряемая доступность (a) (%, ежемесячно) | Перерасчет Ежемесячного платежа (% от начисленного платежа)\* |
| a ≥ 99.970 | 0% |
| 99.970> a ≥99.662 | 7% |
| 99.662>a ≥99.522 | 10% |

Требования по профилю выполнения работ: наличие QoS, не менее 75% трафика класса Real Time, остальной трафик – best-effort.

Задержка распространения пакетов должна составлять не более 100 миллисекунд.

Вариация задержки – 50 ms.

Процент потерянных пакетов – не более 0,0005%.

Интерфейс подключения к коммутирующему оборудованию в МО — Ethernet.

Оператор должен разместить каналообразующее оборудование в помещении узла связи (помещении ввода в соответствии с прилагаемыми этажными планами МО) и обеспечить его подключение к коммутационному оборудованию.

Каналообразующее оборудование должно соответствовать методическим рекомендациям по составу и техническим требованиям к сетевому телекоммуникационному оборудованию учреждений системы здравоохранения для регионального уровня ЕГИСЗ РФ РА, а также функциональные требования к ним, обязательные для создания в 2011-2012 годах в рамках реализации региональных программ модернизации здравоохранения.

Оператор обеспечивает совместимость своего каналообразующего оборудования с коммутационным оборудованием МО.

Оператор обеспечивает круглосуточное дежурство службы технической поддержки и мониторинга за работоспособностью каналов связи, осуществляет приём заявок на восстановление работоспособности.

Граница ответственности за канал связи должна проходить в точках подключения канала связи к коммутаторам распределения МО.

Оператор обеспечивает основной канал на основе волоконно-оптической линии связи, согласно скоростным параметрам, указанным в Таблице 10.

Оператор обеспечивает резервный канал на основе волоконно-оптической линии связи, организуемый по альтернативному от основного канала маршруту (разнесение трасс) согласно скоростным параметрам, указанным в Таблице 10.

Оператор предоставляет резервный канал на основе инфраструктуры мобильного оператора связи по технологии 3G/4G согласно скоростным параметрам, указанным в Таблице 10.

Оператор обеспечивает автоматическое переключение между основным и резервными каналами, исходя из качественных параметров и доступности канала.

Оператор обеспечивает наличие возможности передачи голосового трафика в защищенной закрытой корпоративной сети передачи данных, объединяющей участников, перечисленных в Таблице 11.

Оператор обеспечивает подключение МО к защищенной закрытой корпоративной сети передачи данных, объединяющей объекты РС ЕГИСЗ Республики Алтай для работы с внутриведомственными ресурсами.

Оператор гарантирует, что к организованному защищенному каналу связи VLAN имеют доступ участники ЗКСПД перечисленные в Таблице 9.

Таблица 9. участники ЗКСПД имеющие доступ к организованному защищенному каналу связи VLAN

