Техническое задание по закупке аппаратно-программного комплекса системы SIEM для собственных нужд АКБ “Микрокредитбанк”.

СОДЕРЖАНИЕ:

Раздел/подраздел	Наименование	Стр.
РАЗДЕЛ 1.	НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ	1
Подраздел 1.1	Назначение Системы	1
Подраздел 1.2	Цели создания системы	1
РАЗДЕЛ 2.	ХАРАКТЕРИСТИКИ ОБЪЕКТА АВТОМАТИЗАЦИИ	2
Подраздел 2.1	Дополнительные характеристики объекта автоматизации	2
РАЗДЕЛ 3.	ТРЕБОВАНИЯ К СИСТЕМЕ	3
Подраздел 3.1	Требования к Системе	3
Подраздел 3.2	Требования к функциям Системы	7
Подраздел 3.3	Требования к видам обеспечения	17
ПРИЛОЖЕНИЕ А.	ПЕРЕЧЕНЬ ПОДДЕРЖИВАЕМЫХ ИСТОЧНИКОВ	19

РАЗДЕЛ 1. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

Подраздел 1.1 Назначение Системы

Система предназначена для осуществления комплексного мониторинга информационной безопасности информационных систем (далее — ИС) Заказчика путем сбора, хранения, преобразования и выдачи пользователям информации об объектах информационной инфраструктуры и событиях информационной безопасности (далее — ИБ) в рамках этой инфраструктуры, а также для автоматизации процесса выявления инцидентов информационной безопасности и управления ими.

Подраздел 1.2 Цели создания системы

Целью создания Системы является повышение уровня защищенности ИС Заказчика путем проведения комплексного мониторинга ИБ в рамках инфраструктуры Заказчика и оперативного выявления инцидентов ИБ.

РАЗДЕЛ 2. ХАРАКТЕРИСТИКИ ОБЪЕКТА АВТОМАТИЗАЦИИ

Состав и максимальное количество узлов ИС (под узлом понимается рабочая станция, сервер или сетевое оборудование) на объектах автоматизации, для которых обеспечивается контроль защищенности, приведены в таблице ниже

(Таблица 1).

Таблица 1 — Границы проведения работ

Типовой узел	**Количество узлов**
Рабочие станции	363
Серверы Windows (в т.ч. VM)	35
Серверы Unix-like (в т.ч. VM)	38
Коммутаторы	102
Маршрутизаторы	99
Межсетевые экраны	21
Proxy IPS/IDS	10

Подраздел 2.1 Дополнительные характеристики объекта автоматизации

Требуется интеграция с центром сертификации банка на уровне API

Интерфейс системы должен поддержать русский язык

Требуется сервер со следующими характеристиками

Процессор	Intel Xeon 3rd поколение	Не менее 64 ядер
Память	DDR4	Не менее 192 ГБ
Винчестер	HDD 10K	Не менее 1600 ГБ
СХД	HDD 10K	Не менее 16 ТБ
San switch	Fiber Channel	Не менее 24 портов

Установка, настройка и интеграция системы SIEM в системы банка: под ключ

РАЗДЕЛ 3. ТРЕБОВАНИЯ К СИСТЕМЕ

Подраздел 3.1 Требования к Системе

3.1.1 Требования к структуре и функционированию Системы

Система должна представлять собой программное решение, поддерживающее развертывание как на физическом, так и на виртуальном оборудовании.

Система должна быть построена по модульному принципу и позволять ее использование и установку на единую серверную платформу (виртуальную или аппаратную).

В состав Системы должны входить следующие функциональные компоненты:

- компонент управления;
- компонент обработки;
- компонент хранения событий;
- компонент сбора событий;
- компонент управления доступом;
- база знаний с экспертизой вендора;
- компонент обновления и конфигурирования;
- компонент хранения индикаторов компрометации.

Доступ к веб-интерфейсу, к данным и функциям Системы должен осуществляться с АРМ пользователя Системы.

Таблица 2 — Требования к функциям компонентов Системы

№ п/п	Наименование компонента	Назначение компонента
1.	Компонент управления	Компонент управления должен выполнять следующие функции: – централизованное хранения конфигурации активов; – централизованное управление компонентами системы; – оперативное реагирование на инциденты ИБ и обеспечение взаимодействия подразделений организации при расследовании этих инцидентов; – предоставление графического интерфейса пользователя
2.	Компонент обработки	Компонент обработки должен осуществлять функции по обработке и хранению событий: – агрегацию, нормализацию и корреляцию событий; – автоматическое создание инцидентов; – привязку событий к активам
3.	Компонент	Компонент хранения событий должен осуществлять

