Техническое задание на закупку.

1. Предмет закупки: программно-аппаратный комплекс «Система сбора и обработки событий информационной безопасности» (далее – SIEM) (1 шт.) с услугами по настройке и пуско-наладочными работами.

КОД ОКРБ: 58.29.50.000

Ориентировочная стоимость закупки: 7 841 базовая величина.

2. Требования к предмету закупки:

Все опции, предусмотренные производителем SIEM, должны полноценно функционировать и быть доступными на территории Республики Беларусь.

К поставляемому оборудованию должна прилагаться копия сертификата соответствия Национальной системы подтверждения соответствия Республики Беларусь на соответствие требованиям технического регламента ТР 2013/027/BY (использование SIEM в информационных системах, отнесенных к классу типовых информационных систем 3-ин, 3-спец, 3-дсп, 3-юл согласно Приложению 1 приказа оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»).

Производитель предлагаемого решения должен иметь представительство на территории Республики Беларусь, для возможности оперативного взаимодействия и решения возможных вопросов.

2.1. Минимальные технические требования к серверу:

№	Наименование параметра	Значение	Примечание
1.	Форм-фактор	2U Rack	Для установки в стойку 19”
2.	Тип процессора	Не менее Intel Xeon Scalable 5-го поколения	
3.	Количество процессоров	Не менее 2 шт.	
4.	Общее количество потоков	Не менее 42	
5.	Поддержка инструкций	SSE 4.2	
6.	Тип памяти	DDR5 RDIMM ECC	
7.	Объем установленной памяти	Не менее 128 ГБ	
8.	Возможность расширения	До 8ТБ	
9.	RAID-контроллер	Аппаратный, кэш не менее 4ГБ	RAID 0,1,5,6,10
10.	Системные накопители	2xSSD не менее 480 ГБ	RAID 1 для ОС
11.	Накопители для данных	8x NVMe SSD не менее 3.84 ТБ	
12.	Поддержка Hot-Swap	Да	Горячая замена
13.	Тип сетевого адаптера	OCP 3.0 или PCIe	
14.	Скорость портов	Не менее 2x25Gbe	
15.	Блок питание	2x не менее 1100W	Резервирование N+1
16.	Энергоэффективность	80 PLUS Platinum или выше	
17.	Дополнительные требования:	- Совместимость с ОС: Ubuntu 22.04, Astra Linux SE РУСБ.10015-01 (v1.7+), Debian 12; – Поддержка виртуализации: VMware vSphere, Hyper-V, KVM, zVirt; – Средства удалённого управления: IPMI	

		2.0, Redfish API; − Комплект направляющих для установки в стойку 19"; − Комплект кабелей электропитания (не менее 2 шт.); − Техническая документация на русском языке; - Сертификат соответствия ТР ТС или декларация соответствия; - Оборудование должно быть новым, не бывшим в употреблении; − Год выпуска оборудования: не ранее 2024 года. - Предустановка операционной системы.	

2.2. Минимальные характеристики к Программному обеспечению «Защищенная среда виртуализации»:

1. Обеспечивает работу виртуальных машин и остальных серверных компонентов инфраструктуры.
2. Имеет единый графический веб-интерфейс администратора и интерфейс командной строки администратора службы.
3. Имеет средства управления серверами виртуализации в виде командной строки.
4. Имеет возможность создания шаблонов виртуальных машин и быстрого развертывания виртуальных машин из этих шаблонов, и использования библиотеки образов.
5. Имеет возможность администратору системы получать доступ к гостевой операционной системе через сервер виртуализации даже в случае отсутствия у виртуальной машины сетевого адаптера или подключения к сети.
6. Имеет возможность разграничения доступа к виртуальной среде, построенного на основе классической ролевой политики безопасности и ее интеграции со службой каталога.
7. Имеет возможность перемещения виртуальных машин между серверами без выключения ОС виртуальной машины.
8. Имеет возможность перемещения файлов виртуальных машин между системами хранения без остановки ОС виртуальной машины.
9. Имеет возможность автоматического перезапуска виртуальных машин на других физических серверах виртуализации, находящихся в одном кластере, в случае выхода из строя сервера, на котором они функционировали.
10. Имеет возможность проброса на виртуальные машины USB-устройств физического сервера.
11. Обеспечивает возможность клонировать виртуальные машины без необходимости выключения виртуальные машины.
12. Имеет возможность динамического добавления ресурсов: RAM, vCPU, дискового пространства, без остановки виртуальной машины.
13. Имеет возможность выделять пространство на системе хранения данных для дисков виртуальных машин по требованию, позволяющее более эффективно его использовать
14. Имеет возможность создания мгновенного снимка состояния виртуальной машины с возможностью возврата к нему.
15. Имеет поддержку отображения единого графического веб-интерфейса администратора на русском языке.
16. Имеет единое окно отслеживания состояния системы в реальном времени (Dashboard).

17. Имеет возможность размещения файлов виртуальных машин на следующих типах систем хранения:

a. с файловым доступом по протоколу NFS, локальном диске гипервизора.

b. с блочным доступом по протоколам Fibre Channel и iSCSI.

18. Имеет возможность обеспечения высокой доступности виртуальных машин, файлы которых размещены на системах хранения данных.

19. Имеет возможность автоматического восстановления (перезапуск) виртуальной машины в аварийном состоянии.

20. Имеет возможность автоматической балансировки рабочих нагрузок между хостами путем «горячей» миграции без выключения виртуальных машин.

21. Обеспечивает виртуализацию аппаратных ресурсов в виде обособленных виртуальных машин, работающих на физическом сервере x86 архитектуры.

22. Имеет в своем составе систему резервного копирования, доступную через единый графический веб-интерфейс администратора.

23. Имеет поддержку технологии NVIDIA vGPU.

24. Имеет возможность включения технологии NVIDIA Unified Memory для виртуальных GPU.

25. Имеет возможность передачи данных состояния системы в систему мониторинга Zabbix.

26. Имеет возможность функционирования как с наличием физических СХД, так и в составе гиперконвергентной среды.

27. Имеет функции по созданию и использованию встроенной инфраструктуры Виртуальных Рабочих Столов (VDI).

28. Имеет административный и пользовательский веб-портал.

29. Имеет возможность установки в режиме выделенной физической или виртуальной машины вне управляемого кластера и в режиме виртуальной машины на гипервизорах управляемого кластера.

30. Имеет возможность установки без подключения к сети Интернет.

31. Имеет возможность автозапуска виртуальных машин.

32. Имеет возможность управления локальными пользователями через единый графический веб-интерфейс администратора.

33. Имеет возможность проброса на виртуальные машины локальных дисков и LUN.

34. Обеспечивает доступ к консоли ВМ по протоколам SPICE, VNC, HTML5.

35. Имеет возможность централизованной настройки сетевых компонентов на хостах виртуализации.

36. Имеет поддержку создания метро-кластеров для построения высокодоступной инфраструктуры на нескольких площадках. В качестве гео-распределенного хранилища могут выступать как классические СХД (с соответствующим функционалом), так и программно-определяемые.

37. Имеет поддержку миграции виртуальных машин между кластерами без прерывания работы сервисов в гостевых ОС.

38. Имеет возможность миграции виртуальных машин на базе ОС (Astra Linux, РЕД ОС, Альт, РОСА, Аврора, AlterOS») из других систем виртуализации.

39. Имеет возможность настройки виртуальных сетей на базе распределенного коммутатора с управлением через единый графический веб-интерфейс администратора.

