Приложение № 2

к Договору №_____ от «__» _____ 2018г.

"СОГЛАСОВАНО"

_____ _____

«___» _____ 2018 г.

"УТВЕРЖДАЮ"

Директор по ИТ и связи АО "ЛОЭСК"

_____ **Ю.В. Матвеев**

«___» _____ 2018 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на поставку программно-аппаратного комплекса (ПАК) для защиты периметра корпоративной сети передачи данных АО «ЛОЭСК»

Характеристики корпоративной сети передачи данных АО «ЛОЭСК» (далее КСПД)

- Пропускная способность внешних каналов связи - от 3,5 Гбит/с
- Количество сетевых оконечных устройств - от 1000 устройств, предполагаемый рост за 5 лет до 1500 устройств
- Количество одновременных внешних соединений - от 2 000 000
- Объем трафика электронной почты - не менее 25000 писем/час
- Служба каталога – MS Active Directory
- Платформа виртуализации – Microsoft Hyper-V

Общие требования

ПАК для защиты периметра КСПД АО «ЛОЭСК» должен обеспечивать надежную многоуровневую защиту от любого типа сетевых атак извне на информационные системы, а также оконечные сетевые устройства Общества. Комплекс должен состоять из ряда подсистем:

- **Подсистема межсетевого экранирования** – предназначена для защиты сетевого трафика всех внешних каналов связи. Подсистема должна быть выполнена в виде программно-аппаратного решения. Аппаратная часть должна быть предназначена для установки в телекоммуникационную стойку 19". Решение должно быть отказоустойчивым, состоять, как минимум, из 2-х устройств.
- **Подсистема централизованного управления и защиты конечных узлов** – предназначена для защиты рабочих станций и серверов от различных сетевых угроз и вредоносного ПО. Подсистема должна быть выполнена в виде ПО, устанавливаемого на конечные узлы, а также системы управления этим ПО в виде виртуальной машины на платформе виртуализации Microsoft Hyper-v.
- **Подсистема защиты веб приложений** – предназначена для защиты веб приложений, публикуемых во внешние сети. Подсистема может быть выполнена как в виде программно-аппаратного решения, так и виртуальной машины на платформе виртуализации Microsoft Hyper-v.
- **Подсистема защиты от целенаправленных атак (песочница)** – предназначена для предотвращения новых и неизвестных атак. Подсистема должна быть выполнена в виде программно-аппаратного решения. Аппаратная часть должна быть предназначена для установки в телекоммуникационную стойку 19".
- **Подсистема защиты электронной почты** – предназначена для защиты трафика электронной почты. Подсистема может быть выполнена как в виде программно-аппаратного решения, так и виртуальной машины на платформе виртуализации Microsoft Hyper-v.
- **Подсистема сбора и анализа системных сообщений** – предназначена для сбора, хранения и анализа системных сообщений всех подсистем комплекса, а также создания отчетов на основе собранных данных. Подсистема может быть выполнена в виде виртуальной машины на платформе виртуализации Microsoft Hyper-v.
- **Подсистема централизованного управления и конфигурации** – предназначена для централизованного управления подсистемами комплекса. Подсистема может быть выполнена в виде виртуальной машины на платформе виртуализации Microsoft Hyper-v.

Все подсистемы ПАК для защиты периметра КСПД АО «ЛОЭСК» должны быть произведены одним производителем для организации единого окна по гарантийным обязательствам и обязательствам по технической поддержке. Все подсистемы ПАК

должны поддерживаться технической поддержкой производителя в режиме не менее чем 8х5, сроком не менее 5 лет, включающей:

- доступ к электронной информационной системе технической поддержки;
- технические консультации по электронной почте в режиме не менее чем 8х5;
- замену вышедшего из строя оборудования в течение пяти рабочих дней с момента подтверждения гарантийных обязательств;
- бесплатное предоставление обновленных версий поддерживаемого программного обеспечения по мере их выпуска.

Все сроки действия лицензий или подписок на получение обновлений, требуемых для функционирования ПАК согласно разделу «Технические требования к подсистемам» настоящего ТЗ, должны составлять не менее 5 лет.

