УТВЕРЖДАЮ
Главный врач
УЗ "4-я городская клиническая
больница имени Н.Е. Савченко"
_____ В.В. Сиренко
«____» _____ 2026г.

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ
к предмету закупки

1. Наименование предмета закупки:

программно-аппаратный комплекс «Серверная платформа с системой хранения данных, виртуализацией и системой сбора и анализа событий информационной безопасности» (далее – ПАК) в количестве 1 (одной) штуки.

2. Назначение предмета закупки:

ПАК предназначен для ввода, обработки, хранения и выдачи информационных данных с поддержкой технологий виртуализации вычислительных ресурсов, систем хранения данных и сетей передачи данных, обеспечивает функционирование виртуальных машин и управление ими, обеспечивает работу медицинских информационных систем, обеспечивает сбор и анализ событий информационной безопасности со всей ИТ-инфраструктуры.

3. Требования к предмету закупки.

Предлагаемое техническое решение (ПАК) должно:

состоять из взаимосвязанных и взаимодополняющих компонентов, приобретаемых общим лотом, включающих в себя программные, вычислительные мощности. Компоненты ПАК должны быть полностью совместимы на аппаратном и программном уровнях, обеспечивая совместное функционирование без привлечения дополнительных программных или аппаратных средств, не описанных в настоящем техническом задании;

обеспечивать управление сетевым и межпроцессным взаимодействием между виртуальными машинами и сетевыми службами, создание виртуальных машин с помощью графической и консольных утилит, управление конфигурацией виртуальных машин с помощью графической и консольных утилит;

иметь документы, подтверждающие соответствие аппаратных компонентов, входящих в состав ПАК требованиям ТР ТС 020/2011 «Электромагнитная совместимость технических средств» и ТР ТС 004/2011 «О безопасности низковольтного оборудования»;

иметь сертификаты, подтверждающие соответствие требованиям ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность» на программное обеспечение платформы виртуализации и компьютерную программу, предназначенную для сбора и анализа событий информационной безопасности, входящие в состав ПАК.

4. Состав и архитектура комплекса.

ПАК должен состоять и включать в себя следующие компоненты:

4.1 Аппаратный вычислительный узел (Сервер): 2 шт.;

4.2 Аппаратный модуль хранения данных (Внешняя СХД): 1 шт.;

4.3 Программный модуль гипервизора и кластеризации: Встроенное программное обеспечение (ПО) виртуализации базового уровня (Type-1), включающее в себя функциональные компоненты: модуль гипервизора, диспетчер кластера, подсистему программно-определяемого хранения данных (SDS), подсистему программно-определяемых сетей (SDN), графический веб-интерфейс управления, программный интерфейс API управления, а также встроенные подсистемы мониторинга, аудита и журналирования событий. Накопитель с дистрибутивом облачной платформы виртуализации с действующим сертификатом соответствия ТР 2013/027/BY– 1 шт.;

4.4 Программный модуль анализа безопасности: ПО системы сбора и анализа событий информационной безопасности (класс SIEM) в составе модулей администрирования и управления ролевым доступом, управления инцидентами ИБ, базы знаний с предустановленными правилами корреляции, обогащения поступающих событий, работы с графическими панелями мониторинга (дашбордами), генерации отчетов и отправки уведомлений, запросов и взаимодействия пользователя с системой, хранения событий, файлов и служебных данных, анализа событий и взаимодействия с внешними системами.

5. Технические требования к вычислительным узлам (серверам) — 2 шт.

5.1 Каждая единица серверного оборудования должна иметь характеристики не хуже следующих:

Серверный корпус: форм-фактор 1U Rackmount для монтажа в 19-дюймовую стойку, имеющий до 10 отсеков под установку накопителей формата 2.5" с поддержкой горячей замены (Hot-Swap). В комплекте должны поставляться раздвижные телескопические направляющие (Sliding Rails) для фиксации в шкафу и защитная передняя панель (допускается наличие информационного LCD-дисплея или светодиодной индикации состояния аппаратной платформы на передней панели).

Блок питания: 2 резервируемых блока питания мощностью не менее 800 Вт каждый, с поддержкой горячей замены (Hot-plug) и возможностью автоматической балансировки нагрузки.