40. Имеет возможности распределенной коммутации пакетов уровня L2 без привязки к нижележащей топологии сети и физическому расположению с управлением через единый графический веб-интерфейс администратора.

41. Имеет средства управления IP-адресацией подключенных ВМ с управлением через единый графический веб-интерфейс администратора.

42. Имеет возможность настройки MTU на распределенном коммутаторе через единый графический веб-интерфейс администратора.

43. Имеет возможность настройки маршрутизации трафика между изолированными сетями без выхода трафика за пределы виртуального коммутатора через единый графический веб-интерфейс администратора.

44. Имеет возможность настройки маршрутизации трафика между физической сетью и изолированными сетями через единый графический веб-интерфейс администратора.

45. Имеет возможности трансляции сетевых адресов (SNAT) с управлением через единый графический веб-интерфейс администратора.

46. Имеет возможность настройки правил микросегментации (распределенного межсетевого экрана) входящего и исходящего трафика виртуальных машин на уровне L3 и L4 на порту виртуальной машины и по IP-адресам через единый графический веб-интерфейс администратора.

47. Имеет возможность объединения правил микросегментации в блоки (группы безопасности) через единый графический веб-интерфейс администратора.

48. Имеет возможность редактирования таблицы маршрутизации логического маршрутизатора и задания статических маршрутов через единый графический веб-интерфейс администратора.

49. Имеет возможность подключения виртуальной машины к существующему широковещательному домену с сохранением функционала управления IP-адресацией с управлением через единый графический веб-интерфейс администратора.

50. Имеет возможность присвоения IP-адресов с момента создания виртуального интерфейса - как при создании ВМ, так и при изменении конфигурации (добавление или удаление виртуальных сетевых карт).

51. Имеет возможность настройки отказоустойчивости логического маршрутизатора, включая назначение нескольких серверов виртуализации для данного маршрутизатора и определение приоритета подключения через единый графический веб-интерфейс администратора.

52. Имеет возможность конвертации виртуальных машин на уровне гипервизора с платформы виртуализации VMware vSphere с настройкой размещения (центр данных, кластер и домен хранения) и параметров сети с управлением через единый графический веб-интерфейс администратора.

53. Имеет возможность экспорта списка виртуальных машин, хостов виртуализации, доменов хранения, пулов, событий в CSV формат через единый графический веб-интерфейс администратора.

54. Имеет возможность перевода домена хранения в режим обслуживания без необходимости останавливать все приостановленные виртуальные машины.

55. Имеет функционал сбора сведений об оборудовании, на котором развернута ПО виртуализации, для последующего анализа и передачи в службу поддержки.

56. Имеет возможность автоматической очистки информации о хранилищах на хостах виртуализации после удаления данных хранилищ.

57. Имеет возможность интеграции с системой для централизованного управления безопасностью, событиями и информацией (SIEM), включая: ArcSight, Ankey SIEM, Max Patrol SIEM и Kaspersky Unified Monitoring and Analysis Platform (KUMA).

58. Имеет возможность отправки лог файлов на внешний syslog сервер для отдельного хоста виртуализации, кластера виртуализации и сервера управления и выбора протокола передачи данных лог файлов (TCP, SSL) через единый графический веб-интерфейс администратора.

59. Имеет возможность предоставления информации по загрузке ресурсов хранения в реальном времени в едином графическом веб-интерфейсе администратора и предоставлять возможность задания пороговых значений (при достижении которых приходят уведомления) по

следующим параметрам: скорость чтения на диск, скорость записи на диск, задержка чтения, задержка записи.

60. Имеет возможность ручного и автоматического (по расписанию) резервного копирования конфигурации сервера управления, включая конфигурацию сети (виртуальных сетей, подсетей, логических портов, внешних сетей, логических маршрутизаторов), через единый графический веб-интерфейс администратора с возможностью выбора расположения файла резервной копии.

61. Имеет возможность создания отчетов о состоянии, утилизации и ошибках виртуальной инфраструктуры за выбранный период времени через единый графический веб-интерфейс администратора с учетом часового пояса менеджера управления в следующих форматах: PDF, HTML.

62. Имеет возможность шифрования паролей в конфигурационных файлах с помощью алгоритма AES (Advanced Encryption Standard).

63. Имеет возможность настройки автоматического перевода недогруженных хостов в режим обслуживания и выключать, а также включать данные хосты при необходимости.

64. Имеет возможность формирования диаграммы (карты), на которой отображены объекты виртуальной инфраструктуры (кластеры, серверы, ресурсы хранения), их состояние и связи между ними в реальном времени.

65. Имеет возможность настройки максимального количества сессий для пользователей из внешних доменов через единый графический веб-интерфейс администратора.

66. Производитель программного обеспечения виртуализации должен обеспечивать официальную техническую поддержку на территории Республики Беларусь, а также обеспечить полное лицензирование согласно правилам производителя.

67. Имеет уровень поддержки – 9x5 (в рабочие дни с 09:00 до 18:00). Время реакции на аварийную ситуацию – 30 минут.

68. Обеспечивает работу не менее 250 хостов виртуализации в рамках одного кластера.

69. Обеспечивает управление не менее чем 400 хостами виртуализации из единого графического веб-интерфейса администратора.

70. Сертифицировано на соответствие требованиям ТР 2013/027/BY Оперативно-аналитического центра при Президенте Республики Беларусь.

2.3. Функциональные характеристики системы управления событиями информационной безопасности:

2.3.1. Перечень обозначений и сокращений

ПО	Программное обеспечение
ЧТЗ	Частное техническое задание
СУС ИБ	Системы управления событиями информационной безопасности
ИБ	Информационная безопасность
ИТС	Информационно-телекоммуникационной системы
ОИИ	Объект информационной инфраструктуры
ИС	Информационная система
ВПО	Вредоносное программное обеспечение
СЗИ	Средство защиты информации

АРМ	Автоматизированное рабочее место

2.3.2. Общие требования к системе СУС ИБ

СУС ИБ должна обеспечивать решение следующих общих задач:

– сбор, обработка, отображение и долгосрочное хранение информации о событиях и подозрениях на инциденты информационной безопасности, выявляемых в инфраструктуре Заказчика;

– предоставление инструментов для анализа событий и расследования инцидентов информационной безопасности, в том числе, масштабных инцидентов ИБ, затрагивающие несколько территориальных подразделений;

– предоставление исходной информации для определения влияния события или подозрения на инцидент ИБ на ИТ-сервисы.

СУС ИБ должна строиться как единая система с иерархической функциональной структурой и централизованным пунктом управления и являться составной частью информационно-телекоммуникационной системы Заказчика.

СУС ИБ должна иметь микросервисную архитектуру, обеспечивающую перенос части функции СУС ИБ на отдельные сервера, выполняющие функции:

– Приема событий;
– Нормализации событий;
– Корреляции событий;
– Хранения событий.

СУС ИБ должна удовлетворять следующим общим требованиям:

– Масштабируемость – способность справляться с увеличением рабочей нагрузки на СУС ИБ путем наращивания числа функциональных блоков, выполняющих одни и те же задачи (горизонтальное масштабирование);

– Вертикальная масштабируемость – возможность увеличения ресурсов на выделенных серверах.

– Работоспособность – состояние системы, при котором она способна выполнять заданные функции с параметрами, установленными требованиями технической документации.