Все оборудование должно быть новым, не бывшим в употреблении. Все оборудование, поставляемое в комплекте, совместимо друг с другом. Оборудование комплектуется всеми необходимыми кабелями, обеспечивающими его совместную эксплуатацию и подключение к сети электропитания с использованием российских разъемов.

Все оборудование функционирует при следующих условиях:

- параметры электропитания устройств, подключаемых к сети переменного тока 230 V±10%, 50 Hz ± 1 Hz, если иное не указано в спецификации;
- температура окружающей среды от +5 °C до +40 °C;
- относительная влажность от 40% до 80% при температуре +25 °C;

Упаковка производителя для данного вида товара, целостность упаковки, обеспечивающей сохранность товара при перевозке с учетом возможных перегрузок, складирования, продолжительности и способов транспортировки, при надлежащем и обычном способе обращения с грузом, а также предохраняющей товар от атмосферных воздействий.

Аппаратные средства должны иметь сертификаты соответствия, выданные органами по сертификации, аккредитованными в соответствии с законодательством Российской Федерации об аккредитации в национальной системе аккредитации.

Технические требования к подсистемам

1. Требования к подсистеме межсетевого экранирования

1.1. Лицензирование системы должно осуществляться для неограниченного количества пользователей

1.2. Система должна регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя

1.3. Система должна поддерживать объединение устройств межсетевого экранирования в кластер с возможностью создания типов кластеров:

- Активная система с горячим резервом (active/passive)
- Несколько активных систем - кластер балансировки нагрузки

1.4. Протокол резервирования должен включать в себя синхронизацию сессий и конфигураций между нодами кластера

1.5. Система должна поддерживать функциональность межсетевого экранирования

1.6. Система должна поддерживать возможность устанавливать соединения виртуальных частных сетей (VPN)

1.7. Система должна поддерживать функциональность балансировки нагрузки

1.8. Система должна поддерживать функциональность управления полосой пропускания трафика (traffic shaping)

1.9. Система должна поддерживать обнаружение и контроль использования служб мгновенных сообщений

1.10. Система должна поддерживать возможность работы по протоколу WCCP (как в режиме сервера, так и в режиме клиента)

1.11. Система должна поддерживать возможность блокировки частных VPN (SSH, OpenVPN и пр.), средств удалённого доступа (TeamViewer, LogMeIn и пр.), пиринговых сетей и неизвестных приложений (Unknown-TCP/UDP/P2P)

1.12. Система должна поддерживать возможность создания кастомных сигнатур приложений

1.13. Система должна поддерживать классификацию трафика по протоколам, приложениям, категориям приложений и пользователям

1.14. Система должна поддерживать выделение и ограничение полосы пропускания для классифицированного трафика, включая возможность задания полосы по расписанию

1.15. Система должна поддерживать динамическую маршрутизацию Ipv4, ipv6;

1.16. Система должна поддерживать оптимизацию WAN соединений (оптимизация трафика удаленных подключений по протоколам CIFS, FTP, HTTP, MAPI);

1.17. Система должна поддерживать функционал защиты от утечек данных DLP (фильтрация передачи файлов по типу, имени, отпечатку, размеру, регулярному выражению);

1.18. Система должна поддерживать антивирусную защиту с аппаратным ускорением для достижения низкой задержки при обработке трафика межсетевым экраном;

1.19. Система должна поддерживать возможность проверки на наличие вирусов внутри HTTP, HTTPS, SMTP, POP3, IMAP, FTP трафика;

1.20. Система должна поддерживать возможность автоматически по расписанию получать обновления антивирусных баз;

1.21. Система должна поддерживать возможность помещать инфицированные сообщения электронной почты в карантин;

1.22. Система должна поддерживать возможность лицензионного расширения для поддержки функций защиты от спама (антиспам);