Материнская плата и сетевые интерфейсы: двухсокетная архитектура с поддержкой 64-битных серверных процессоров. Наличие интегрированного сетевого адаптера с 2 портами 1GbE. Наличие встроенного выделенного модуля удаленного администрирования и мониторинга аппаратной платформы уровня Enterprise, обеспечивающего независимый доступ к текстовой и графической консоли сервера через HTML5 vKVM, управление электропитанием и перенаправление виртуальных медианосителей. Оптический привод отсутствует (No DVD).

Дополнительные сетевые адаптеры:

дополнительный двухпортовый сетевой адаптер со скоростью передачи данных 10/25 Гбит/с на каждый порт, с разъемами под установку трансиверов SFP28, интерфейс подключения PCIe;

дополнительный двухпортовый интерфейсный адаптер для подключения к сети хранения данных (HBA) Fibre Channel со скоростью передачи данных не менее 8 Гб/с, интерфейс подключения PCIe — 1 шт. на каждый сервер. В комплекте должны поставляться оптические патч-корды для подключения к СХД — 2 шт. на каждый сервер;

дополнительный двухпортовый сетевой адаптер со скоростью передачи данных 10 Гбит/с на каждый порт, стандарта Base-T (разъемы RJ45), специализированного форм-фактора OCP.

процессор: 12-ядерный процессор архитектуры x86-64 с базовой тактовой частотой не менее 2.1 ГГц, объемом кэш-памяти не менее 18 МБ, частотой системной шины не менее 2666 МГц и расчетной тепловой мощностью (TDP) не более 120 Вт — 2 шт. (итого 2 физических процессора на узел).

оперативная память: Модули памяти объемом 32 ГБ типа DDR4 ECC Registered DIMM с частотой функционирования не менее 3200 МГц — 4 шт. (итого не менее 128 ГБ установленной оперативной памяти на каждую единицу серверного оборудования).

RAID-контроллер: Выделенный аппаратный дисковый контроллер с пропускной способностью интерфейса 12 Гб/с, со встроенной энергонезависимой кэш-памятью объемом не менее 8 ГБ, обеспечивающий аппаратную поддержку создания дисковых массивов уровней RAID 0, 1, 5, 6, 10, 50, 60.

накопители SSD (тип 1) — Системные: Твердотельный накопитель класса Enterprise SSD объемом не менее 960 ГБ, интерфейс подключения SATA, обладающий повышенным ресурсом износостойкости (индекс DWPD не менее 5) — 2 шт.

накопители SSD (тип 2) — Данные: Твердотельный накопитель класса Enterprise SSD объемом не менее 1.92 ТБ, интерфейс подключения SAS со скоростью передачи данных 12 Гб/с, оптимизированный для систем с высокой интенсивностью чтения (Read Intensive), в форм-факторе 2.5" с поддержкой горячей замены — 6 шт.

6. Технические требования к внешней системе хранения данных (СХД) — 1 шт.

Входящая в состав ПАК внешняя дисковая подсистема должна обладать облачно-интегрированной унифицированной архитектурой и иметь характеристики не хуже следующих:

Тип архитектуры: единая унифицированная система хранения данных, обеспечивающая одновременную нативную поддержку блочного (Block Storage/SAN), файлового (NAS).

Контроллерная подсистема: наличие двух полностью дублированных аппаратных контроллеров, функционирующих в режиме высокой доступности (отказоустойчивая двухконтроллерная подсистема).

Память контроллеров: наличие установленных модулей памяти типа DDR4 ECC DIMM общим объемом не менее 64 ГБ на систему (4 модуля по 16 ГБ).

Интерфейсы расширения СХД: не менее двух портов расширения со скоростью передачи данных 12 Гб/с SAS на систему для подключения дополнительных дисковых полок.

Базовые порты ввода-вывода: не менее 8 интегрированных портов 1GbE iSCSI для организации сетевого доступа к данным.

Слоты расширения интерфейсов: наличие не менее 4 свободных слотов для установки дополнительных интерфейсных хост-плат.

Дополнительные интерфейсные платы: Ввкомплекте поставки должны быть установлены 2 конвергентные платы расширения хост-интерфейсов, несущие в совокупности не менее 8 портов Fibre Channel (FC) со скоростью передачи данных 8 Гб/с каждый (по 4 порта на плату).

Электропитание и охлаждение: наличие 2 комбинированных резервируемых модулей, каждый из которых сочетает в себе блок питания и вентилятор охлаждения (2x PSU+FAN Module).