– Отказоустойчивость – свойство системы непрерывно сохранять работоспособность в течение некоторого времени. СУС ИБ должна поставляться в отказоустойчивой конфигурации (кластере) для обеспечения функционирования в случае сбоев оборудования или ПО.

– Унификация – использование типовых проектных решений, обеспечение возможности использования таких решений.

– Информационная безопасность – обеспечение конфиденциальности, целостности и доступности хранящейся и обрабатываемой СУС ИБ информации.

СУС ИБ должна обеспечивать функционирование в следующих режимах:

– штатный режим – режим функционирования СУС ИБ, при котором обеспечивается выполнение функциональных возможностей системы в объеме, соответствующем текущему этапу реализации;

– автономный режим – режим, характеризующийся ограничением возможностей контроля. В этом случае сохраняется основной функционал СУС ИБ за исключением функции консолидации информации;

– аварийный режим – режим функционирования системы в случае сбоя (ев)/отказа(ов) одного или нескольких компонентов СУС ИБ. В аварийном режиме должна обеспечиваться сохранность данных при возникновении аварийной ситуации с программно-техническими комплексами СУС ИБ;

– сервисный режим – режим функционирования системы при проведении работ по обслуживанию инфраструктуры СУС ИБ (виртуальной или аппаратной) и обновлению ее компонентов. Сервисный режим должен обеспечивать реализацию основных функций СУС ИБ, за исключением работ, требующих временной приостановки работы компонента(ов) СУС ИБ.

Нарушение штатной работы, включая перерывы и выход за установленные пределы параметров электропитания на время не более 30 минут не должны приводить к:

– появлению ложных сигналов управления;
– потере информации, важной для работы системы управления.

В СУС ИБ должна обеспечиваться сохранность данных при возникновении аварийной ситуации с программно-техническими комплексами СУС ИБ путем резервного копирования и восстановления данных и программного обеспечения. Для этого информационные ресурсы СУС ИБ должны включаться в контур существующих систем резервного копирования.

Все серверные компоненты СУС ИБ должна строится на базе Linux подобных систем и не требовать приобретения дополнительных лицензий.

По окончании действия услуг технической поддержки СУС ИБ система должна сохранять полную работоспособность.

Мониторинг и анализ событий информационной безопасности от контролируемых ресурсов ИТС не должен оказывать отрицательного воздействия с точки зрения скорости исполнения обычных процессов функциональной деятельности подразделений Заказчика.

2.3.3 Требования к структуре СУС ИБ

В СУС ИБ должны быть реализованы следующие функциональные подсистемы:

– Подсистема сбора и обработки событий ИБ;
– Подсистема хранения событий ИБ;
– Подсистема корреляции событий ИБ;
– Подсистема поиска событий и подозрений на инциденты ИБ;
– Подсистема регистрации инцидентов;
– Подсистема обеспечение информационной безопасности самой системы;
– Подсистемы управления.

2.3.4 Требования к функционированию СУС ИБ

СУС ИБ должна обеспечить выполнение следующих функций:

- консолидация и хранение информации о инцидентах ИБ, регистрируемых Системой с целью выявления подозрений на инциденты ИБ;
- анализ информации о подозрениях на инциденты ИБ с целью их подтверждения и назначения для последующего реагирования;
- сбор и систематизация данных для проведения специалистами по ИБ последующего анализа причин и источников инцидентов информационной безопасности для определения корректирующих действий по снижению вероятности наступления аналогичных инцидентов информационной безопасности в будущем;
- обобщенное представление информации о выявленных в ИТС подозрениях на инциденты ИБ на единой консоли СУС ИБ;
- уведомление ответственных сотрудников ИБ об обнаружении инцидентов/подозрений на инцидент;
- администрирование компонентов СУС ИБ;
- мониторинг состояния, устранение сбоев и отказов компонентов СУС ИБ;
- поддержка иерархической структуры с назначением головной и подчиненных площадок СУС ИБ

2.3.5 Требования к функциональным подсистемам

Реализация функциональных подсистем должна учитывать иерархическую структуру СУС ИБ в целом.

Проектные решения по созданию СУС ИБ должны предусматривать возможность поэтапного внедрения и интегрирования функциональных подсистем. Решения по обеспечению информационного взаимодействия между функциональными уровнями и подсистемами СУС ИБ, а также с объектами контроля не должны предусматривать создания дублирующих по отношению к уже созданным сетевых и телекоммуникационных инфраструктур.

2.3.5.1 Подсистема сбора и обработки событий ИБ

Подсистема сбора и обработки событий ИБ должна обеспечивать реализацию следующего набора типовых действий:

- сбор и обработка **не менее 2000** событий в секунду;
- автоматизированный сбор и нормализация событий ИБ, включая:
  - присвоение событиям категорий в соответствии с типом зарегистрированного события;
  - присвоение событию степени критичности, управляемой администраторами СУС ИБ;
  - приведение событий ИБ к единому формату СУС ИБ;
  - обогащение событий (запись пользовательских значений в любое поле события) на основании пользовательских правил;
  - сохранение исходного события и нормализованного.
  - нормализация объединенного потока событий от различных источников;

– передача информации о событиях ИБ в подсистему управления инцидентами ИБ, подсистему хранения событий ИБ;
– поддержка передачи событий в другие системы;
– возможность передачи событий в нормализованном и сыром формате, в том числе по заданному условию;
– события должны содержать как минимум следующую информацию:
  - дата и время возникновения события;
  - источник (IP-адрес или сетевое имя);
  - уникальный идентификатор события;
  - тип (категория) события;
  - описание события;
  - критичность (приоритет) события;
  - время получения события от источника;
  - дополнительные поля.

Информация об источнике события должна быть представлена в формате IPv4 и IPv6-адресации, либо в формате DNS-hostname.

Информация о внешних IP адресах должна быть также представлена в виде геопозиционных меток (страна, город, координаты местонахождения).

Дополнительные поля таксономии могут содержать информацию о протоколах прикладного уровня, MAC-адресах, DNS-адресах, файловых доступах, различные переменные и т.д. Должна допускаться возможность расширения схемы полей таксономии администраторами СУС ИБ.

Подсистема сбора должна иметь унифицированные транспорты для сбора событий и допускать подключение новых источников администраторами СУС ИБ без привлечения сторонних организаций и разработчиков.

Подсистема должна обеспечивать мониторинг syslog источников.

Подсистема должна обеспечивать возможность разработки правил нормализации событий для существующих полей таксономии с использованием встроенного инструментария и не требовать привлечения разработчиков.

Подсистема сбора должна автоматически применять соответствующие формулы нормализации, без необходимости настройки типа источника или вендора в СУС ИБ.

Подсистема должна гарантировать кэширование событий на агенте, при потере связи с центральным компонентом СУС ИБ.

Подсистема должна обеспечивать автоматическую однопоточную и многопоточную архивацию и шифрование событий при передаче их с агента СУС ИБ.

При сборе событий с использованием агента СУС ИБ должна иметь возможность настраивать модули по умолчанию, автоматически подключаемые настройки сбора для всех новых агентов.

Экземпляр агента СУС ИБ должен иметь возможность сбора данных с не менее чем 20 различных типов источников событий одновременно.

Экземпляр агента СУС ИБ должен предоставлять возможность удаленно расширить аудит на источнике событий без необходимости настройки самого источника.

В рамках иерархической структуры СУС ИБ должны быть реализованы следующие варианты хранения и передачи событий:

- хранение событий на подчиненных площадках;
- передача всех событий с подчиненных площадок на головную.