№ п/п	Наименование компонента	Назначение компонента
	хранения событий	централизованное хранение информации о событиях — как исходных («сырых»), так и нормализованных
4.	Компонент сбора событий	Компонент сбора событий должен обеспечивать сбор событий от различных источников и позволять осуществлять сканирование узлов ИС в режимах черного и белого ящика
5.	Компонент управления доступом	Компонент управления доступом должен обеспечивать доступ к системе через сервис единого входа, управление пользователями системы и журналирование действий пользователей
6.	База знаний с экспертизой вендора	База знаний с экспертизой вендора должна обеспечивать получение данных, необходимых для структурирования сведений, собранных от объектов инфраструктуры, правил обработки событий
7.	Компонент обновления и конфигурирования	Компонент обновления и конфигурирования должен обеспечивать проверку наличия, загрузку и установку новых версий отдельных компонентов Системы, а также обновление базы знаний
8.	Компонент хранения индикаторов компрометации	Компонент хранения индикаторов компрометации должен обеспечивать доставку данных об угрозах информационной безопасности и индикаторах компрометации, характерных для отдельной организации в данный момент времени

Система с помощью функциональных компонентов должна обеспечивать реализацию следующих функциональных возможностей:

- сбор событий;
- управление активами;
- обработку событий;
- управление событиями;
- управление инцидентами;

- отправку уведомлений;
- визуализацию и построение отчетов;
- обновление;
- разграничение доступа пользователей Системы.

3.1.1.1 Требования к способам и средствам связи для информационного обмена между компонентами Системы

Унифицированное информационное взаимодействие между компонентами Системы должно обеспечиваться с использованием шины передачи данных и веб-служб, работающих на стеке протоколов TCP/IP.

3.1.1.2 Требования к характеристикам взаимосвязей со смежными системами

Система должна предоставлять программный интерфейс (API) для взаимодействия с решениями других производителей.

Система должна обеспечивать возможность подключения внешних систем хранения данных.

3.1.1.3 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, при котором поддерживается выполнение всех заявленных функций.

Сервисный режим является вспомогательным режимом функционирования для проведения регламентных работ по обслуживанию, реконфигурации и модернизации. При успешном окончании работы в сервисном режиме Система должна переводиться в штатный режим функционирования.

Аварийный режим функционирования применяется при обнаружении сбоев и отказов в работе Системы, нарушении функционирования поддерживающей инфраструктуры — сетей электропитания, каналов связи и т. п. Аварийный режим характеризуется полной или частичной потерей работоспособности Системы.

3.1.1.4 Требования к диагностированию Системы

Должны быть предусмотрены механизмы диагностирования неисправностей в процессе установки ПО Системы.

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

Система должна обеспечивать мониторинг доступности источника событий и характеристик потока событий.

3.1.1.5 Перспективы развития, модернизации Системы

Система должна обеспечивать возможность развития и модернизации в следующих направлениях в рамках технической поддержки вендора:

- увеличение количества систем и источников для сбора событий ИБ, в том числе новых, ранее не поддерживаемых;
- модернизация и оптимизация логики обработки собираемых событий ИБ.

Программные средства Системы должны поддерживать возможность обновления аппаратных средств при условии сохранения неизменной системы команд и исключения возможности ухудшения количественных показателей работы Системы (скорость выполнения операций, объемы памяти и пр.).

3.1.2 Требования к показателям назначения

Система должна обеспечивать следующие показатели назначения:

- количество источников событий — до 700 узлов;
- срок хранения событий — 36 дней.

3.1.3 Требования к надежности

Для обеспечения надежности доставки событий должны применяться алгоритмы и протоколы, гарантирующие доставку сообщений при образовании устранимых нештатных и аварийных ситуаций на каналах связи.

Для обеспечения надежной работы модулей обработки сообщений и исключения информационной перегрузки должны применяться алгоритмы регулирования потоков данных и буферизации событий в точках их сбора.

3.1.4 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.

3.1.5 Требования по стандартизации и унификации

Компоненты Системы при взаимодействии со смежными системами должны использовать стандартные процедуры и протоколы.

3.2 Требования к функциям Системы

3.2.1 Функции сбора событий

3.2.1.1 Компоненты Системы должны обеспечивать удаленный (сетевой) и локальный сбор событий.

3.2.1.2 Компоненты Системы должны обеспечивать как пассивный (без подключения к источнику), так и активный (с подключением к источнику) сбор событий.

3.2.1.3 Компоненты Системы должны обеспечивать возможность сбора событий в режиме, близком к режиму реального времени.

3.2.1.4 Управление сбором событий из различных типов источников должно осуществляться из единой консоли.

3.2.1.5 Система должна обеспечивать возможность фильтрации и поиска задач сбора данных по их атрибутам.

3.2.1.6 Учетные данные, необходимые для активного подключения к источникам, должны храниться в единой базе.

3.2.1.7 Должна быть обеспечена возможность использования одной записи с учетными данными для подключения к различным источникам с целью минимизации трудозатрат на корректировку учетных данных.