Защита кэш-памяти: наличие не менее 2 модулей аварийного резервного копирования кэша, состоящих из суперконденсаторов и плат энергонезависимой Flash-памяти (SuperCap + Flash module) для предотвращения потери данных при аварийном отключении электропитания.

Дисковая емкость и накопители:

Шасси СХД: форм-фактор 4U с возможностью фронтальной установки до 24 накопителей формата 3.5";

Жесткие диски в комплекте: 18 (восемнадцать) жестких дисков корпоративного класса (Enterprise) в форм-факторе 3.5" с интерфейсом SAS 12 Гб/с, скоростью вращения шпинделя 7200 об/мин и емкостью каждого накопителя не менее 20 ТБ;

Комплектация корзин: полный комплект из 24 салазок (лотков) для установки дисков.

Конструктивные элементы: наличие сертифицированного комплекта крепежа (форм-фактор под шкаф 19 дюймов) для монтажа СХД в стойку.

7. Функциональные требования к ПО виртуализации.

7.1. ПО платформы виртуализации должно удовлетворять требованиям:

Использование серверного оборудования для предоставления ресурсов вычисления, сетевых подключений и дисков хранения виртуальных машин (VM Instances).

Запуск нескольких виртуальных машин на одном вычислительном узле (Host).

Объединение вычислительных узлов в логические группы (Clusters) для возможности использования общих ресурсов и единых настроек.

Объединение ресурсов (кластеров, сетевых интерфейсов, хранилищ данных) в логические группы (Zones), таким образом, чтобы ресурсы одной группы не были видны и не могли взаимодействовать с ресурсами, включенными в другую группу.

Предоставление общих вычислительных ресурсов (vCPU, Memory), хранения данных (Storage), сетевых интерфейсов (L2 Network), сетей (L3 Network), сетевых служб (Network Services).

Поддержка LXC системы контейнеризации. Возможность создания контейнеров LXC из образов OCI

Поддержка состояния TPM в формате qcow2.

7.2. Требования к вычислительным ресурсам:

Объединение ресурсов физических серверов (CPU, Memory, Storage) в пулы ресурсов, которые динамически распределяются по запросу.

Для виртуальных машин должны поддерживаться операционные системы Microsoft Windows и основные операционные системы семейства Linux (Debian, Red Hat (RHEL) и Arch Linux).

Поддержка функций перераспределения процессорных ресурсов, объема оперативной памяти, ресурсов хранения.

7.3. Требования к ресурсам хранения:

Возможность предоставления ресурсов хранения (Storage) для размещения данных экземпляров виртуальных машин, данных приложений и пользователей, образов, мгновенных снимков и т.п;

В качестве ресурсов хранения данных должны поддерживаться:

локальные диски;

сетевые хранилища по протоколам блочного доступа iSCSI и Fibre Channel (FC);

сетевые хранилища NFS;

сетевые файловые системы (MooseFS, GlusterFS, OCFS2, GFS2)

распределенные хранилища Ceph.

7.4. Требования к сетевым ресурсам:

Возможность предоставления сетевых ресурсов (Network) и сетевых сервисов (Network Services):

возможность изоляции на канальном уровне (L2 Network): поддержка технологий VLAN, Virtual Extensible LAN (VXLAN);

поддержка сервисов DHCP, DNS для виртуальных сетей;

возможность создания изолированных виртуальных частных сетей (VPC Network);

возможность создания и применения правил сетевой безопасности для групп экземпляров виртуальных машин (Security Group);

возможность создания виртуальных интерфейсов (VIP) и подключение их к виртуальным машинам;

возможность создания виртуальных интерфейсов с функцией трансляции сетевых адресов (Elastic IP) и подключение их к виртуальным машинам;

возможность перенаправления трафика портов указанных публичных IP-адресов на порты соответствующих виртуальных машин (Port forwarding).

Поддержка стека программно-определяемых сетей (SDN). Поддержка создания сетей OpenFabric и OSPF из узлов виртуальной среды.

7.5. Требования к управлению платформой:

Консоль управления должна иметь веб-интерфейс;

Консоль управления должна предоставлять возможность для выполнения всех операций по управлению платформой.

Доступ к управлению платформой должен предоставляться авторизованному пользователю.