2.3.5.2 Подсистема хранения событий ИБ

Подсистема хранения событий ИБ должна быть реализована в виде единого распределенного хранилища на базе Elasticsearch и обеспечивать реализацию следующего набора типовых действий:

- выделение отдельного сервера управления, при необходимости, для оптимизации нагрузки;
- выделения отдельного сервера индексирования, при необходимости, для оптимизации нагрузки;
- долгосрочное хранение событий ИБ как в нормализованном, так и в исходном виде;
- хранение событий ИБ в сжатом виде для экономии объема требуемого места в хранилище;
- возможность хранения событий как на локальных, так и на внешних (сетевых) хранилищах;
- адаптация системы хранения событий ИБ под разные часовые пояса (отображение всех событий в едином временном пространстве);
- распределенное хранение событий без консолидации в единое хранилище с возможностью оперативного доступа ко всем событиям из единой консоли;
- возможность распределенного поиска по всем событиям в едином запросе без передачи события в единое хранилище;
- долгосрочное хранение событий с оперативным доступом к любым событиям на всем интервале хранения;
- сокращение объемов хранения за счет автоматической очистки несущественных и информационных данных на основе заданной и управляемой администраторами СУС ИБ критичности событий;
- автоматическая очистка хранилища от неинформативных событий;
- возможность установки глубины хранения пользователем для всех типов событий;
- автоматическое восстановление базы данных после сбоев.

Хранилище системы СУС ИБ должно обеспечивать хранение оперативной информации за период не менее 1 последнего месяца.

Должна быть обеспечена возможность последующего увеличения емкости хранилищ без изменения всей архитектуры решения (горизонтальное масштабирование).

Подсистема должна обеспечивать использование «Горячих серверов хранения» обеспечивающей хранение событий, к которым необходим оперативный доступ и «Холодных серверов хранения» для хранения событий, доступ к которым постоянно не требуется.

Подсистема хранения должна иметь возможность горизонтального масштабирования путем ввода новых серверов хранения событий, без привлечения сторонних организаций и разработчиков.

Подсистема хранения должна включать в себя модуль архивации, обладающий следующим функционалом:

1) Модуль должен обеспечивать возможность автоматической однопоточной и многопоточной архивации событий с выгрузкой их в отдельные файлы на сетевом хранилище.
2) Модуль должен обеспечивать возможность настройки глубины хранения событий в системе – события старше указанного срока должны автоматически выгружаться в архив
3) Модуль должен обеспечивать возможность просмотра имеющихся архивов, возможность временного подключения архива к системе для оперативной работы с ним, возможность отключения архива от системы после его использования.
4) Модуль должен обеспечивать возможность нескольких видов архивации событий – режим быстрой архивации с минимальной степенью сжатия и медленной архивации с большей степенью сжатия – не менее 7 раз от размера событий в системе.
5) Модуль должен обеспечивать возможность автоматического мониторинга состояния подключенного сетевого хранилища с предупреждением в интерфейсе в случае его недоступности.

Подсистема хранения должна включать в себя модуль агрегации событий, обладающий следующим функционалом:

1) Модуль должен уменьшать объема хранилища событий (ElasticSearch);
2) Модуль должен обеспечивать прекращение хранения однотипных и неважных событий;
3) Модуль должен обеспечивать возможность создания и корректировки правил агрегации в графическом конструкторе без знания языков программирования;
4) Модуль должен хранить первое и последнее события, содержащие временные метки всех подобных событий.

Подсистема хранения должна включать в себя модуль фильтрации приходящих событий:

1) Модуль должен обеспечивать фильтрацию событий по созданным правилам фильтрации;
2) Модуль должен осуществлять экспорт и импорт правил фильтрации;

3) Модуль должен обеспечивать возможность создания и корректировки правил фильтрации в графическом конструкторе без знания языков программирования;

4) Модуль должен обеспечивать копирование правил фильтрации на подчиненные ноды при режиме Multitenancy.

2.3.5.3 Подсистема корреляции событий ИБ

Подсистема корреляции событий ИБ должна обеспечивать реализацию следующего набора типовых действий:

- выявление подозрений на инциденты ИБ посредством корреляции событий ИБ по заданным в СУС ИБ правилам. Должны выявляться подозрения на следующие инциденты, включая, но не ограничиваясь:
  - превышение числа указанного количества попыток неуспешного доступа;
  - успешных вход под учетной записью после многочисленных неуспешных попыток;
  - попытки подбора пароля к сервисам удаленного управления серверов и сетевого оборудования, а также для критичных учетных записей;
  - блокирование учетной записи после многочисленных неуспешных попыток;
  - блокирование критичной/сервисной учетной записи по превышению лимита неудачных входов;
  - интерактивный вход под служебной/сервисной учетной записью;
  - попытки входа под несуществующей учетной записью;
  - попытки входа под заблокированной учетной записью;
  - удаленный/интерактивный вход на критичные ресурсы под учетными записями, не перечисленными в указанном списке;
  - изменение или создание учетных записей пользователями, не входящими в доверенную группу;
  - изменение учетных записей и групп вне рабочего времени;
  - изменение сервисных учетных записей;
  - вход с использованием привилегированных или сервисных учетных записей, в том числе в нерабочие часы;
  - массовое изменение учетных записей и групп;
  - включение опции Password Never Expires;
  - очистка журналов событий;
  - превышение допустимого числа запрещенных межсетевым экраном соединений;
  - превышение допустимого числа сброшенных соединений;
  - превышение допустимого числа неустановленных соединений;
  - многочисленные ошибки доступа к источнику (нет прав доступа).
- создание корреляций по историческим данным (хранящимся в системе) с использованием всех доступных функций корреляции без необходимости установки дополнительных модулей;
- историческая корреляция должна иметь функционал ручного и автоматического запуска;
- создание и корректировка правил корреляции событий ИБ в графическом конструкторе без знания языков программирования;
- установка приоритета инцидента, регистрируемого в результате срабатывания правила корреляции;

- установка категории инцидента, в соответствии со следующей классификацией:
  - Кибератаки:
    - Использование ОИИ для осуществления кибератак и (или) распространения вредоносных программ;
    - Прекращение функционирования ОИИ, вызванное кибератакой «отказ в обслуживании»;
    - Многочисленные неуспешные попытки авторизации к ОИИ;
    - Попытки внедрения ВПО на ОИИ;
    - Проведение кибератаки «отказ в обслуживании», направленной на ОИИ, не вызвавшей негативных последствий;
    - Попытки эксплуатации уязвимости на ОИИ;
    - Нерегламентированное сетевое сканирование ОИИ;
    - Попытки проведения кибератаки на веб-приложения и иные сетевые протоколы и службы;
    - Использование вычислительных мощностей ОИИ для проведения кибератак.
  - Киберинциденты:
    - Внедрение и функционирование ВПО на ОИИ;
    - Попытка использования ОИИ для распространения ВПО;
    - Прослушивание, захват, перенаправление сетевого трафика ОИИ;
    - Рассылка спам-сообщений, фишинговых писем с ОИИ;
    - Компрометация учетных записей привилегированных пользователей;
    - Несанкционированное изменение информации;
    - Нарушение порядка хранения и обработки информации ограниченного распространения (во внешней и внутренней сети);
    - Несанкционированный доступ к ОИИ, в том числе к средствам защиты информации, с использованием информационно-коммуникационных технологий;
    - Успешная эксплуатация уязвимостей на ОИИ;
    - Несанкционированное подключение каналообразующих устройств к ОИИ;
    - Создание нерегламентированного файлообменного сервиса;
    - Использование нерегламентированного ПО;
    - Попытка несанкционированного доступа к ОИИ;
    - Несанкционированное заведение учетных записей, повышение привилегий учетных записей пользователей;
    - Очистка журналов безопасности ОС;
    - Удаление СЗИ с АРМ.
  - Сбои работоспособности оборудования и ПО:
    - Системные сбои и перегрузки ИС;
    - Сбои программного обеспечения или отказы технических средств.
- установки зоны видимости инцидента на основе ролевой модели применительно к каждому правилу корреляции;
- возможность использования в правилах корреляции изменяемых пользователем статических списков;
- возможность использования в правилах корреляции динамических списков;
- возможность использования в правилах корреляции динамических таблиц;