3.2.1.8 Система должна обеспечивать коррекцию времени в событиях от источника без дополнительной настройки источника.

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

3.2.1.10 Сбор событий должен быть реализован посредством модулей сбора данных на основе сохраняемых профилей.

3.2.1.11 В Системе должны быть предусмотрены предустановленные профили для сбора данных.

3.2.1.12 Пользователи Системы должны иметь возможность создавать собственные профили для сбора данных на базе системных (с возможностью редактирования различных параметров профиля, например портов подключения, названий и полей таблиц, из которых производится сбор, частоты забора данных, количества передаваемых сообщений).

3.2.1.13 Система должна позволять подключать источники событий новых типов посредством дополнения множества правил преобразования событий (нормализации, агрегации).

3.2.1.14 Система должна позволять разрабатывать пользовательские модули сбора для работы с неподдерживаемыми поставщиками программных средств Системы протоколами передачи событий на скриптовом языке Python. Разработка и работа с такими модулями должна осуществляться через интерфейс Системы.

3.2.1.15 Запуск пользовательских модулей сбора должен осуществляться средствами агента Системы. Запуск модулей сторонними планировщиками не допускается в целях обеспечения информационной безопасности.

3.2.1.16 Система должна обеспечивать централизованную настройку и мониторинг работы модулей сбора событий из единой консоли управления.

3.2.1.17 При выполнении иерархической инсталляции Система должна обеспечивать отображение связей между площадками и возможность настройки правил репликации событий в цепочке иерархии.

3.2.1.18 Система должна обеспечивать возможность мониторинга источников, позволяя отслеживать:

- задержку между временем возникновения событий и временем их получения Системой;
- количество событий, получаемых в единицу времени.

3.2.2 Функции управления активами

3.2.2.1 Система должна обеспечивать идентификацию и добавление активов путем:

- сбора и анализа событий;
- сетевого сканирования для обнаружения узлов сети;
- анализа защищенности по методам черного и белого ящика;
- добавления актива пользователями (вручную).

3.2.2.2 Система должна обеспечивать идентификацию сетевых служб, использующих протоколы TCP и UDP в качестве протоколов транспортного уровня.

3.2.2.3 Система должна обеспечивать выявление и идентификацию активов, функционирующих в момент сканирования.

3.2.2.4 Система должна обеспечивать сбор идентификационных данных об активах (IP-адреса, имени узла, FQDN). Механизм идентификации должен обеспечивать выявление и корректную работу с кластерными конфигурациями активов.

3.2.2.5 Система должна обеспечивать выявление и идентификацию доступных в момент сканирования портов, использующих сетевые протоколы транспортного уровня.

3.2.2.6 Система должна обеспечивать сбор сведений о составе программного и аппаратного обеспечения сканируемого актива.

3.2.2.7 Система должна обеспечивать сбор параметров конфигурации актива по следующим протоколам удаленного управления: WMI, SAP RPC, SSH, Telnet, ODBC, SNMP, Checkpoint OPSEC.

3.2.2.8 Система должна обеспечивать автоматическую привязку событий к активам при условии, что в событии содержится идентификационная информация.

3.2.2.9 Система должна обеспечивать построение иерархии групп активов и управление ею.

3.2.2.10 Система должна обеспечивать автоматическое определение типа и роли узла по результатам сканирования в режимах черного или белого ящика.

3.2.2.11 Система должна обеспечивать построение и визуализацию топологии сети на актуальный момент времени на уровне L3 модели OSI.

3.2.2.12 Система должна иметь следующие механизмы для управления списком активов:

- фильтрацию активов по заданному набору атрибутов и их значений с использованием специализированного языка запросов (в том числе с возможностью объединения запросов);
- отображение активов, удовлетворяющих условиям запроса, в таблице активов и на топологии;

– возможность сохранения пользовательских запросов для последующего быстрого доступа к ним;

– функции группировки и сортировки активов, анализа данных об активах.

3.2.2.13 Система должна обеспечивать отображение активов, участвовавших в событии или инциденте, на топологии сети.

3.2.2.14 Система должна обеспечивать расчет сетевой достижимости между выбранными активами на топологии с учетом протоколов и портов.

3.2.2.15 Система должна обеспечивать возможность задания активам уровня значимости и использование этой величины при количественной оценке опасности событий ИБ и инцидентов.

3.2.2.16 Система должна обеспечивать возможность мониторинга доступности активов (узлов, сетевых сервисов и устройств).

3.2.2.17 Система должна обеспечивать отслеживание изменений конфигурации активов, включая:

– просмотр состояния актива на заданный момент времени в прошлом;

– сравнение конфигураций актива в разные моменты времени;

– экспорт истории конфигурации актива.

3.2.2.18 Система должна позволять объединять активы в динамические группы исходя из собранных данных об их конфигурации. Формирование динамических групп должно осуществляться как на основе пользовательских запросов, так и при помощи интерактивного конструктора запросов.