Должны поддерживаться функции управления экземпляром виртуальной машины:

создание: выделение процессорных ресурсов, памяти, размера корневого диска, подключение к сетям;

запуск, остановка, перезагрузка, выключение;

создание мгновенных снимков;

создание шаблонов виртуальных;

импорт, экспорт;

удаление, с возможностью восстановления;

подключения/отключения виртуальных дисков (Volume) и образов (ISO).

Должны поддерживаться функции управления виртуальными дисками (Volume):

создание: выбор размера и общего хранилища;

подключение к экземпляру виртуальной машины, отключение;

удаление, с возможностью восстановления.

Должны поддерживаться функции управления образами и шаблонами виртуальных машин (Image):

создание: выбор типа, хранилища, источника загрузки;

удаление, с возможностью восстановления.

Должна сохраняться информация о всех действиях по управлению объектами платформы.

Должна поддерживаться возможность управления с использованием консольных интерфейсов CTL, CLI.

Должен поддерживаться вход в систему с использованием домена OpenID Connect (OIDC).

Пользовательский графический интерфейс (GUI) платформы облачной виртуализации должен обеспечивать выбор русского языка (без использования средств перевода).

Поставщик обязан предоставить программное обеспечение платформы облачной виртуализации в актуальной версии, имеющей действующий сертификат соответствия требованиям технического регламента Республики Беларусь (ТР 2013/027/BY) на дату поставки комплекса.

8. Функциональные требования к по системы сбора и анализа событий ИБ (siem) ПАК

Требования к ПО системы управления и мониторинга событиями информационной безопасности (далее – система):

8.1. Система должна представлять собой компьютерную программу, разворачиваемую на физическом либо виртуальном серверном оборудовании.

Система должна иметь сертификат соответствия требованиям

ТР 2013/027/BY, утверждённого Постановлением Совета Министров Республики Беларусь от 15.05.2013 № 375.

8.2. Система должна быть построена по модульному принципу и позволять её установку и использование в различных конфигурациях.

8.3. Архитектура системы должна включать следующие функциональные компоненты:

модуль администрирования и управления доступом;
модуль управления инцидентами;
модуль базы знаний с правилами;
модуль обогащения событий;
модуль работы с панелью мониторинга;
модуль отчетов;
модуль уведомлений;
модуль запросов;
модуль работы с внешними системами;
модуль хранения событий;
модуль хранения файлов;
модуль хранения служебных данных;
модуль анализа событий;
модуль взаимодействия пользователя с системой.

8.4. Система должна поддерживать установку в распределенных и изолированных сетях без необходимости доступа в Интернет.

8.5. Информационное взаимодействие между компонентами системы должно обеспечиваться с использованием шины передачи данных и веб-служб, работающих на стеке протоколов TCP/IP.

8.6. Централизованное управление системой должно обеспечиваться посредством веб-консоли без установки дополнительного программного обеспечения на автоматизированные рабочие места пользователя системы.

8.7. Графический интерфейс пользователя системы, формируемые системой отчеты, эксплуатационная документация должны быть выполнены на русском языке.

8.8. С помощью функциональных компонентов система должна обеспечивать реализацию следующих возможностей:

сбор событий с различных источников;

анализ событий в соответствии с правилами нормализации и корреляции, а также табличными списками;

управление встроенной базой правил и создание пользовательских правил и табличных списков;

автоматическое и ручное формирование инцидентов;

управление инцидентами, событиями, базой правил, пользователями и ролями, а также другими объектами в Системе;

визуализация данных в виде графиков, диаграмм и таблиц;

формирование и выгрузка отчетов об инцидентах за период времени;

интеграции, в том числе с SOAR-системами;

почтовые уведомления об инцидентах;

мониторинг и индикация состояния Системы;

хранение событий, инцидентов и служебных данных.

8.9. Требования к характеристикам взаимосвязей со смежными системами.

система должна обеспечивать возможность создания, редактирования и удаления интеграций с ограничением срока ее действия.

система должна предоставлять возможность экспорта инцидентов в SOAR-системы с настройкой сопоставления уровня критичности передаваемых инцидентов с их классификацией во внешней системе.

8.10. Требования к режимам функционирования Системы.

Система должна обеспечивать возможность работы в следующих режимах:

штатный режим (непрерывная круглосуточная работа);

сервисный режим;

аварийный режим.

Штатный режим является основным режимом функционирования Системы и характеризуется непрерывной круглосуточной работой и выполнением всех заявленных функций.