- установка временных ограничительных параметров срабатывания правила корреляции;
- автоматическая регистрация выявленных подозрений на инциденты ИБ, оповещение об их выявлении ответственных лиц и передача их в подсистему хранения;
- приоритезация выявленных подозрений на инциденты ИБ с учетом критичности событий ИБ, вызвавших данный инцидент и критичности ресурсов, затронутых им;
- автоматические механизмы поиска событий и подозрений на инциденты ИБ по заданным критериям и значениям полей событий без создания правил корреляции для каждого конкретного типа инцидентов;
- формирование пользовательского события в результате срабатывания правила корреляции;
- проактивные сценарии при срабатывании правила корреляции;
- передача в проактивные сценарии одиночных значений или массивов имен пользователей, исходных IP адресов, прочих переменных, фигурирующих в инциденте;
- отправка уведомления о регистрации инцидента по электронной почте сотрудникам, не имеющих доступа к системе;

Подсистема корреляции событий ИБ должна обеспечивать корреляцию:

- по отдельным событиям;
- по количеству событий за интервал времени;
- по количеству уникальных значений за интервал времени;
- по последовательности действий.

Подсистема корреляции должна обеспечивать выполнение следующих функций:

- возможность использования категории события для дальнейшего использования в правилах корреляции, вместо перечисления id конкретных событий;
- возможность использования уровня критичности события;
- использование операций равенства "Значения";
- использование операций больше "Значения";
- использование операций больше или равно "Значения";
- использование операций меньше "Значения";
- использование операций меньше или равно "Значения";
- использование операция строкового равенства "Значения";
- использование операция строкового неравенства "Значения";
- сравнение (равенство) не зависимо от регистра значений в поле;
- сравнение (неравенство) не зависимо от регистра значений в поле;
- поиск неполного значения;
- сравнение поля (значения) за временной диапазон. Фиксация изменений;
- Значение в поле начинается с определенного значения;
- проверка наличия значения в поле (поле не пустое);
- проверка отсутствия значения в поле (пустое поле);
- значение из поля входит в указанный список или списки, как в статические, так и динамические
- значение из поля не входит в указанный список или списки;

- проверка наличия определённого поля в событии;
- проверка отсутствия определённого поля в событии;
- проверка наличия инцидентов по значению в указанном поле;
- использования отрицания к определенному условию или группе условий;
- проверка доменных имен на вредоносность;
- поиск в списках не зависимо от регистра значений;
- сравнение (равенство) значения и поля;
- сравнение (неравенство) значения и поля;
- поиск подстроки по значениям статических списков;
- копирование списков на подчиненные ноды при режиме Multitenancy;
- постраничный поиск значений статического списка;
- сортировка значений таблиц;
- массовое удаление значений таблиц;
- вывод правил со статическими списками.

Подсистема должна обеспечивать агрегацию инцидентов. Агрегация должна осуществляться при совпадении значений любых заданных администратором полей событий. При регистрации большого количества однотипных событий, превышающего количественные значения правила корреляции, должен быть создан только один инцидент.

Подсистема должна обеспечивать возможность добавления информации в динамические списки и удаления информации из них.

Подсистема должна обеспечивать хранение событий вызвавший инцидент в отдельной базе данных.

Администраторы СУС ИБ должны иметь возможность:

- включения и отключения отдельных правил корреляции;
- копирования правила корреляции с созданием нового без повторного написания условия;
- добавление категории инцидентов к правилу корреляции;
- изменения пользовательского правила корреляции с уточнением его условия;
- экспортировать и импортировать правила корреляции;
- привязка событий к инцидентам, созданным вручную;
- экспортировать содержимое статических и динамических таблиц.

Условие правила корреляции должно трактоваться однозначно, быть интуитивно понятным.

Подсистема должна иметь возможность использовать любые поля событий из таксономии.

В рамках иерархической структуры СУС ИБ должна быть обеспечена следующая логика работы подсистемы корреляции событий ИБ:

- в случае работы подсистемы корреляции на стороне головной площадки корреляция должна осуществляться независимо по каждой из подчиненных площадок;

– в случае работы подсистемы корреляции на стороне подчиненной площадки должна быть обеспечена возможность передачи правил корреляции с головной площадки на подчиненные с возможностью выбора пользователем площадок, на которые необходимо передать правила.

2.3.5.4 Подсистема поиска событий и подозрений на инциденты ИБ

Подсистема поиска событий и подозрений на инциденты ИБ должна обеспечивать реализацию следующего набора типовых действий:

– формирование графических представлений и визуализаций данных в событиях;
– сортировка и группировка событий;
– отображение нормализованных событий с выводом указанной последовательности и набора полей;
– изменение очередности и количества выводимых полей при детальном просмотре событий;
– группировка по указанному пользователем полю;
– создание сохраненных фильтров просмотра событий пользователями и администраторами;
– использование составных поисковых запросов;
– поиск событий без знания текста события, по категориям и критериям;
– возможность использования логических операторов;
– выгрузка событий по фильтрам с указанными полями и их очередностью;
– гибкое формирование отчетов по событиям на базе поисковых запросов;
– поиск событий ИБ, связанных с конкретным подозрением на инцидент ИБ;
– сортировка событий по каждому из возможных полей;
– полнотекстовый поиск по сырым событиям;
– перемещение по событиям клавишами ↑ и ↓;
– группировка поля события, при детальном его просмотре.
– отображение порядка групп полей в соответствии с уровнем важности;
– визуальное построение взаимосвязей между событиями по произвольным полям;
– запоминание последнего фильтра, введенного во взаимосвязях;
– поиск по всем подключенным средствам хранения событий;
– полнотекстовой поиск по событиям, с возможностью использования логических операторов, а также преобразования результатов в диаграммы на лету без необходимости создания отчетов или инструментальных панелей.

В рамках иерархической структуры СУС ИБ подсистема поиска событий должна обеспечивать возможность распределенного поиска событий по всех подчиненным площадкам из интерфейса управления головной площадки.

В рамках иерархической структуры СУС ИБ должна быть обеспечена возможность разграничения доступа пользователей головной площадки СУС ИБ к событиям каждой из подчиненных площадок.

2.3.5.5 Подсистема регистрации инцидентов ИБ

Подсистема регистрации инцидентов безопасности СУС ИБ должна быть выполнена в виде единого решения с остальными подсистемами в единой консоли управления.