1.23. Система должна иметь поддержку функциональности предотвращения вторжений IPS с аппаратным ускорением для достижения низкой задержки при обработке трафика межсетевым экраном;
1.24. Система должна поддерживать web фильтрацию трафика с возможностью ограничения доступа к определённым категориям сайтов;
1.25. Система должна поддерживать возможность блокировки по URL/ключевому слову/фразе;
1.26. Система должна поддерживать «белые» списки URL;
1.27. Система должна поддерживать функциональность контроля приложений с поддержкой распознавания и блокирования сетевых и веб-приложений вне зависимости от номеров портов;
1.28. Система должна поддерживать функциональность выявления и предотвращения коммуникации с серверами управления и контроля бот-сетями (Command and Control)
1.29. Система должна поддерживать функциональность явного web proxy
1.30. Система должна поддерживать наличие виртуальных доменов (полнофункциональных виртуальных межсетевых экранов внутри одного устройства) в количестве не менее 10 штук без дополнительного лицензирования;
1.31. Система должна поддерживать возможность автоматически по расписанию получать обновления антивирусных баз
1.32. Система должна поддерживать возможность блокировки передачи файлов в зависимости от размера
1.33. Система должна поддерживать возможность блокировки передачи файлов в зависимости от типа
1.34. Система должна поддерживать соединения множества WAN сетей
1.35. Система должна поддерживать протокол pppoe
1.36. Система должна поддерживать протокол DHCP в конфигурациях клиент и сервер;
1.37. Система должна поддерживать маршрутизацию на основе политик;
1.38. Система должна поддерживать динамическую маршрутизацию на основе протоколов RIP v1 и v2, OSPF, BGP, multicast;
1.39. Система должна поддерживать использование зон безопасности;
1.40. Система должна поддерживать маршрутизацию между зонами;
1.41. Система должна поддерживать маршрутизацию между виртуальными сетями;
1.42. Система должна поддерживать администрирование на основе ролей;
1.43. Система должна поддерживать несколько уровней администраторов и пользователей;
1.44. Система должна поддерживать обновление встроенного программного обеспечения через протокол tftp и web-интерфейс;
1.45. Система должна поддерживать возможность возврата к предыдущему состоянию (версии) встроенного ПО;
1.46. Система должна поддерживать аутентификацию пользователей посредством внутренней базы данных;
1.47. Система должна поддерживать аутентификацию пользователей посредством Windows active directory; при этом аутентификация пользователей операционных систем Windows 7 и выше, включённых в домен, должна выполняться автоматически без дополнительных процедур запроса паролей;
1.48. Система должна поддерживать аутентификацию пользователей посредством внешней базы данных RADIUS/LDAP;
1.49. Система должна поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу;

1.50. Система должна поддерживать авторизацию на основе групп пользователей;
1.51. Система должна поддерживать функции NAT, PAT, «прозрачный» (мост);
1.52. Система должна поддерживать функции NAT на основе политик;
1.53. Система должна поддерживать функции VLAN tagging (802.1q);
1.54. Система должна поддерживать функции SIP/h.323 NAT traversal;
1.55. Система должна поддерживать настройку профилей безопасности и политик доступа через веб-интерфейс без необходимости установки дополнительного ПО на АРМ администратора;
1.56. Система должна поддерживать возможность пересылки записей журналов на удалённый Syslog сервер;
1.57. Система должна поддерживать графические средства для отображения результатов мониторинга сетевого трафика, состояния системы и обнаруженных угрозах;
1.58. Система должна поддерживать возможность отправки уведомлений по электронной почте о сетевых атаках;
1.59. Система должна поддерживать интеграцию с внешней системой подсистемой сбора и анализа системных сообщений;
1.60. Система должна поддерживать возможность установления гарантированной, максимальной или приоритетной пропускной способности;
1.61. Система должна поддерживать управление через web интерфейс и интерфейс командной строки;
1.62. Система должна поддерживать возможность интеграции с подсистемой централизованного управления и конфигурации;
1.63. Система должна поддерживать режим обратного прокси-сервера (reverse proxy) с балансировкой нагрузки;
1.64. Система должна поддерживать возможность управления политиками безопасности в интерфейсе командной строки;
1.65. Система должна поддерживать протоколы NetFlow, sFlow
1.66. Система должна поддерживать возможность опроса состояния по протоколу SNMP
1.67. Система должна иметь возможность интеграции и управления коммутационным оборудованием для расширения функций безопасности (802.1x) для организации защиты доступа к сети WiFi.
1.68. Реализация в виде программно-аппаратного комплекса с поддержкой установки в стандартную телекоммуникационную стойку 19”
1.69. Система должна поддерживать интеграцию с подсистемой защиты конечных узлов, иметь возможность получения телеметрической информации (активированных функций безопасности конечного узла, модели и версии ОС, имени узла, IP адреса, MAC-адреса, и иной системной информации) и обеспечивать контроль не менее 2000 конечных узлов (срок действия лицензии не менее 5 лет)
1.70. Высота оборудования в единицах: не более 1RU на одно устройство
1.71. Задержка при работе функциональности межсетевого экранирования на пакетах UDP размером 64 байт: не более 3 микросекунд
1.72. Заявленная производителем совокупная производительность межсетевого экрана следующего поколения (NGFW) с включенным функционалом контроля приложений и системы IPS: не менее 3.8 Гбит/с
1.73. Количество интерфейсов 10 GE для установки модулей SFP+: не менее 2
1.74. Количество интерфейсов 1000base-T: не менее 8