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование учреждения | Адрес учреждения |
| 1 | БУЗ РА «Кожно-венерологический диспансер» | г. Горно-Алтайск, ул. Чаптынова, 18  |
|  | г. Горно-Алтайск, ул. Социалистическая, 7 |
| 2 | БУЗ РА «Республиканская больница» | г. Горно-Алтайск, пр-т Коммунистический, 140  |
|  | г. Горно-Алтайск, ул. Ленина, 195  |
|  | г. Горно-Алтайск, ул. Чорос-Гуркина, 6  |
|  | г. Горно-Алтайск , пр-т Коммунистический, 170 |
| 3 | БУЗ РА «Перинатальный центр» | г. Горно-Алтайск, ул. Чаптынова, 12 |
| 4 | БУЗ РА «Центр по профилактике и борьбе со СПИД» | г. Горно-Алтайск, ул. Шоссейная, 38 |
| 5 | БУЗ РА «Центр медицины катастроф» | г. Горно-Алтайск, ул. Шоссейная, 36 |
|  | г. Горно-Алтайск, пр-т Коммунистический, 13 |
|  | с. Майма, ул. Ленина, 67/1 |
| 6 | КУЗ РА «Медицинский информационно-аналитический центр» | г. Горно-Алтайск, пр-т Коммунистический, 54 |
| 7 | КУЗ РА «Бюро судебно-медицинской экспертизы» | г. Горно-Алтайск, пр-т Коммунистический, 77 |
| 8 | АУЗ РА «Республиканская стоматологическая поликлиника» | г. Горно-Алтайск, ул. Социалистическая, 19 |
| 9 | АУЗ РА «Стоматологическая поликлиника №2» | г. Горно-Алтайск, пр-т Коммунистический, 105 |
| 10 | БУЗ РА «Майминская РБ» | с. Майма, ул. Строителей, 6 к.1 |
|  |  | с. Майма, ул. Гидростроителей, 44а |
|  |  | с. Майма, ул. Карьерная Алгаир, 10, кв. 80 |
|  |  | с. Майма, ул. Советская, 62 |
| 11 | БУЗ РА «Кош-Агачская РБ» | с. Кош-Агач, ул. Медицинская, 3 |
| 12 | БУЗ РА «Улаганская больница» | с. Улаган, ул. Больничная, 30 |
| с. Акташ, ул. Парковая, 8 |
|  |  | с. Акташ, ул. Пушкина, 11 |
| 13 | БУЗ РА «Турочакская РБ» | с. Турочак, ул. Набережная, 1 |
| 14 | БУЗ РА «Онгудайская РБ» | с. Онгудай, ул. Космонавтов, 84 |
| 15 | БУЗ РА «Усть-Канская РБ» | с. Усть-Кан, ул. Юбилейная, 3 |
|  |  | с. Усть-Кан, ул. Первомайская, 8г |
|  |  | с. Усть-Кан, ул. Ленинская, 34 |
| 16 | БУЗ РА «Усть-Коксинская РБ» | с. Усть-Кокса, ул. Советская, 153 |
| 17 | БУЗ РА «Чемальская РБ» | с. Чемал, ул. Чемальская, 4  |
| 18 | БУЗ РА «Шебалинская РБ» | с. Шебалино, ул. Фёдорова, 24 |
| 19 | БУЗ РА «Чойская РБ» | с. Гусевка, ул. 40 лет Победы, 2а |
| 20 | БУЗ РА "Центр общественного здоровья и медицинской профилактики" | г. Горно-Алтайск, ул. Ленкина, 2 |
| 21 | КУЗ РА «Врачебно-физкультурный диспансер» | г. Горно-Алтайск, ул. Ленкина, 2 |

Оператор гарантирует предоставление до 20 каналов защищённых каналов связи, организованных по технологии 3G/4G для обеспечения доступа планшетных устройств, используемых службой скорой медицинской помощи к серверу управления, находящемуся по адресу г. Горно-Алтайск, пр-т Коммунистический, 140.

По адресу г. Горно-Алтайск, пр-т Коммунистический, 140 Оператор обеспечивает:

- наличие 5-ти различных подсетей с различной ip-адресацией для подключения отдельных отделений Заказчика;

- Бридж интерфейс до 5 портов для работы с глобальной сетью интернет на скорости до 20 Мбит/сек с возможностью зеркалирования трафика.

Требования к Оператору связи

При оказании услуг, выполнении работ Оператор должен:

- в соответствии с правилами оказания услуг связи, утвержденными постановлением Правительства Российской Федерации от 23 января 2006 года №32 и правилами оказания телематических услуг связи, утвержденными постановлением Правительства Российской Федерации от 10 сентября 2007 года №575, в соответствии с требованиями Федерального закона от 07.07.2003 № 126-ФЗ "О связи", Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» и постановления Правительства РФ от 18.02.2005 № 87 "Об утверждении перечня наименований услуг связи, вносимых в лицензии, и перечней лицензионных условий" иметь следующие лицензии: лицензия на телематические услуги связи, лицензия на услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации, лицензия на услуги связи по предоставлению каналов связи на территории Республики Алтай, осуществление предоставления услуг в области шифрования информации, осуществление распространения шифровальных (криптографических) средств, осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации, на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- выполнять работы с требуемым качеством;

- обеспечивать техническую безопасность сети;

- обеспечивать возможности по масштабированию и развитию сети (в пределах цены контракта) с учётом следующих факторов:

а) увеличение технической оснащенности объектов и развития телекоммуникационных технологий;

б) расширение номенклатуры выполняемых работ.

Иметь зарегистрированные в Роскомнадзоре узлы доступа, расположенные в населенных пунктах, в которых расположены Объекты ЗКСПД, указанные в Таблице 10 с соблюдением следующих условий:

а) срок эксплуатации этих узлов не менее 4 лет;

б) постоянно размещенный штатный технический персонал для обслуживания узлов связи без выездных бригад.