Подсистема регистрации инцидентов должна обеспечивать реализацию следующих типовых действий:

- ведение процессов инцидент-менеджмента согласно стандарту ITIL;
- создание инцидента вручную;
- регистрация инцидентов в результате срабатывания по правилам корреляции;
- ролевое разделение доступа к инцидентам;
- разделение доступа по группам и пользователям системы на основе условий, задаваемых в правилах корреляции;
- постановка задач сотрудникам и группам в рамках инцидентов;
- оповещение посредством электронной почты о назначенных инцидентах;
- оповещение посредством электронной почты о поставленных задачах в рамках инцидентов;
- звуковое оповещение о новом инциденте;
- уведомления для инцидентов, созданных вручную;
- постановка задач сотрудникам, не имеющим доступа к инциденту с изменением зоны видимости инцидента;
- эскалация инцидентов с изменением зоны видимости инцидентов;
- поиск и навигация по событиям, попавшим под инцидент;
- повторное открытие ранее закрытого инцидента при его повторном возникновении;
- навигация по закрытым инцидентам;
- просмотр решения инцидентов;
- просмотр истории инцидента;
- возможность массового изменения статуса инцидентов;
- должен обеспечиваться функционал добавления информации в инцидент при ведении расследования;
- отображение событий, вызвавших инцидент и обеспечение поиска, сортировки и группировки полей событий в карточке инцидента;
- привязка событий к инцидентам, созданным вручную;
- удаление определённых инцидентов из системы и всех инцидентов с удалением всей информации об инцидент и событий, связанных с ними, без удаления событий из централизованного хранилища;
- массовое удаление инцидентов, сгруппированных по тенанту (при включенном режиме Multitenancy), по наименованию или по категории;
- в рамках иерархической структуры СУС ИБ:
  - должна осуществляться автоматическая передача карточек инцидентов с подчиненных площадок на головную;
  - должна быть обеспечена возможность разграничения доступа пользователей головной площадки СУС ИБ к карточкам инцидентов каждой из подчиненных площадок.
- возможность создавать, отслеживать, назначать, удалять задачи по инцидентам;

- отображение идентификатора инцидента;
- закрытие инцидента из головной ноды (при режиме Multitenancy);
- экспорт инцидентов в формате json.

Функционал удаления инцидентов должен иметь возможность ограничения определенными ролей пользователей или отключения данного функционала для всех пользователей СУС ИБ.

Инциденты информационной безопасности, равно как и связанные с ними события должны храниться в системе не менее 1 года, не зависимо от срока хранения обычных сырых и нормализованных событий в системе.

2.3.5.6 Подсистема информационной безопасности

Подсистема информационной безопасности СУС ИБ должна обеспечивать реализацию следующих действий:

- аутентификация пользователей посредством встроенных механизмов, интеграции с LDAP и гибридной аутентификации;
- разграничение доступа к функциям и информации, обрабатываемой в СУС ИБ посредством ролевой модели;
- логирование входов и действий обслуживающего персонала СУС ИБ;
- защита от несанкционированного доступа к информации, находящейся в СУС ИБ;
- регистрация и предотвращение попыток несанкционированного доступа к средствам контроля и контролируемой информации;
- ограничение количества неуспешных попыток входа в СУС ИБ;
- настройка парольных политик пользователей СУС ИБ;
- ограничение количества параллельных сеансов доступа в СУС ИБ;
- контроль целостность компонентов СУС ИБ и уведомление пользователя в случае нарушения целостности.

2.3.5.6 Подсистема управления

Управление СУС ИБ осуществляется посредством графического веб-интерфейса, адаптированного под использование с различных веб-браузеров и мобильных устройств.

Интерфейс должен отображать текущее состояние всех компонентов системы и текущую нагрузку на ресурсы системы СУС ИБ, такие как CPU, память, диск.

Интерфейс должен позволять пользователям создавать и формировать отчеты с возможностью визуализации данных с помощью таблиц и диаграмм.

Интерфейс должен позволять отображать текущее количество инцидентов, графики по возникновению инцидентов с разведкой по времени и обеспечивать формирование отчетов по инцидентам с возможностью выбора полей инцидентов.

Подсистема управления должна обеспечивать возможность управления настройками и правилами корреляции на всех серверах СУС ИБ из единой консоли.

Подсистема должна обеспечивать управление обновлением системы, в случае доступности обновления, подсистема должна отображать список изменений в версии. Обновление системы должно обеспечиваться автоматически, без необходимости остановки системы или отдельных ее компонентов. Обновление компонентов СУС ИБ может включать исправление работы СУС ИБ, новый функционал, обновление правил корреляции и нормализации. Все новые правила корреляции и нормализации, полученные в рамках обновлении системы, должны быть активны по умолчанию, без необходимости взаимодействия с пользователем.

Подсистема должна обеспечивать отображение состояния системы хранения и текущую ее загрузку. В случае использования кластерной сборки системы хранения, подсистема должна обеспечивать отображение состояния каждой ноды в отдельности.

Подсистема должна обеспечивать централизованное хранение всех лицензий компонентов СУС ИБ (нод) в едином интерфейсе.

Подсистема должна обеспечивать отображение на головной ноде статуса лицензий на подчиненных нодах.

Подсистема должна обеспечивать функционал множественной активации и деактивации правил корреляции и нормализации событий.

Подсистема должна обеспечивать отображение статуса активации и деактивации правил, а также отображать статус наличия ошибок корреляции и нормализации.

Подсистема должна иметь функционал передачи парсеров на подчинённые компоненты сбора событий.

В рамках иерархической структуры СУС ИБ подсистема должна иметь функционал передачи пользовательских парсеров на подчинённые площадки.

Подсистема должна обеспечивать хранение и отображение списков в системе. Обеспечивать поиск по значениям в списке. В случае удаления из системы списка, используемого в корреляциях, система должна ограничивать удаление данного списка с отображением списка корреляция, где он используется.

Подсистема должна обеспечивать функционал автоматического удаления записей из списков по истечению времени или отсутствую обновлений данных в списке (TTL).

Подсистема должна обеспечивать возможность отображения состояния подсистемы Хранения событий в веб интерфейсе.

Подсистема должна обеспечивать возможность диагностики правил нормализации с возможностью выявления событий, влияющую на производительность системы.

Подсистема должна обеспечивать возможность сбора статистики по правилам корреляции, включая время выполнения правил корреляции, и количество инцидентов, сгенерированных правилами и созданными вручную.

Подсистема должна обеспечивать возможность сбора статистики по парсерам, включая количество прошедших событий, процессорное время и общее время выполнения по каждому парсеру.

Подсистема должна обеспечивать массовое удаление агентов, экспорт списка агентов и модулей, групповое управление агентами, шаблоны настроек модулей агентов.

Подсистема должна обеспечивать управление локальной базой агента.

2.3.6 Требования к интеграции СУС ИБ

Технические решения по интеграции функциональных подсистем должны быть унифицированы и обеспечивать масштабируемость, наращиваемость и дальнейшее совершенствование СУС ИБ при развитии ИТС.

Агент СУС ИБ должен включать в себя компонент сбора низкоуровневых событий с ядра ОС. Данный компонент должен включаться/выключаться для каждой установки агента СУС ИБ через центральный интерфейс СУС ИБ.