1.75. Количество интерфейсов Gigabit Ethernet SFP: не менее 8
1.76. Количество SFP+ Трансиверов (MM, 850nm, duplex LC, 10Gbase-SR): 4 шт.
1.77. Поставляемое решение должно иметь действующий сертификат соответствия требованиям «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевого экрана типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ»(ФСТЭК России, 2012).

2. Требования к подсистеме централизованного управления и защиты конечных узлов

2.1. Система должна обеспечивать защиту конечных узлов путем установки специализированного ПО на клиентские устройства
2.2. Система должна обеспечивать антивирусную защиту конечных узлов
2.3. Система должна поддерживать web фильтрацию трафика с возможностью ограничения доступа к определённым категориям сайтов
2.4. Система должна поддерживать функциональность межсетевого экрана приложений с возможностью блокировки определенных администратором категорий приложений
2.5. Система должна обеспечивать интеграцию с системой двухфакторной аутентификации, в том числе с применением токенов с одноразовыми паролями временного действия для дополнительной защиты удаленных подключений
2.6. Система должна поддерживать сканер уязвимостей на конечных узлах средствами специализированного ПО.
2.7. Система должна обеспечивать мониторинг состояния конечных узлов в реальном времени
2.8. Система должна регулярно получать обновления сигнатур модулей безопасности с сервера производителя
2.9. Система должна поддерживать удалённое развертывание, настройку и централизованное управление из единой консоли (графического интерфейса) администратора
2.10. Система должна иметь встроенный функционал и поддерживать интеграцию с внешними системами для передачи информации телеметрии, включающей информацию о пользователях, используемой модели и версии операционной системы, IP адрес, MAC адрес, информацию об обнаруженных уязвимостях
2.11. Система должна иметь встроенный функционал и поддерживать интеграцию с внешними системами для оценки соответствия рабочих станций корпоративной политике безопасности. В случае несоответствия политике безопасности проверяемый хост должен быть помещен в карантин с ограничением сетевого доступа
2.12. Возможность интеграции с системой централизованного сбора событий и передача информации обо всех зарегистрированных клиентах в данную систему
2.13. При интеграции с системой централизованного сбора событий система должна передавать в нее всю необходимую информацию для построения сводных отчетов по узлам и угрозам, отчета модулей антивируса, веб-фильтра, отчета по угрозам по времени, устройствам и/или пользователям, отчета по использованию VPN
2.14. Система должна поддерживать интеграцию с внешней специализированной системой для защиты от целенаправленных и ранее не известных атак, входящей в состав решения

2.15. Система должна иметь возможность контролировать доступ к файловой системе подключаемых USB устройств и запрещать доступ к файлу (открытие/запуск) до получения результата его проверки антивирусным модулем, в том числе отправка его на проверку во внешние системы противодействия направленным атакам и защиты от атак нулевого дня
2.16. Система централизованного управления должна обеспечивать поддержку централизованного управления до 1500 клиентских устройств
2.17. Система должна быть масштабируемой методом лицензионного расширения
2.18. Возможность удаленно запускать на управляемых клиентских устройствах антивирусное сканирование и в случае необходимости переводить зараженный хост в карантин
2.19. Поддержка управления на основе групп и интеграция с Microsoft Active Directory для централизованного развертывания клиентов на рабочих станциях в том числе с помощью GPO
2.20. Поддержка клиентских, серверных и мобильных операционных систем:

- Microsoft Windows 10/8.1/8/7 (32-bit, 64-bit), XP (32-bit)
- Windows Server 2008 R2/2012/2012 R2/2016
- Mac OS X 10.12 Sierra, OS X v10.11 El Capitan, OS X v10.10 Yosemite, OS X v10.9 Mavericks, OS X v10.8 Mountain Lion
- iOS 5.1 и более свежие версии для iPhone, iPad, iPod Touch
- Android OS 4.0.4 и более свежие версии

2.21. Система должна поддерживать возможность устанавливать соединения виртуальных частных сетей (VPN) – SSL и IPSec, в том числе с применением двухфакторной аутентификации и сертификатов
2.22. Система должна поддерживать установление VPN подключения до Windows logon
2.23. Система должна поддерживать централизованное управление сертификатами
2.24. Система должна поддерживать возможность передачи информации об учетной записи текущего пользователя Active Directory для реализации прозрачной аутентификации пользователей
2.25. Система должна поддерживать возможность отслеживания сетевого взаимодействия с ботнет-сетями
2.26. Система должна поддерживать локальный карантин в случае срабатывания антивирусного модуля
2.27. Система должна поддерживать WAN оптимизацию для следующих протоколов: CIFS, FTP, HTTP, MAPI
2.28. Система должна обеспечивать просмотр включенных функций, ОС, имени узла, IP адреса и иной системной информации
2.29. Система должна отображать статус клиентского ПО для каждого узла

3. Требования к подсистеме защиты веб приложений

3.1. Лицензирование системы должно осуществляться для неограниченного количества защищаемых веб-приложений;
3.2. Обеспечение защиты от основных атак на веб-приложения из перечня OWASP Top 10
3.3. Поддержка определения собственных правил на основе различных критериев запросов пользователей к защищаемым веб-серверам и ответов защищаемых веб-серверов
3.4. Наличие встроенного сканера уязвимостей веб-приложений

3.5. Поддержка интеграции со сторонними сканерами уязвимостей веб-приложений с возможностью автоматической генерации правил для устранения выявленных уязвимостей
3.6. Поддержка автоматического профилирования, т.е. генерации профиля, отражающего контекст и параметры взаимодействия пользователей с защищаемым веб-приложением
3.7. Обеспечение защиты от атак типа «brute force», т.е. атак подбора пароля на вход в веб-приложение
3.8. Обеспечение защиты от атак типа «defacement», т.е. атак, направленных на подмену контента веб-сайта
3.9. Обеспечение защиты от атак типа отказ в обслуживании
3.10. Поддержка терминации системой HTTPS соединений с разгрузкой с веб-приложения функций SSL/TLS
3.11. Поддержка предоставления нескольких сертификатов на один защищаемый адрес, в зависимости от значения поля SNI в клиентском запросе
3.12. Система должна регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя;
3.13. Система должна поддерживать развертывание в различных режимах:
- обратный прокси (reverse proxy);
- прозрачный прокси (transparent proxy);
- оффлайн сниффер (offline sniffing);
- веб кеш (клиент протокола WCCP);

3.14. Система должна иметь функциональность балансировки нагрузки;
3.15. Система должна иметь функционал защиты от утечек данных DLP;
3.16. Система должна поддерживать антивирусное сканирование выгружаемых на веб-сервер файлов;
3.17. Система должна поддерживать наличие административных доменов (т.е. независимых наборов политик, с разделением доступа по группам администраторов), доступных по умолчанию;
3.18. Система должна иметь возможность автоматически по расписанию получать обновления антивирусных баз;
3.19. Система должна поддерживать администрирование на основе ролей;
3.20. Система должна поддерживать несколько уровней администраторов и пользователей;
3.21. Система должна поддерживать обновление встроенного ПО через протокол TFTP и web-интерфейс;
3.22. Система должна поддерживать аутентификацию пользователей посредством внутренней базы данных;
3.23. Система должна поддерживать аутентификацию пользователей веб-приложения по протоколам RADIUS, LDAP, Kerberos;
3.24. Система должна поддерживать авторизацию на основе групп пользователей;
3.25. Система должна поддерживать различные методы авторизации в рамках протокола HTTP, в т.ч. HTTP basic;
3.26. Система должна иметь возможность пересылки записей журналов на удалённый syslog сервер;
3.27. Система должна иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угроз;