3.2.2.19 Система должна позволять добавлять в модель актива пользовательские поля и их описание.

3.2.2.20 Система должна позволять выполнять экспорт данных об активах в табличный список.

3.2.3 Функции обработки событий

3.2.3.1 Система должна обеспечивать нормализацию событий с использованием встроенных формул.

3.2.3.2 Система должна поддерживать возможность создания пользователями собственных формул нормализации.

3.2.3.3 Система должна обеспечивать агрегацию событий с использованием встроенных правил.

3.2.3.4 Система должна обеспечивать поддержку мультиязычных событий.

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

3.2.3.6 Система должна обеспечивать возможность проверки ранее полученных событий на наличие в них актуальных индикаторов компрометации.

3.2.3.7 В состав Системы должны входить встроенные правила корреляции, обеспечивающие выявление целенаправленных атак в автоматическом режиме.

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

- выявление активности на рабочих станциях в ночное время и выходные (праздничные) дни;
- контроль VPN-соединений;
- контроль выполнения команд, которые могут угрожать информационной безопасности ИС, на серверах и сетевом оборудовании;
- контроль учетных записей;
- контроль изменения конфигурации на сетевом оборудовании и серверах;
- контроль установки и запуска новых сервисов ОС и сетевых служб.

3.2.3.9 Система должна предоставлять пользователю интерфейс создания пользовательских правил корреляции (визуальный конструктор привил корреляции) и возможность создания пользовательских правил корреляции на основе встроенных системных правил.

3.2.3.10 Система должна обеспечивать возможность управления списком активных правил корреляции с отображением статистики их срабатывания.

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

3.2.3.12 Система должна обеспечивать контроль потребляемой коррелятором памяти и при достижении порогового значения отключать нагружающие ее правила корреляции.

3.2.3.13 Система должна обеспечивать использование табличных списков при формировании правил корреляции. Пользователю должна быть доступна возможность их создания, удаления и редактирования через графический интерфейс.

3.2.3.14 Функциональность табличных списков должна позволять выполнять:

- контроль времени жизни записей в таблице (TTL);
- индексацию выделенных колонок в целях ускорения доступа к записям;
- определение первичного ключа таблицы;
- импорт и экспорт всего содержимого табличного списка.

3.2.3.15 При обращении к табличным спискам из правил корреляции должны быть доступны функции:

- создания, обновления, удаления строк, а также очистки всей таблицы;
- обогащения корреляционного события найденными данными из табличного списка;
- выполнения математических функций инкремента, декремента, вычисления максимального, минимального и среднего при вставке данных в табличный список;
- выполнения математических функций вычисления максимального, минимального, среднего и подсчета общего числа строк при выборке данных из табличного списка.

3.2.3.16 Система должна обеспечивать возможность задания правил обогащения событий, поступающих в систему, данными из табличных списков (в том числе данными из репутационных списков).

3.2.3.17 Система должна обеспечивать хранение исходных и нормализованных событий.

3.2.4 Функции управления событиями

3.2.4.1 Система должна содержать текстовое описание каждого события, предоставленное экспертами вендора.

3.2.4.2 Система должна обеспечивать категоризацию событий.

3.2.4.3 Система должна иметь следующие механизмы для управления списком событий:

- фильтрацию событий по группе активов и периоду;

– фильтрацию событий по заданному набору атрибутов и их значений с использованием специализированного языка запросов;

– сохранение пользовательских фильтров для последующего быстрого доступа к интересующим событиям (с возможностью создания иерархического списка фильтров);

– функции группировки и сортировки событий в выводе на экран по всем доступным полям;

– анализ данных о событиях с помощью математических операций.

3.2.5 Функции управления инцидентами

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

3.2.5.2 Система должна обеспечивать импорт инцидентов из специально подготовленных файлов.

3.2.5.3 Система должна обеспечивать категорирование инцидентов.

3.2.5.4 Система должна обеспечивать управление автоматической генерацией инцидентов.

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

3.2.5.6 Система должна обеспечивать просмотр и редактирование карточки инцидента.

3.2.5.7 Для управления списком инцидентов Система должна иметь следующие механизмы:

– фильтрации инцидентов по группе активов и периоду;

– фильтрации инцидентов по заданному набору атрибутов и их значений с использованием специализированного языка запросов;

– фильтрации инцидентов с использованием системных и пользовательских фильтров;

– сохранения пользовательских фильтров для последующего быстрого доступа (с возможность создания иерархического списка фильтров);

– сортировки инцидентов по времени создания, статусу, критичности, категории, названию.

3.2.5.8 Система должна обеспечивать возможность построения процесса расследования инцидента: формирования поручений для расследования, определения порядка реагирования и устранения последствий инцидентов, назначения ответственных лиц.