Сервисный режим является вспомогательным режимом функционирования для проведения работ по обновлению программного обеспечения, при успешном окончании которых Система возвращается к штатному режиму работы.

Аварийный режим функционирования применяется при обнаружении сбоев и отказов в работе Системы, а также при нарушении функционирования поддерживающей инфраструктуры (сетей электропитания, каналов связи и т.п.).

Должны быть предусмотрены механизмы диагностирования неисправностей в процессе эксплуатации Системы.

Система должна поддерживать возможность обновления конфигурации или перезапуска компонентов, в том числе форсированного.

Система должна обеспечить индикацию собственного состояния и уведомления в интерфейсе Системы о сбоях в работе, критичных для штатного функционирования сервисов.

8.11. Требования к показателям хранения.

Система должна обеспечивать хранение событий ИБ на срок не менее 365 дней.

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

8.12. Требования к защите информации от несанкционированного доступа.

В системе должна быть реализована модель ролевого доступа, обеспечивающая возможность разграничения доступа пользователей к объектам системы и разрешения или запрета выполнения определенных действий путем определения ролей.

Пользовательские учетные записи должны храниться непосредственно во внутренней базе системы в зашифрованном виде в целях предотвращения несанкционированного доступа.

8.13. Требования к надежности.

Система должна сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

перезагрузка серверного оборудования;

временное отсутствие связи с источниками событий;

временное отсутствие связи с компонентами Системы.

Система должна поддерживать восстановление из резервных копий в случае необходимости.

8.14. Требования к функциям системы.

8.14.1 Функции сбора событий.

Система должна обеспечивать удаленный (сетевой) и локальный сбор событий.

Система должна обеспечивать сбор и обработку не менее 500 событий в секунду.

Система должна иметь в своем составе программные сервисы собственной разработки для сбора событий с источников под управлением ОС Windows и их пересылки посредством syslog в формате XML.

Система должна обеспечивать возможность сбора событий в режиме, близком к режиму реального времени.

Управление сбором событий из различных типов источников, централизованная настройка и мониторинг работы модулей сбора событий должно осуществляться из единой консоли.

Система должна обеспечивать стабильную работу с событиями, полученными от источников с некорректным временем.

Система должна позволять подключать источники событий новых типов посредством дополнения множества правил преобразования событий.

Система должна обеспечивать возможность сбора событий по протоколу syslog с использованием одного TCP или UDP порта с двух и более источников событий.

Возможность разработки сервисов для сбора событий с нестандартных источников по договоренности с разработчиком Системы.

Система должна работать 24/7.

8.14.2. Функции обработки событий.

Наличие встроенной базы знаний производителя.

В состав системы должен входить архив с набором правил нормализации и корреляции.

Система должна обеспечивать автоматическую нормализацию событий. Должна быть возможность добавления собственных правил нормализации и изменения существующих.

Система должна обеспечивать поддержку мультиязычных событий.

Система должна обеспечивать возможность корреляции событий в режиме, близком к режиму реального времени.

События должны содержать как минимум следующую информацию:

дата и время возникновения события;

источник (IP-адрес или сетевое имя);

уникальный идентификатор события;

описание события;

время получения события от источника;

дополнительные поля.

В состав Системы должны входить встроенные правила корреляции, обеспечивающие в автоматическом режиме контроль действий пользователей и администраторов, выявление аномалий, включая, но не ограничиваясь:

превышение числа указанного количества попыток неуспешного доступа;

успешный вход под учетной записью после многочисленных неуспешных попыток;

удаленный/интерактивный вход на критичные ресурсы под учетными записями, не перечисленными в указанном списке;

изменение сервисных учетных записей;

контроль учетных записей;

попытки подбора пароля к сервисам удаленного управления серверов и сетевого оборудования, а также для критичных учетных записей;

контроль изменения конфигурации на сетевом оборудовании и серверах;

контроль установки и запуска новых сервисов ОС и сетевых служб.

Система должна обеспечивать функцию многоуровневой корреляции, когда результаты срабатывания правил корреляции подаются на вход другому правилу корреляции.

Система должна предоставлять возможность ручного создания, редактирования и удаления правил нормализации и корреляции, а также табличных списков.

Система должна обеспечивать возможность запуска и остановки работы правил и табличных списков.

В Системе должны быть доступны как экспорт выбранного файла в формате XML или CSV в зависимости от его типа, так и скачивание архива с набором правил.