- Обладать средствами управления и мониторинга состояния сети, позволяющих предоставлять круглосуточную поддержку Заказчику (24 часа в день, 7 дней в неделю).

Оператор должен обеспечить техническую возможность географического охвата наземными каналами связи учреждений здравоохранения на территории Республики Алтай.

1. Требования к единой защищенной виртуальной сети с целью обеспечения безопасного межсетевого взаимодействия объектов РС ЕГИСЗ Республики Алтай (Extranet VPN).

Нормативно-методическая документация:

При разработке технических требований РС ЕГИСЗ использовались следующие нормативно-методические документы:

Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и защите информации».

Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных».

Методические рекомендации Министерства здравоохранения и социального развития РФ по оснащению медицинских учреждения компьютерным оборудованием и программным обеспечение для регионального уровня единой государственной информационной системы в сфере здравоохранения, а также функциональные требования к ним.

Методические рекомендации Министерства здравоохранения и социального развития РФ по составу и техническим требованиям к сетевому телекоммуникационному оборудованию учреждений системы здравоохранения для регионального уровня единой государственной информационной системы в сфере здравоохранения, а также функциональные требования к ним.

Методические рекомендации Министерства здравоохранения и социального развития РФ по составу, создаваемых в 2011-2012 годах в рамках реализации региональных программ модернизации здравоохранения, прикладных компонентов регионального уровня единой государственной информационной системы в сфере здравоохранения, а также функциональные требования к ним.

Методические рекомендации медицинским организациям по организации криптографической защиты каналов при взаимодействии в рамках ЕГИС в сфере здравоохранения.

Требования:

- Интерфейс подключения к коммутирующему оборудованию в МО — Ethernet.

- наличие возможности передачи голосового трафика по защищённым каналам связи

- обмен информацией по защищенным каналам связи необходимо производить в соответствии с техническими требованиями к взаимодействию информационных систем в СМЭВ, утвержденными Приказом министерства связи и массовых коммуникаций Российской Федерации от 27 декабря 2010 года № 190;

- пропускная способность оборудования, выполняющего криптографическое преобразование при передаче данных по защищенным каналам:

На основных узлах не менее 280 Мб/с;

На неосновных узлах не менее 20 Мб/с;

- Для обеспечения доверительности отношений, безопасности коммуникаций, технических средств и информационных ресурсов ГИСЗ Республики Алтай Оператор должен обеспечить техническую возможность создания виртуальной защищенной среды (VPN с использованием в качестве криптографического протокола ГОСТ 28147-89) которая архитектурно должна включать в себя:

□ Программно-аппаратный комплекс, реализующий функции средства обнаружения атак и вторжений, обнаруживающий атаки в масштабе реального времени, с возможностью регистрации, визуализации и экспорта в файл формата PCAP IP-пакетов, соответствующих зарегистрированным событиям (атакам) для последующего анализа и доказательств произошедшего инцидента, сертифицированный на соответствие требованиям к системам обнаружения атак и системам обнаружения вторжений.

□ Распределенную систему межсетевых экранов, защищающую информационные ресурсы ГИСЗ РА, как от внешних, так и внутренних сетевых атак.

□ Распределенную систему межсетевого шифрования трафика любых приложений, гарантирующую целостность и конфиденциальность информации, как на внешних, так и внутренних коммуникациях, и обеспечивающую разграничение доступа к техническим и информационным ресурсам ГИСЗ РА.

□ Систему контроля и управления связями, правами и полномочиями защищаемых объектов ГИСЗ Республики Алтай, обеспечивающую автоматизированное управление политиками безопасности в ГИСЗ Республики Алтай.

□ Комбинированную систему управления ключами, включающую подсистему асимметричного распределения ключей, обеспечивающую информационную независимость объектов РС ЕГИСЗ РА в рамках заданных политик безопасности от центральной администрации. Подсистему распределения симметричных ключей, гарантирующую высокую надежность и безопасность всех элементов централизованного управления средствами защищённой сети.

□ Систему, обеспечивающую защищенное взаимодействие между разными виртуальными частными сетями путём взаимного согласования между администрациями сетей допустимых межобъектных связей и политик безопасности (защищённые сети Минздрава РФ, ТФОМС РА, органов исполнительной власти РА и др.).