3.2.5.9 Система должна обеспечивать хранение истории расследования инцидента.

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

3.2.6 Функции отправки уведомлений

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

- об изменении списка активов в Системе;
- изменении состава выбранных динамических групп активов (включении, исключении активов);
- событиях и инцидентах — при их попадании под системный или пользовательский фильтр;
- выходе параметров потока событий за пределы допустимых значений;
- выполнении задач сбора данных;
- состоянии Системы.

3.2.6.2 Система должна обеспечивать возможность отправки уведомления об изменении числа активов и изменениях в группах активов.

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

3.2.7 Функции визуализации и построения отчетов

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

3.2.7.2 Система должна обеспечивать возможность создания и конфигурирования пользовательских дашбордов.

3.2.7.3 Система должна предоставлять возможность экспорта отчетов как минимум в одном из следующих форматов: PDF, XLSX, CSV.

3.2.7.4 Система должна обеспечивать отображение следующих статистических данных по инцидентам в графическом формате (на виджетах):

- созданные инциденты,
- закрытые инциденты за период,
- незакрытые инциденты по уровню опасности,
- среднее время устранения инцидента.

3.2.7.5 Система должна обеспечивать выпуск отчетов (стандартных и пользовательских) вручную или по расписанию.

3.2.7.6 Система должна предоставлять пользователю интерфейс создания пользовательских отчетов с данными об активах, событиях и инцидентах (конструктор отчетов).

3.2.7.7 Система должна обеспечивать возможность формирования отчетов из состава имеющихся шаблонов:

- по активам,
- событиям,
- инцидентам,
- мониторингу.

3.2.7.8 Система должна обеспечивать построение следующих отчетов по активам:

- инвентаризация групп пользователей Windows,
- инвентаризация аппаратного обеспечения,
- инвентаризация операционных систем,
- инвентаризация узлов с открытыми портами,
- инвентаризация сетевых сервисов,
- инвентаризация ресурсов общего доступа,
- инвентаризация ресурсов общего доступа по узлам,
- инвентаризация программного обеспечения,
- инвентаризация пользователей Windows,
- инвентаризация служб Windows.

3.2.7.9 Система должна обеспечивать построение следующих отчетов по инцидентам:

- распределение новых инцидентов по времени,
- распределение утвержденных инцидентов по времени,

- распределение инцидентов в работе по времени,
- все открытые инциденты по времени,
- распределение разрешенных инцидентов по времени,
- распределение закрытых инцидентов по времени,
- все завершенные инциденты по времени.

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

3.2.7.11 Графический интерфейс пользователя должен быть реализован по технологии Web.

3.2.8 Функции обновления

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

3.2.8.2 Система должна обеспечивать возможность обновления компонентов Системы без потери накопленных данных.

3.2.9 Функции разграничения доступа пользователей Системы

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

3.2.9.2 Система должна обеспечивать идентификацию и аутентификацию пользователей через сторонний LDAP-сервер.

3.2.9.3 В Системе должна быть реализована модель ролевого доступа, обеспечивающая возможность разрешения или запрета доступа пользователей к информации об определенных узлах (активах).

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

3.3 Требования к видам обеспечения

3.3.1 Требования к лингвистическому обеспечению

Эксплуатационная документация, графический интерфейс пользователя Системы и формируемые Системой отчеты должны быть выполнены на русском языке.

3.3.2 Требования к программному обеспечению

Компоненты Системы должны разворачиваться на одной из следующих программных платформ:

- Microsoft Windows Server 2019;
- Microsoft Windows Server 2016;
- Debian 10.

Доступ к пользовательскому интерфейсу Системы должен осуществляться с использованием одного из следующих браузеров:

- Google Chrome 49 (и выше);
- Mozilla Firefox 45 (и выше);
- Microsoft Internet Explorer 11 (и выше).

Компоненты Системы должны быть развернуты с учетом карты поддерживаемых операционных систем (далее – ОС) (Таблица 3).

Таблица 3 — Карта поддерживаемых ОС

Компонент	**Windows Server 2019**	**Windows Server 2016**	**Debian 10**
Компонент управления	+	+	+
Компонент обработки	+	+	+
Компонент хранения	+	+	+
Компонент сбора событий	+	+	+
Компонент управления доступом	+	+	+
База знаний с экспертизой вендора	+	+	+
Компонент обновления и конфигурирования	–	–	+
Компонент хранения индикаторов компрометации	–	–	+