В Системе должен быть импорт архива с файлами, одного или несколько файлов, а также архива с папками и файлами для сохранения предусмотренной иерархической структуры.

В Системе должна быть предусмотрена отдельная страница с проверкой правил путем ввода события и последующей генерацией результата его обработки.

Система должна обеспечивать хранение как нормализованные (приведенные к единому формату), так и ненормализованные события информационной безопасности (в том виде, в котором они были получены от источника).

8.14.3. Функции управления событиями.

Система должна содержать текстовое описание каждого нормализационного события, предоставленное специалистами аттестованного центра кибербезопасности.

Система должна иметь следующие механизмы для управления событиями:

группировка событий с указанием количества событий в сформированных группах;

фильтрация событий по временному периоду;

быстрый фильтр событий по категории (ненормализованные, нормализованные, все);

быстрое создание фильтра путем одиночного нажатия на основных атрибутах события;

фильтрация событий по заданному набору атрибутов и их значениям с использованием языка запросов;

сохранение пользовательских фильтров;

выгрузка событий в файл в формате CSV;

привязка событий к инциденту.

В Системе должна быть реализована ассоциация события с правилами, на основе которых оно было сформировано.

Система должна иметь следующие механизмы для управления списками запросов:

сохранение пользовательских фильтров;

создание, редактирование и удаление списков;

отнесение запросов к определенному списку;

экспорт и импорт списков запросов.

8.14.4. Функции управления инцидентами.

Система должна обеспечивать автоматическое и ручное формирование инцидентов при обнаружении критичных с точки зрения пользователя событий.

Система должна обеспечивать категорирование инцидентов.

Система должна обеспечивать формирование инцидента с автоматической и ручной привязкой к нему событий.

Система должна обеспечивать просмотр и редактирование карточки инцидента.

Для управления списком инцидентов система должна иметь следующие механизмы:

сортировка инцидентов по полям таблицы («ID», «Название», «Описание», «Критичность», «Статус», «Правило корреляции», «Создал», «Время создания», «Изменил», «Время изменения», «Ответственный», «Адрес источника», «Адрес назначения»);

фильтрация инцидентов по временному периоду;

быстрый фильтр инцидентов по критичности («Низкая», «Средняя», «Высокая») и статусам («Новый», «В работе», «Закрыт», «Закрыт как ложноположительный»);

создание, редактирование и удаление инцидентов;

создание комментариев к инциденту;

назначение пользователя, ответственного за расследование инцидента информационной безопасности.

В системе должна быть реализована ассоциация инцидента с событиями и правилами, на основе которых он был сформирован.

Система должна обеспечивать наличие журнала изменений инцидента для регистрации изменений атрибутов и состояний инцидента.

Функции отправки уведомлений.

Система должна обеспечивать возможность формирования и отправки уведомлений по электронной почте:

инцидентах — при их попадании под системный или пользовательский фильтр;

состоянии Системы.

Система должна обеспечить индикацию собственного состояния и уведомления в интерфейсе пользователя о сбоях в работе, критичных для штатного функционирования сервисов.

Система должна обеспечивать возможность формирования и отправки уведомлений в веб-интерфейсе Системы о превышении заданных лимитов свободного пространства на жестком диске.

8.14.5. Функции визуализации и построения отчетов.

Система должна предоставлять оперативные данные о событиях, инцидентах и мониторинге функционирования Системы в виде графиков, диаграмм и таблиц на виджетах и дашбордах.

Для настройки таблиц в Системе должны быть доступны ручное обновление и настройка периодичности автоматического обновления, добавление и удаление колонок таблицы, а также изменение их размера.

Система должна обеспечивать возможность создания и конфигурирования пользовательских дашбордов, с возможностью гибкой настройки виджетов и их распространения между пользователями Системы.

Система должна обеспечивать возможность настройки периодичности обновления как виджетов по отдельности, так и всего дашборда в целом.

Виджеты должны обладать следующими свойствами:

кликабельность – переход на страницу с соответствующим фильтром при нажатии на часть диаграммы;

респонсивность – возможность изменения размера виджета на пользовательском дашборде;

возможность сокрытия некоторых параметров на виджете с его последующей перестройкой.

Система должна позволять генерировать и выгружать по заданному шаблону в формате XLSX отчеты по инцидентам за определенный период времени.