□ Внутри защищённой VPN сети ГИСЗ Республики Алтай требуется создать несколько информационно–независимых виртуальных защищенных контуров, включающих как отдельные, здания, кампусные сети, так и сегменты сетей ФЦОД, ТФОМС для обеспечения функционирования в единой телекоммуникационной среде различных по конфиденциальности или назначению информационных задач.

Оператор должен обеспечить:

□ Независимость режимов безопасности, установленных в виртуальной сети (VPN), от сетевых администраторов, управляющих различными физическими сегментами ГИСЗ Республики Алтай (в том числе сегментов, которые арендуются или отданы в эксплуатацию по модели аутсорсинга), и от ошибочных или преднамеренных действий с их стороны, представляющих одну из наиболее вероятных и опасных угроз.

□ Защиту (обеспечение конфиденциальности, подлинности и целостности) любого вида трафика, передаваемого между любыми компонентами защищённой сети ГИСЗ Республики Алтай.

□ Защиту управляющего трафика для систем и средств удаленного управления объектами сети: маршрутизаторами, межсетевыми экранами, серверами и пр., а также защиту самих средств удаленного управления от возможных атак из глобальной сети.

□ Контроль доступа к любому узлу и сегменту сети ГИСЗ Республики Алтай, включая фильтрацию трафика, правила которой могут быть определены для каждого узла отдельно как с помощью набора стандартных политик, так и с помощью индивидуальной настройки.

□ Защиту от НСД к информационным ресурсам защищённой сети ГИСЗ Республики Алтай, хранимым на рабочих местах (удаленных и локальных), серверах (WWW, FTP, SMTP, SQL, файл-серверах и т.д.).

□ Оперативное управление распределенной VPN-сетью и политикой информационной безопасности на сети из единого центра.

1. **Место оказания сервиса.**

Таблица 10.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование Получателя | Адрес предоставления услуги ЗСПД | Основной канал, Мбит/сек  | Резервный канал, Мбит/сек | Резервный канал 3G/4G, Мбит/сек |
| 1 | БУЗ РА "Кош-Агачская РБ" | с. Кош-Агач, ул. Медицинская, 3 | 60 | 20 | 5 |
| 2 | БУЗ РА "Майминская РБ" | с. Майма, ул. Строителей, 6 к.1 | 20 | 5 | 5 |
| с. Майма, ул. Гидростроителей, 44а | 20 | 5 | 5 |
| с. Майма, ул. ул. Карьерная Алгаир, 10 кв. 80 | 15 | 5 | 5 |
| с. Майма, ул. Советская, 62 | 15 | 5 | 5 |
| 3 | БУЗ РА "Онгудайская РБ" | с. Онгудай, ул. Космонтавтов, 84 | 60 | 20 | 5 |
| 4 | БУЗ РА "Турочакская РБ" | с. Турочак, ул. Набережная, 1 | 20 | 5 | 5 |
| 5 | БУЗ РА "Улаганская РБ" | с. Улаган, ул. Больничная, 30 | 20 | 5 | 5 |
| с. Акташ, ул. Парковая, 8 | 20 | 5 | 5 |
| с. Акташ, ул. Пушкина, 11 | 20 | 5 | 5 |
| 6 | БУЗ РА "Усть-Канская РБ" | с. Усть-Кан, ул. Юбилейная, 3 | 20 | 5 | 5 |
| с. Усть-Кан, ул. Первомайская, 8г | 20 | 5 | 5 |
| с. Усть-Кан, ул. Ленинская, 34 | 20 | 5 | 5 |
| 7 | БУЗ РА "Усть-Коксинская РБ" | с. Усть-Кокса, ул. Советская, 153 | 20 | 5 | 5 |
| 8 | БУЗ РА "Чемальская РБ" | с. Чемал, ул. Чемальская, 4 | 20 | 5 | 5 |
| 9 | БУЗ РА "Чойская РБ" | с. Гусевка, ул. 40 лет Победы, 2а | 20 | 5 | 5 |
| 10 | БУЗ РА "Шебалинская РБ" | с. Шебалино, ул. Фёдорова, 24 | 60 | 20 | 5 |
| 11 | БУЗ РА "КВД" | г. Горно-Алтайск, ул. Чаптынова, 18 | 20 | 5 | 5 |
| г. Горно-Алтайск, ул. Социалистическая, 7 | 20 | 5 | 5 |
| 12 | КУЗ РА "МИАЦ" | г. Горно-Алтайск, пр-т Коммунистический, 54 | 50 | 30 | 10 |
| 12 | БУЗ РА "ПЦ" | г. Горно-Алтайск, ул. Чаптынова, 12 | 30 | 10 | 10 |
| 14 | БУЗ РА "РБ" | г. Горно-Алтайск, пр-т Коммунистический, 140 | 110 | 30 | 10 |
| г. Горно-Алтайск, ул. Ленина, 195 | 17 | 5 | 5 |
| г. Горно-Алтайск, ул. Чорос-Гуркина, 6 | 110 | 30 | 10 |
| г. Горно-Алтайск, пр-т Коммунистический, 170 | 17 | 5 | 5 |
| 15 | БУЗ РА "ЦМК" | г. Горно-Алтайск, ул. Шоссейная, 36 | 15 | 5 | 5 |
| г. Горно-Алтайск, пр-т Коммунистический, 13 | 20 | 5 | 5 |
| с. Майма, ул. Ленина, 67/1 | 20 | 5 | 5 |
| 16 | БУЗ РА "ЦПБС" | г. Горно-Алтайск, ул. Шоссейная, 38 | 30 | 5 | 5 |