ПРИЛОЖЕНИЕ А. ПЕРЕЧЕНЬ ПОДДЕРЖИВАЕМЫХ ИСТОЧНИКОВ

№ п/п	Наименование источника	Версия
Системы AAA		
1.	Open Source freeRADIUS	2.2.0
2.	Аванпост Avanpost IDM	5.0, 5.1.1
3.	Swivel Secure PINsafe	3.9.5
4.	RSA Authentication Manager	8.2
5.	Microsoft Network Policy Server	2012 R2
6.	Xceedium Xsuite	2.4
7.	Cisco Identity Services Engine	2.3
8.	Cisco ACS	5.4.x, 5.6.x
9.	Open Source tac_plus	4.0.4.19
Антивирусное ПО		
10.	Kaspersky Anti Targeted Attack Platform	1.0.2, 2.0.0, 3.0.0
11.	Kaspersky Security for SharePoint Server	9.3.58811
12.	Kaspersky Security for Microsoft Exchange Servers	9.4.189
13.	Kaspersky Secure Mail Gateway	1.1.0
14.	Kaspersky Linux Mail Server	8.0
15.	Positive Technologies MultiScanner	0.5.9, 1.0
16.	McAfee ePolicy Orchestrator VirusScan Enterprise	5.1
17.	Dr.Web Enterprise Security Suite	6, 10
18.	Microsoft Windows Defender	4
Системы обеспечения безопасности приложений		
19.	Imperva SecureSphere Management Server	11.0, 12.0, 13.0

№ п/п	Наименование источника	Версия
20.	Cisco Email Security Appliance	7, 9.7.0, 10.0.2, 11.0.0
21.	FortiNet FortiMail	5.4, 6.2.0
22.	Positive Technologies Application Firewall	3.7.1
23.	IBM InfoSphere Guardium	9.1
Бизнес-приложения		
24.	СЭДО	1, 2
25.	New Security Technologies SafeInspect	2.1
26.	Wallix AdminBastion	4.2, 5.0
27.	АИС «Налог-3»	–
28.	Vaultize Technologies VDR	18.07.09
29.	SAP Mobile Platform	2.0
30.	Microsoft SharePoint	2013
31.	1С: Предприятие	8.2, 8.3
32.	SAP AS JAVA	7.x
33.	SAP NetWeaver AS ABAP	6.4, 7.0, 7.02, 7.10, 7.20, 7.30, 7.40, 7.42
Системы резервного копирования		
34.	Veeam Backup & Replication	7, 8
35.	Acronis Backup	12.5
36.	Veritas NetBackup	8.1.1
37.	RSA Certificate Manager	6.9
38.	Microsoft Certification Authority	2008, 2008R2, 2012, 2012R2
39.	Commvault Backup & Recovery	11 SP 17
40.	NetApp SnapCenter	4.2

№ п/п	Наименование источника	Версия
СУБД		
41.	Microsoft SQL Server	2005, 2008, 2012, 2014
42.	Open Source PostgreSQL	9.6
43.	SAP HANA	1.x
44.	Oracle MySQL	5.7.10
45.	Oracle Database Net Listener	11, 12, 18
46.	Oracle Database Audit Trail	10g, 11g, 12c
DHCP серверы		
47.	Microsoft DHCP Server	2003, 2003R2, 2008, 2008R2, 2012, 2012R2, 2016
Active Directory		
48.	Open Source OpenLDAP	–
49.	Microsoft Active Directory	2008, 2008R2, 2012, 2012R2
50.	Microsoft ADFS	2.0, 3.0
DLP-системы		
51.	Websense Data Security	7.7
52.	Varonis DatAdvantage	6.2.80.74
53.	Серчинформ КИБ Серчинформ	5.0
54.	Zecurion zGate	7.0
55.	InfoWatch Traffic Monitor	4.1, 6.1, 6.5, 6.7, 6.10, 6.11
56.	Конфидент Dallas Lock	8.0.347.20
57.	Ростелеком-Солар Solar Dozor	6.7.2
DNS-серверы		
58.	Open Source BIND	9.9.4, 9.11.6
59.	Open Source NSD	4.x

№ п/п	Наименование источника	Версия
60.	Open Source PowerDNS	3.x, 4.x
61.	Open Source Unbound	1.4.x
62.	Microsoft Windows DNS server	2008, 2008R2, 2012, 2012R2
DPI		
63.	TRITON AP-WEB	8.2
64.	Positive Technologies NAD	7.0
Файловые серверы		
65.	Open Source Nextcloud	13
66.	Open Source NFS	1.2.8
Honeypot		
67.	Lastline Enterprise	6.5
68.	Positive Technologies HoneyPot	2.1
Системы обеспечения безопасности оконечного оборудования		
69.	Kaspersky Endpoint Security	8, 10, 11
70.	Kaspersky Security Center	8, 9, 10, 11
71.	Security Code Secret Net Studio	8.2, 8.3, 8.4, 8.5, 8.6
72.	Security Code Secret Net	6.5, 7.3, 7.6, 7.7
73.	Security Code TrustAccess	1.3
74.	Security Code vGate	2.7, 2.8, 3.0, 4.1
75.	ESET Security Management Center	7.0
76.	ESET Remote Administrator	5.3.3
77.	Symantec Endpoint Protection	12.1, 14
78.	SmartLine DeviceLock DLP	7.3, 8.1, 8.2, 8.3
79.	ОКБ САПР Аккорд СУЦУ	1.0, 1.0.8
80.	McAfee SolidCore	2.7.0.5