3.28. Система должна иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках;
3.29. Система должна поддерживать интеграцию с системой сбора и анализа событий безопасности, входящей в состав решения;
3.30. Система должна поддерживать возможность локального кеширования Web контента для оптимизации полосы пропускания и скорости доступа к Web ресурсам;
3.31. Система должна поддерживать управление через Web интерфейс;
3.32. Система должна поддерживать возможность управления политиками безопасности в интерфейсе командной строки;
3.33. Реализация в виде виртуальной машины
3.34. производительность системы по веб-трафику: не менее 100 Мбит/с;
3.35. количество доступных административных доменов: не менее 4;

4. Требования к подсистеме защиты от целенаправленных атак

4.1. Система должна предоставлять сервис по сканированию объектов, представленных в виде файлов и гиперссылок (URL), на предмет ранее неизвестного вредоносного ПО
4.2. Система должна обеспечивать проверку объектов посредством антивирусного сканирования
4.3. Система должна обеспечивать проверку объектов посредством эмуляции в виртуальной среде с целью выявления поведенческих признаков, характерных для вредоносного ПО
4.4. Система должна иметь возможность поддерживать следующие виртуальные среды для эмуляции: Windows XP, Windows 7, Windows 8.1, Windows 10, Android
4.5. Доступные в комплекте поставки для использования виртуальные среды для эмуляции: Windows 7, Windows 8.1, Windows 10
4.6. Система должна поддерживать возможность эмуляции в собственных образах операционных систем, а также возможность установки собственных приложений в эти образы.
4.7. Система должна поддерживать приём объектов и передачу результатов сканирования от систем межсетевого экранирования и систем защиты электронной почты, входящих в комплект поставки
4.8. Система должна поддерживать открытый протокол Internet Content Adaptation Protocol (ICAP) для приёма объектов на сканирование
4.9. Система должна поддерживать открытый прикладной программный интерфейс (API) для приёма объектов на сканирование
4.10. Решение должно обеспечивать поддержку внешнего Syslog-сервера
4.11. Решение должно поддерживать экспорт журналов в систему централизованного сбора событий и построения отчетов
4.12. Система должна поддерживать управление через Web интерфейс
4.13. Реализация в виде программно-аппаратного комплекса с поддержкой установки в стандартную телекоммуникационную стойку 19". Высота оборудования в единицах: не более 2RU.
4.14. Производительность проверки объектов посредством предварительной фильтрации: не менее 6000 файлов в час

4.15. Производительность проверки объектов посредством эмуляции в виртуальной среде: не менее 160 файлов в час

5. Требования к подсистеме защиты электронной почты

5.1.Решение должно предоставлять собой шлюз безопасности электронной почты

5.2.Решение должно поддерживать работу в режимах:

- Почтовый сервер
- Прозрачный шлюз
- Шлюз (агент MTA)

5.3.Решение должно обеспечивать анти-спам фильтрацию электронной почты;

5.4.Решение должно обеспечивать анти-фишинг фильтрации электронной почты

5.5.Решение должно обеспечивать антивирусную фильтрации электронной почты

5.6.Решение должно обеспечивать фильтрацию URL в теле электронных писем

5.7.Решение должно обеспечивать предотвращение утечек конфиденциальных данных

5.8.Решение должно обеспечивать карантин для электронной почты

5.9.Решение должно обеспечивать фильтрацию входящей и исходящей электронной почты

5.10. Решение должно поддерживать не менее 3 почтовых доменов

5.11. Решение должно поддерживать политики защиты и маршрутизация почты на основе атрибутов LDAP (домена)

5.12. Решение должно поддерживать SMTP-аутентификацию посредством LDAP, RADIUS, POP3 или IMAP

5.13. Решение должно поддерживать очередь сообщений для ошибочных, поврежденных, задержанных и недоставленных сообщений

5.14. Решение должно обеспечивать возможность интеграции с внешними RBL (Realtime Blackhole List) сервисами

5.15. Решение должно поддерживать технологии Email аутентификации – Domain Key Identified Management (DKIM), Sender Policy Framework (SPF);