Система должна позволять автоматически обновлять список событий и инцидентов в выводе на экран через определенные промежутки времени.

Графический интерфейс пользователя должен быть реализован по технологии Web.

Возможность разработки дополнительных виджетов по договоренности с разработчиком Системы.

8.14.6. Функции обновления.

Обновление системы должно обеспечиваться автоматически при наличии доступа к репозиториям, либо в полуавтоматическом режиме путем загрузки пакетов обновлений из локального каталога/носителя без необходимости прямого доступа в Интернет.

Система должна обеспечивать возможность обновления как с использованием сети интернет, так и без.

Система должна обеспечивать возможность обновления и расширения встроенных баз знаний вендора, в том числе формул нормализации и правил корреляции, в рамках действующей лицензии.

Система должна обеспечивать возможность обновления компонентов системы без потери накопленных данных.

Функции разграничения доступа пользователей системы.

В системе должна быть реализована модель ролевого доступа, обеспечивающая возможность разграничения доступа пользователей к объектам системы, а также разрешения или запрета определенных действий путем установления ролей.

Система должна обеспечивать идентификацию и аутентификацию пользователей по уникальному идентификатору и паролю.

Система должна обеспечивать генерацию и валидацию паролей по критерию: длина не менее 10 символов, включая латинские заглавные и строчные буквы, цифры и специальные символы (!@#$%^&* и т. д.).

Система должна обеспечивать регистрацию действий пользователей при работе с компонентами Системы.

9. Требования к структуре, функционированию системы и вводу в эксплуатацию:

Поставщик должен:

- Смонтировать поставленное оборудование ПАК в монтажные шкафы, предоставленные Заказчиком.
- Провести тестирование работоспособности аппаратной платформы.
- Провести тестирование работоспособности программного обеспечения.
- После успешного завершения тестирования совместно со специалистами Заказчика принять участие в приемо-сдаточных испытаниях ПАК.

10. Требования к гарантийным обязательствам.

Срок гарантийного обслуживания оборудования ПАК - не менее 36 месяцев в режиме 8 часов х 5 рабочих дней в неделю с даты подписания акта приемо-сдаточных испытаний. Предоставление технической поддержки должно включать в себя в том числе предоставление обновленных пакетов программного обеспечения для оборудования, а также предоставление консультаций в течение всего срока гарантийного обслуживания оборудования.

В период гарантийного срока комплектующие узлы для замены вышедших из строя, при соблюдении требований, изложенных в технической документации, должны предоставляться за счет Поставщика ПАК.

Гарантийный ремонт и техническое обслуживание оборудования должно производится на площадях Заказчика. В случае невозможности ремонта оборудования на площадях Заказчика транспортировка неисправного оборудования в сервисный центр и обратно Заказчику осуществляется транспортом и силами Поставщика. Время восстановления в полном объёме функциональности оборудования должно составлять не более 14 (четырнадцати) календарных дней.

Претендент на поставку оборудования должен предоставить письмо от дистрибьютора на территории Республики Беларусь (статус подтверждается письмом от производителя оборудования) или производителя оборудования, в котором должно быть подтверждено наличие сервисного центра, осуществляющего техническую поддержку и гарантийное обслуживания на территории Республики Беларусь: наименование сервисного центра, юридический и фактический адрес сервисного центра, контактные данные сервисного центра.

11. Требования к документации.

Комплект технической и эксплуатационной документации на ПАК должен включать:

руководство по эксплуатации;

паспорт (формуляр);
гарантийный талон;
ведомость эксплуатационной документации;

Вся документация должна быть поставлена на русском языке в виде твердой копии и/или в электронном виде (документ Word, PDF) на компакт-дисках или электронных носителях. Допустимо предоставление производителем оборудования и программного обеспечения, входящего в состав ПАК, документации на английском языке, при отсутствии у него документации на русском языке.

12. Требования к состоянию товара:

Товары должны быть новыми (товарами, которые не были в употреблении, ремонте, в том числе которые не были восстановлены, у которых не была осуществлена замена составных частей, не были восстановлены потребительские свойства).

РАЗРАБОТАНО:

Начальник отдела АСУ
учреждения здравоохранения
«4-я городская клиническая
больница им. Н.Е. Савченко» К.А. Коптяков

СОГЛАСОВАНО:

Главный внештатный специалист
по информационным технологиям
комитета по здравоохранению МГИК А.Г. Смирный