№ п/п	Наименование источника	Версия
81.	Воентелеком СОА, СЗИ НСД, САВЗ	–
82.	Trend Micro Deep Security	9.5.5623
83.	Positive Technologies Endpoint Monitor	15
84.	Lumension Endpoint Security	4.4
Серверы электронной почты и обеспечения безопасности электронной почты		
85.	CommuniGate Systems CommuniGate Pro	6.1.9, 6.2.8
86.	Microsoft Exchange	2003, 2007, 2010, 2013, 2016
87.	Open Source Sendmail	8.x
88.	Open Source Postfix	2, 3
89.	McAfee Mail Gateway	7.5, 7.6
Сетевое оборудование		
90.	Cisco UCS Manager	3.1
91.	Cisco NX-OS	4.*,5.*,6.*,7.*
92.	Cisco IOS XR	4, 5, 6
93.	Cisco IOS XE	2.*, 3.*
94.	Cisco IOS	12.x, 15.x
95.	Juniper JunOS	11, 12, 13, 14, 14.1
96.	Huawei VRP	5.70, 5.110, 5.170, 8.150
97.	Huawei-3Com	3, 5
98.	Элтекс Service gateway	–
99.	Элтекс Ethernet Access Switch	–
100.	Булат BS-5100	–
101.	Булат BK-A908	–

№ п/п	Наименование источника	Версия
102.	Avaya ERS 8600	–
103.	Avaya ERS 5500	5.0.0.4, 6.0.0.18
104.	Mikrotik RouterOS	6.30, 6.37.2
105.	HPE Comware Software	5.20
106.	Alcatel AOS	6.x
107.	Allied Telesis	8516F
108.	Qtech QSW	7.0.3.5
109.	HPE VSR	7.1
110.	Протокол NetFlow	5, 9
111.	Микролинк-связь	5.70
Системы мониторинга сети		
112.	Zabbix	4.0
113.	Infotecs ViPNet StateWatcher	3.2, 3.2.5, 4.3.0
114.	Infoblox DDI	8.2.1
115.	Bot-Trek TDS Group-IB	1.2
116.	Microsoft SCCM	4.00
117.	Microsoft SCOM	2012 R2
Системы обеспечения сетевой безопасности		
118.	Entensys UserGate UTM	5.0
119.	McAfee Advanced Threat Defense	3.6
120.	МФИ Софт АПК "Периметр"	3.x, 4.x
121.	МФИ Софт Garda Monitor	1.0, 1.2, 2.1
122.	Arbor Peakflow SP	5.8, 5.11, 7.6, 8.x
123.	Palo Alto Networks PAN-OS	4.1, 6, 8.0
124.	RSA ESA	10.4

№ п/п	Наименование источника	Версия
125.	FireEye EX	7.9.0, 7.9.1, 7.9.2, 7.9.3
126.	Watchguard Fireware XTMv	11.12.2
127.	Kerio Control Technologies	9.0, 9.2.4
128.	Check Point GAiA OS	76, 77.10, 77.20, 77.30, 80, 80.20
129.	TCC Diamond VPN/FW	3.18.1.4
130.	Cisco ASA FirePOWER	6.2.0, 6.3.0
131.	Cisco NGIPS	6.2
132.	Кодмастер Mirada	1.0
133.	Инфосистемы Джет СОВ ПАК Плутон	2.2.26
134.	Arbor Pravail NSI	5.5.1
135.	Центр Специальной Схемотехники Аргус	1.5
136.	РНТ Форпост	2.0, 2.1
137.	Radware DefencePro	12412, 4412, версия ОС - 6.12.00
138.	Snort	2.9, 3
139.	Suricata	2, 3.1
140.	Infotecs ViPNet IDS	2.2, 2.4, 3.4, 3.5
141.	Infotecs ViPNet TIAS	3.4
142.	Cisco ASA	8, 9
143.	Cisco FWSM	3.2
144.	НПО Фрактел ССПТ-2	1.3
145.	Stonesoft StoneGate Management Center	5.3
146.	SAP SAProuter	38
147.	Open Source Iptables	1.4.8