Источники событий должны интегрироваться с платформой СУС ИБ одним из следующих способов:

- сбор событий по протоколу syslog, netflow, snmp;
- Сбор событий с компонента, собирающего информацию о низкоуровневых событиях ядра ОС.
- сбор событий, хранящихся в лог-файлах локально и на сетевых ресурсах (SMB, FTP);
- сбор событий, хранящихся в журналах hpe Event Log;
- сбор событий, хранящихся в БД MS SQL, Oracle, MySQL, PostgreSQL;
- сбор информации об установленном ПО и патчах на ОС Windows;
- сбор информации по произвольным WMI запросам;
- сбор событий посредством проприетарных протоколов, используемых соответствующими источниками: Cisco SDEE, Checkpoint OPSEC, Amazon Web Services;
- сбор результатов выполнения команд на удаленном хосте по протоколу SSH;
- сбор результатов выполнения команд на удаленном хосте по протоколу Telnet;
- сбор событий посредством REST API (также возможность получения EPS по Rest API-запросу).

СУС БД должна иметь функционал отделяемых компонентов, обеспечивающий сбор и нормализацию событий без необходимости приобретения дополнительных лицензий.

При передаче событий должна обеспечиваться их целостность и гарантированная доставка в хранилище.

Должно быть предусмотрено временное хранилище при невозможности передачи событий, собранных с источников. При этом, должна обеспечиваться целостность и неизменность событий.

В случае превышения лицензионных ограничений система не должна прерывать процесс сбора событий с источников данных без ограничения сроков, прошедших с момента выявления этих ограничений системой.

В случае избыточной нагрузки, система должна уметь буферизовать поступающий поток во избежание потерь событий и распределения оптимальной нагрузки. СУС ИБ должна содержать инструментарий подключения новых источников событий через поддерживаемые транспорты, доступные через интерфейс пользователя.

СУС ИБ должна обеспечивать функционал импорта данных в списки, используемые в системе из командной строки или с использованием RestAPI.

СУС ИБ должна обеспечиваться возможность передачи инцидентов и событий инцидентов во внешние системы с использование RestAPI.

2.3.5.7 Список основных поддерживаемых источников

• 1C 8.3 • 1C Bitrix • 3Com • Abrt-server • Aide • Algosec FW Analyzer • Allied telesis • Amavis • Anacron • Aoavt • Apache web server (syslog) • A-real	• Clearswift Secure Email Gateway • Communigate • Courier-MTA • Cowrie • CrushFTP • Cybertec-Postgresql • CyberProtego • DallasLock • dbus-daemon • DejaVU (engine) • Dell • Diasoft • Distkontrol	• Gitolite over syslog • Gnome-shell • Grafana • Group-ib Bot-Trek TDS (cef, json) • Haproxy • hMailServer • HPE • IBM BladeCenter Switch • IBM Storage Networking • Ideco • IDS HS

- Arbor Networks
- Arp-scan
- Asterisk
- Atlassian
- AuditD
- Avaya
- Bastion
- Bastion-tech
- BDCom
- Bind
- Bluecoat
- Bolid Orion
- Brocade switch
- Bro-ids
- Caddy
- CEF syslog
- CentOS
- Checkpoint
- Cisco
  - Cisco ASA 5/6
  - Cisco ASA Firepower
  - Cisco Catalyst
  - Cisco Email Security Appliance (ironport)
  - Cisco FW
  - Cisco IPS
  - Cisco NGIPS
  - Cisco PIX
  - Cisco WLC
  - Cisco WSA
  - Cisco firepower
- Linux Monit
- Linux postmaster
- Linux/Unix/BSD/Suse syslog
- Mac OS over syslog
- D-LINK
- DLP DeviceLock 8.3
- Dnsmasq
- Docker
- Dovecot (syslog)
- Drupal
- DrWeb
- DWDM Volga
- Echelon (Scaner-VS)
- Elastic auditbeat (Filelog)
- Eltex
- ESET Endpoint Security
- EtherStat Microolap Technologies
- Exim
- Extreme Networks
- F5 (ASM)
- fail2ban (syslog)
- failoverd
- Falcongaze
- Filelog (IIS)
- Forcepoint
  - Forcepoint NGFW 6x (LEEF/CEF)
- Fortinet
  - Fortinet Fortianalyzer (syslog)
  - Fortinet Fortigate (syslog, cef)
  - Fortinet FortiMail
- FreeRADIUS
- Gamma(krechet)
- Maipu
- ManageEngine
- Mate
- MDeamon
- Indeed
- Infotecs (требуется наличие ПО ViPNet StateWatcher)
  - InfoTecs VipNet Coordinator
  - InfoTecs VipNet IDS
  - Infotecs VipNet TIAS
- Infowatch Traffic Monitor
- Iptables
- Isimplelab
- Juniper
- Kaspersky
  - Kaspersky Antitarget Attack Platform
  - Kaspersky Secure Mail Gateway
  - Kaspersky Security Center CEF/LEEF
  - Kaspersky Security Center Syslog
  - Kaspersky (KLMS)
- Keepalived
- Kerio
- Kiwi solarwinds
- Klnagent
- Kron
- Kubernetes
- Laurel
- Mysql over syslog
- Named
- Netflow
- Netgate

- McAfee Email Gateway (syslog, CEF, splunk)
- McAfee ESM
  - McAfee Firewall (LEEF)
  - McAfee GTI (global threat exchange) parser splunk format
  - McAfee IPS (LEEF, CEF)
  - McAfee NGFW (CEF)
  - McAfee Web Gateway (syslog)
- Poligon
- Positive
- Postfix over syslog
- Postgresql
- Proxmox (PVE)
- PSQL
- PTAF
- Python
- Qnap
- Qtech
- Safeinspect (syslog plain/CEF)
- Safib
- SDEE (http/https)
- SearchInform
- Security code (vGate)
- Sendmail
- Session watcher
- Shtormtech
- SNORT (syslog)
- SNR
- Ubiquiti
- Ubiquiti UniFi AP LR
- Merak mail server
- Microsoft Windows
- Mikrolink
- Mikrotik: DNS, SMB, web-proxy
- Modsecurity
- Maipu
- ManageEngine
- Mate
- MDeamon
- Merak mail server
- Microsoft Windows
- Mikrolink
- Mikrotik: DNS, SMB, web-proxy
- Modsecurity
- Multifactor
- Radware Defence pro
- RedHat
- RedHat IDM
- RNT Forpost Monitoring
- Rspamp
- LogAgent
- Rusiem
- SolidSoft
- Sophos Antivirus
- Sophos XG Firewall SFVH
- Spectrum
- Squid
- Ssec
- Ssecline
- SSH (LogAgent)
- Sshd
- Staffcop
- S-terra
- Stonegate Stonesoft
- Suricata (syslog+CEF)
- Netlogon
- Network Manager
- NewSecurity
- NextCloud
- Nginx
  - Nginx over syslog
- NInetlabs unbound
- NSD (Transit 2.0)
- Ntpd
- ODBC
- OpenVAS
- OpenVPN
- Oracle Audit
- OracleDB for Linux
- Ossec
- PaloAlto (CEF, LEEF)
- Panda Antivirus
- Pcp
- Pgsql
- Php-fpm 7.1
- Symantec (over MS SQL)
- Symantec Endpoint Protection
- Synology
- Sysco
- Syslog (tcp/udp)
- Syslog TLS
- Sysmon (LogAgent)
- System info (LogAgent)
- Systemd
- systemd-resolved
- TrendMicro Control Manager (CEF syslog)
- TrendMicro Proxy IWSVA (syslog)
- Tripwire (enterprise)
- Xello