5.16. Решение должно обеспечивать поддержку «черных» и «белых» списков отправителей (email адрес\email домен\IP адрес)

5.17. Решение должно обеспечивать поддержку технологии Greylisting («серые списки»);

5.18. Решение должно обеспечивать защиту от DoS атак на почтовую инфраструктуру

5.19. Решение должно поддерживать интеграцию с подсистемой защиты от целенаправленных атак (песочница), входящем в состав решения, для осуществления эффективной защиты от угроз класса “0-day”. Письмо, содержащее подозрительные вложение не должны перенаправляться на принимающий почтовый сервер до окончания инспекции (с положительным заключением) на решении класса Sandbox.

5.20. Предотвращение утечек конфиденциальных данных. Идентификация и блокировка контента должна быть возможна как минимум по ключевым словам, словарям, регулярным выражениям, хэшу файла

5.21. Контроль содержимого электронных писем (по типу, числу, размеру вложений)

5.22. Решение должно поддерживать экспорт журналов событий

5.23. Решение должно поддерживать мониторинг по протоколу SNMP

5.24. Решение должно обеспечивать возможность архивирования входящих и исходящих сообщений на основе политик с поддержкой резервных копий на отчуждаемых носителях

5.25. Решение должно обеспечивать поддержку отказоустойчивых кластеров в режимах Active-Active, Active-Passive
5.26. Решение должно обеспечивать встроенную, основанную на политиках, маршрутизацию почты и управление очередями
5.27. Решение должно поддерживать карантин сообщений электронной почты
5.28. Наличие защищенной операционной системы. Кастомизированная операционная система, специально адаптированная на обработку и анализ почтового трафика. Специально разработанное ПО почтового стека (MTA).
5.29. Администрирование решения должно выполняться через графический веб-интерфейс управления и интерфейс командной строки (CLI)
5.30. Количество защищаемых почтовых ящиков или пользователей не должно быть ограничено лицензией
5.31. Решение должно обеспечивать эвристические методы фильтрации
5.32. Решение должно обеспечивать фильтрацию вложений/содержимого
5.33. Решение должно обеспечивать усиленную проверку заголовков сообщения
5.34. Решение должно обеспечивать проверку в реальном времени на спам с помощью «черных» списков URL (SURBL)
5.35. Решение должно обеспечивать проверку в реальном времени с использованием Байесовского статистического фильтра
5.36. Решение должно обеспечивать фильтрацию по запрещенным словам
5.37. Решение должно обеспечивать управление спамом (принять, передать, отклонить или отвергнуть), основанное на блоклисте проверок контрольных сумм спама SHFSH
5.38. Решение должно обеспечивать сканирование и анализ графических изображений
5.39. Решение должно обеспечивать поддержку общих и пользовательских настраиваемых «черных»/«белых» списков
5.40. Решение должно обеспечивать поддержку «черных» списков третьих фирм, формируемых в реальном времени (RBL)
5.41. Решение должно обеспечивать проверку на ложность IP-адреса
5.42. Решение должно обеспечивать проверку с использованием грейлистинга
5.43. Решение должно обеспечивать различные действия при выявлении спама, включающие маркировку писем, вставку дополнительного заголовка, пересылку на альтернативный почтовый сервер, архивирование, уведомление получателя или предварительно настроенных адресатов, отмену доставки с/без уведомления отправителя, персональный карантин, смену адресата.
5.44. Решение должно обеспечивать проверку на вирусы SMTP-сообщений
5.45. Решение должно обеспечивать поддержку сжатых присоединенных файлов и вложенных архивов
5.46. Решение должно обеспечивать помещение зараженных файлов на карантин
5.47. Решение должно обеспечивать поддержку уведомлений при замене сообщений
5.48. Решение должно обеспечивать фильтрацию вложений
5.49. Решение должно обеспечивать проверку и блокирование по типам файлов
5.50. Решение должно поддерживать антивирусный движок и сигнатуры для него собственной разработки (от производителя)
5.51. Решение должно обеспечивать протоколирование изменения конфигураций и событий управления
5.52. Решение должно обеспечивать протоколирования вирусных инцидентов