№ п/п	Наименование источника	Версия
148.	FortiNet Fortigate	4.0, 5.4.2, 5.6.4, 5.6.5
149.	McAfee Next Generation Firewall	5.3.3, 5.8.3
150.	Positive Technologies ISIM	1.6
151.	Positive Technologies NAD	8.0, 9.0
Операционные системы		
152.	FreeBSD	4.x, 5x, 6.x, 7.x, 8.x, 9.x, 10.x, 11.x
153.	SUN Solaris	9.x, 10.x, 11.x
154.	HP-UX	11.31
155.	РусБИТех Astra Linux	1.4 SE , 1.5 SE
156.	Microsoft DHCP client v.6, v.9	2008, 2012
157.	Debian	7
158.	IBM AIX	5.3, 6.1, 7.1
159.	Microsoft Windows	XP (только WMI), Vista+, 7, 8, 8.1, 10, 2003 (только WMI), 2008, 2008R2, 2012, 2012R2
160.	Red Hat Enterprise Linux	4.x, 5.x, 6.x, 7.x
161.	SUSE Linux Enterprise Server	10
162.	Ubuntu	12.04,14.10
163.	МСВС	3.0
Системы обеспечения физической безопасности		
164.	СШС групп SHS-Office	4.157.49
165.	Rusguard Rusguard Soft	1.7.0
166.	Insyres VisitorControl	4.1
167.	Parsec ParsecNET	3.7

№ п/п	Наименование источника	Версия
168.	ЕС-ПРОМ АПК "Бастион"	1.7.4.10
	Прокси серверы	
169.	Cisco Web Security Appliance	8.0, 11.5
170.	Open Source HAProxy	1.7.9
171.	Microsoft Forefront TMG	7.0
172.	Microsoft ISA	2006
173.	Entensys UserGate Proxy & Firewall	6, 6.5
174.	Squid	3.0, 3.1, 3.2, 3.3, 3.4, 3.5
	SCADA системы	
175.	НИИТеплоприбор Квинт	5.9.6
	Системы хранения	
176.	NetApp AFF	A700
	Телеком	
177.	Zoom International Call Recording	5.6.6
178.	Huawei iManager	U2000, M2000
179.	Polystar OSIX	5.1.5.25
	Терминальные серверы	
180.	Dameware Mini Remote Control	7.5.9.1
181.	Citrix NetScaler	11
182.	Microsoft Windows Terminal Services	6.3
	Системы виртуализации	
183.	VMware vSphere	6.5
184.	VMware vCenter	5.5, 6.0, 6.5
185.	VMware ESXi	5.x, 6.x
186.	ТИОНИКС VDI	1.3

№ п/п	Наименование источника	Версия
187.	Nutanix AHV	5.5.5
188.	Open Source KVM	2.5
189.	Open Source libvirt	1.3.1
190.	Open Source LXD	2.x
VoIP		
191.	Avaya Aura	8
192.	Iskratel vIMS	SI3000
193.	Microsoft Skype for Business	15.0
VPN		
194.	КриптоПРО NGate	1.0.1
195.	Infotecs ViPNet Administrator	4.6.2
196.	Infotecs VipNet Coordinator (Linux)	3.2, 2.4
197.	Security Code АПКШ «Континент»	3.7, 4.0.2
198.	Security Code Континент TLS VPN	1.x
199.	OpenVPN Inc. OpenVPN	2.4
200.	Фактор-ТС Dionis NX	1.2-1, 2.0
201.	ЭЛВИС-ПЛЮС Застава	6, 7
202.	S-Terra VPN Gate	4.1, 4.2
Web-серверы и системы обеспечения веб-безопасности		
203.	FortiNet FortiWeb	5.4, 6.3
204.	Microsoft IIS Server	6, 7.5, 8.5
205.	Apache HTTP Server	2.4
206.	Lighttpd	1.4
207.	Nginx	1.2, 1.8, 1.9
208.	Positive Technologies Application Firewall	4.0

№ п/п	Наименование источника	Версия
209.	Wallarm WAF	2.14
Системы обеспечения и контроля беспроводного доступа		
210.	Extreme Networks Summit Wireless LAN Controller	–
211.	Aruba Networks Aruba OS	6.3.1.14
212.	Cisco WLC	7
Иные системы		
213.	CyberArk Enterprise Password Vault	10.9
214.	Positive Technologies FCSP	1.12, 1.14, 1.15, 2.1.3
215.	Positive Technologies MaxPatrol 8	–
216.	ЦФТ IBSO	18.5
217.	CyberArk Enterprise Password Vault	10.3
218.	НИИ СОКБ SafePhone	4.0
219.	Open Source Ansible	2.6.2
220.	Open Source Umbraco CMS	7.7.1
221.	One Identity Safeguard for Privileged Sessions	5.0.8
222.	Microsoft Windows Sysinternals Sysmon	7.01, 8.0
223.	Windows Server Update Services	Windows Server 2008, 2008R2, 2012, 2012R2
224.	APC Smart-UPS VT	–
225.	IBM SiteProtector	2.0, 3.1
226.	АЛТЭКС-СОФТ RedCheck	2.6
227.	Netwrix Auditor for Active Directory	9.6
228.	Netwrix Auditor for Windows File Servers	9.6

№ п/п	Наименование источника	Версия
229.	HPE iLo	4