• Unlimited
• Useradd
• Userdel
• UserGate
  ○ UserGate NGFW (CEF)
  ○ UserGate UTM (CEF)
• АРМ КБР-Н
• БОСС-кадровик
• ДБО (Бифит)
• КриптоПро NGate
• Маршрутизатор huawei
• Микросервисы RuSIEM
  ○ Cisco BGP
• Система видеонаблюдения Trassir
	• SwordFish
	• vGate
	• VMware ESX
	• VMware ESXi
	• Vsftpd over syslog
	• WAF Fortiweb
	• Watchguard
	• Windows EventLog
	• Windows Task Scheduler
	• Windows Power Shell
	• Windows Message Tracking
	• СКУД SIGUR
	• СКУД RusGuard
	• СКУД Интеллект
	• СЭД TESSA
	• ЦБ РМ КБР-Н
		• Yum
		• Zabbix
		• Zalando
		• Zecurion
		• Zimbra
		• Zyxel
		• АудитПлюс
		• АПКШ “Континент” 3.9, 4
		• СКУД Сфинкс

2.3.5.7 Перечень поддерживаемых протоколов (транспортов) сбора событий:

• Microsoft Windows standard event logs (System/Applications/Security) • Microsoft Windows custom event logs • Microsoft Windows applications event logs • Microsoft Windows softwares list • Microsoft Windows patches list • Microsoft Windows WMI command (get answer to events) • Hasher for Windows (get processes, its hashes to events) • ms evt and wmi transport • Microsoft SQL (tables, views) — any logs • Secure Shell Protocol (ssh) • Telnet	• SysMon • Oracle — any logs, Oracle Audit trail • MySQL (tables, views) • PostgreSQL • Cisco SDEE • Checkpoint LEA • File — log files over network shares • Ftp — logs into ftp servers • Syslog plain • Syslog TLS • Syslog CEF • Syslog LEEF • NetFlow (3,6,9)

2.3.6 В поставку должны быть включены следующие опции:

-Право на использование SIEM-системы (лицензии) — лицензия - **бессрочно**. В стоимость лицензии должно быть включено оказание технической поддержки и доступ к обновлениям - **не менее 36 месяцев.**

- Лицензирование СУС ИБ должно осуществляться по количеству событий в секунду -**не менее 2000**. Количество узлов для сканирования - **не ограничено**.

- Право на использование ПО «Защищённая среда виртуализации» — лицензия - **бессрочно**. В стоимость лицензии должно быть включено оказание технической поддержки и доступ к обновлениям - **не менее 36 месяцев.**

2.3.7 Состав и содержание пуско-наладочных работ в рамках поставки:

- Настройка всех необходимых параметров серверного оборудования, предустановка операционной системы.

- Установка ПО «Защищённая среда виртуализации».

- Внедрение системы управления событиями информационной безопасности (разработка перечня необходимых настроек и выполнение настройки SIEM системы).

- Обучение специалистов заказчика администрированию и использованию SIEM системы.

- Подготовка итогового отчета по проекту внедрения.

3. Дополнительные требования:

- Документ, содержащий информацию о стране производства.

4. Требования по гарантии:

4.1 Гарантийный срок:

Гарантия на аппаратную платформу – **не менее 3-х лет**.

4.2. Срок выполнения работ при возникновении гарантийного случая не более 14 (четырнадцати) календарных дней с момента передачи оборудования. В случае необходимости проведения сложного ремонта срок может быть продлен по письменному согласованию с Заказчиком.

4.3. Наличие пост гарантийного технического обслуживания.

4.4. Авторизованный сервисный центр по обслуживанию, находящийся в г. Минск или Минском районе, либо документы (соглашение, договор и др.) с организацией, осуществляющей сервисное обслуживание в г. Минске или Минском районе.

5. Требования к качеству:

- товар должен быть промаркирован в соответствии с требованиями технических регламентов Таможенного Союза (знаком «ЕАС») и подтверждаться декларацией о соответствии или сертификатом соответствия, сопровождаться эксплуатационной документацией на русском языке.

6. Место, условие и срок поставки: ПАК в течении 40 (сорока) календарных дней с момента подписания договора, срок выполнения пусконаладочных работ 50 (пятидесяти) календарных дней с даты заявки Заказчика.

Доставка товара осуществляется транспортом и за счёт средств Поставщика на склад Заказчика: г. Заславль, ул. Советская, 128.

7. Оплата стоимости ПАК и услуг производится Заказчиком на расчетный счет Поставщика: в размере 80% от стоимости закупки в течение 15 (пятнадцать) банковских дней со дня поставки ПАК на основании счета и оставшейся части в размере 20% от стоимости закупки в течение 15 (пятнадцать) банковских дней со дня выполнения **услуг на пусконаладочные работы** на основании счета. Датой выполнения услуг считается дата подписания **Заказчиком** Акта выполненных услуг.

8. Проверка поступившего товара по качеству, количеству, комплектности, маркировке, легальности установленного ПО осуществляется в соответствии с законодательством Республики Беларусь на складе Заказчика не позднее 5 (пяти) рабочих дней с момента доставки товара на склад Заказчика.

9. Порядок формирования суммы договора на закупку осуществляется с учетом расходов на доставку, страхование, уплату таможенных пошлин, налогов, сборов и других обязательных платежей.

10. Источник финансирования закупки – собственные средства РУП «Минская Фармация».

11. Вид процедуры закупки – запрос ценовых предложений.

Обоснование выбора процедуры закупки – п. 5.3 Порядка осуществления закупок товаров (работ, услуг) за счёт собственных средств РУП «Минская Фармация», так как ориентировочная стоимость закупки от 1000 до 15000 базовых величин.

12. В случае производственной необходимости допускается увеличение/уменьшение суммы договора (до 30%), за счет увеличения/уменьшения предмета закупки, в соответствии с требованиями Порядка осуществления закупок товаров (работ, услуг) за счет собственных средств РУП «Минская Фармация».

13. Критерии для выбора наилучшего предложения: наименьшая цена предложения с учетом полного соответствия требованиям задания на закупку и документации о закупке.

14. Представляемая участником спецификация должна в обязательном порядке содержать полное и точное наименование моделей, используемых комплектующих (развернутую информацию технических характеристик программно-аппаратного комплекса), заявленных в п.2 настоящего задания, цену за единицу товара с НДС и общую стоимость товара с НДС.

Предложение должно содержать цену, представленную в белорусских рублях. Цена предложения должна содержать расходы на доставку, страхование, уплату таможенных пошлин, налогов, сборов и других обязательных платежей. Цена должна оставаться фиксированной в течение всего срока выполнения договора.

Предложение должно содержать информацию, указанную в п.3 задания на закупку.

Предложение должно быть действительно до исполнения всех обязательств по заключенному договора с момента представления предложений.

Подача альтернативных предложений не допускается. Участник в праве предоставить только одно ценовое предложение.

15 Требования к организациям и физическим лицам, включая индивидуальных предпринимателей, которые могут быть участниками процедуры закупки, перечень документов для подтверждения данных участников изложены в Приложении 1.

16. Проведение процедуры закупки возложено на конкурсную комиссию, созданную приказом РУП «Минская Фармация» от 10.07.2026 №159 «О создании комиссии по закупкам».

Начальник отдела
программно-технического обеспечения П.А. Гончарова

Заместитель начальника отдела
программно-технического обеспечения Е.Н. Кучко

СОГЛАСОВАНО:
Заместитель генерального директора
_____ Е.И. Павлюкевич
«24» 07 2026г.