5.53. Решение должно обеспечивать протоколирование активности модуля противодействия спаму
5.54. Решение должно обеспечивать поддержку внешнего Syslog-сервера
5.55. Решение должно обеспечивать уведомление о критических событиях и вирусных инцидентах
5.56. Решение должно позволять изменять содержимое уведомлений о событиях и инцидентах
5.57. Решение должно поддерживать полноценную систему отчетности, включающая генерацию отчетов по категориям
5.58. Решение должно поддерживать предустановленные шаблоны отчетов
5.59. Решение должно обеспечивать формирование отчетов по расписанию
5.60. Решение должно обеспечивать формирование и отправка отчетов в PDF-формате
5.61. Реализация в виде виртуальной машины
5.62. Производительность маршрутизации электронной почты с антивирусной и антиспам проверкой на типовых сообщениях размером 100Кб: не менее 25000 сообщений в час

6. Требования к подсистеме сбора и анализа системных сообщений

6.1.Совместимость с системами межсетевого экранирования, системами защиты электронной почты, системами защиты от целенаправленных атак, системами защиты веб приложений, входящими в комплект поставки
6.2.Обеспечение сбора и анализа событий журналов, создания отчётов на основе данных, получаемых с систем межсетевого экранирования;
6.3.Возможность построения сводных графических отчётов с анализируемых устройств
6.4.Поддержка создания отчётов по сетевой активности, системным событиям, вирусам, атакам, web фильтрации
6.5.Наличие встроенных шаблонов для быстрого создания наиболее востребованных отчётов
6.6.Поддержка импорта и экспорта шаблонов отчётов
6.7.Возможность просмотра логов в реальном времени
6.8.Возможность поиска и фильтрации данных в логах
6.9.Возможность создания оповещений при возникновении определённых событий в логах
6.10. Возможность рассылки оповещений по электронной почте или передачи по протоколу Syslog
6.11. Поддержка сервиса индикаторов компрометации, для ретроспективного выявления скомпрометированных узлов
6.12. Реализация в виде виртуальной машины
6.13. Производительность данных логов: не менее 5 Гб логов в день
6.14. Доступный объём хранилища данных: не менее 3 ТБ

7. Требования к подсистеме централизованного управления и конфигурации

7.1. Полная совместимость с системами межсетевого экранирования, входящими в комплект поставки
7.2. Система должна обеспечивать управление системами межсетевого экранирования
7.3. Система должна обеспечивать управление политиками безопасности и подключениями VPN

7.4. Система должна иметь возможность централизованного обновления встроенного программного обеспечения систем межсетевого экранирования
7.5. Система должна иметь возможность локально хранить обновления сигнатур модулей безопасности и предоставлять эти обновления совместимым системам
7.6. Система должна иметь возможность группировки управляемых устройств для назначения политик по отдельным группам
7.7. Система должна иметь возможность назначения глобальных политик безопасности, которые могут применяться ко всем управляемым устройствам одновременно
7.8. Система должна поддерживать администрирование на основе ролей
7.9. Система должна поддерживать несколько уровней администраторов и пользователей
7.10. Система должна поддерживать создания шаблонов политик для быстрого добавления новых управляемых устройств
7.11. Система должна поддерживать управление через Web интерфейс
7.12. Реализация в виде виртуальной машины
7.13. Лицензия должна включать управление устройствами или виртуальными (административными) доменами в количестве не менее 10 штук

Дополнительные условия поставки

Компания поставщик должна иметь авторотационное письмо от производителя на право поставки данного оборудования.

С момента передачи в собственность Заказчику ПАК для защиты периметра корпоративной сети передачи данных АО «ЛОЭСК», все гарантийные обязательства и обязательства по технической поддержке несет производитель Товара, который входит в ПАК для защиты периметра КСПД АО «ЛОЭСК».

Состав предоставляемой документации:

- инструкция по быстрому запуску от производителя
- руководство администратора продукции от производителя
- руководство по установке продукции от производителя

Поставщик производит консультации при установке и первичной настройке Заказчиком программно-аппаратного комплекса для защиты периметра КСПД.

Поставщик должен иметь сертификат, подтверждающий квалификацию сотрудников, которые будут проводить консультации при установке и первичной настройке Заказчиком программно-аппаратного комплекса для защиты периметра КСПД.