Таблица 11

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование учреждения | Адрес учреждения |
| 1 | БУЗ РА «Майминская РБ» | с. Майма, ул. Строителей, 6 к.1 |
|  |  | с. Майма, ул. Гидростроителей, 44а |
|  |  | с. Майма, ул. Карьерная Алгаир, 10, кв. 80 |
|  |  | с. Майма, ул. Советская, 62 |
| 2 | БУЗ РА «Кош-Агачская РБ» | с. Кош-Агач, ул. Медицинская, 3 |
| 3 | БУЗ РА «Улаганская больница» | с. Улаган, ул. Больничная, 30 |
| с. Акташ, ул. Пушкина, 11 |
| 4 | БУЗ РА «Турочакская РБ» | с. Турочак, ул. Набережная, 1 |
| 5 | БУЗ РА «Онгудайская РБ» | с. Онгудай, ул. Космонавтов, 84 |
| 6 | БУЗ РА «Усть-Канская РБ» | с. Усть-Кан, ул. Ленинская, 34 |
| 7 | БУЗ РА «Усть-Коксинская РБ» | с. Усть-Кокса, ул. Советская, 153 |
| 8 | БУЗ РА «Чемальская РБ» | с. Чемал, ул. Чемальская, 4  |
| 9 | БУЗ РА «Шебалинская РБ» | с. Шебалино, ул. Фёдорова, 24 |
| 10 | БУЗ РА «Чойская РБ» | с. Гусевка, ул. 40 лет Победы, 2а |

Сроки оказания сервиса.

После завершения комплекса работ по предоставлению доступа Заказчика к Услуге Исполнитель в срок не более 2 рабочих дней тестирует Услугу на соответствие ее техническим параметрам, указанным в Разделе 1. «Защищенная корпоративная сеть передачи данных» настоящей документации об аукционе.

При успешном результате тестирования Исполнитель извещает Заказчика о готовности предоставлять Услугу. Заказчиком осуществляется тестирование услуги по передаче данных, проверяется возможность приема/передачи трафика.

Начало оказания Услуг - не позднее чем через два рабочих дня со дня заключения Контракта, и до 31.12.2024 г. включительно. Услуга должна оказываться круглосуточно, ежедневно, 7 дней в неделю, без перерывов, с 00 часов 00 минут (время по г. Горно-Алтайску) по всем объектам, перечисленным в Таблице 10.

Исполнитель вправе сдать Услугу по предоставлению доступа досрочно.

1. Обеспечение работоспособности электронной подписи в защищенной сети:

Оператор должен обеспечить работоспособность электронной подписи в защищенной сети, доступ к списку отозванных сертификатов удостоверяющих центров, определенных Заказчиком.

1. Отчеты:

Ежемесячно, не позднее 5 числа, следующего за отчетным периодом, Исполнитель должен предоставлять отчет о количестве трафика и пиковых нагрузках по каждому объекту, обозначенному в Таблице 10 настоящего Технического задания в разрезе каждого дня отчетного периода, согласно Приложению № 3 Контракта.