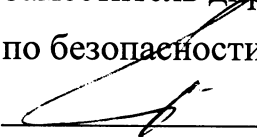




**УТВЕРЖДАЮ:**

Заместитель директора  
по безопасности

 / П.В. Горохов

**Техническое задание**

на внедрение системы мониторинга событий информационной безопасности  
MaxPatrol SIEM

Предмет закупки: Приобретение программно-аппаратного комплекса для  
мониторинга событий информационной безопасности

г. Заречный

2020

## СОДЕРЖАНИЕ

1. Назначение
2. Условия доставки
3. Условия заказа лицензий и оборудования
4. Состав выполняемых работ
  - Этап 1 Предпроектное обследование
  - Этап 2 Проектирование и создание системы
  - Этап 3 Ввод Системы в эксплуатацию
5. Система мониторинга событий информационной безопасности
  - 5.1 Требования к структуре и функционированию Системы
  - 5.2 Требования к функциям Системы
  - 5.3 Требования по совместимости

### **1. Назначение:**

Поставка:

- неисключительной лицензии на систему мониторинга событий информационной безопасности, соответствующей требованиям данного ТЗ;
- оборудования и услуг по его установке, настройке, а также обучению сотрудников.

### **2. Условия доставки:**

Доставка Оборудования и Лицензий осуществляется силами Исполнителя, до проходной административного здания АО «ИРМ».

Контактное лицо – Татаринова Марина Олеговна, телефон (34377) 3-53-54, [tatarinova\\_mo@irmatom.ru](mailto:tatarinova_mo@irmatom.ru)

### **3. Условия заказа Лицензий и Оборудования:**

Сроки поставки Лицензий: не более 14 рабочих дней с момента заключения договора.

Срок использования неисключительных прав - 1 год, с момента подписания акта приема-передачи.

Гарантийные обязательства на оборудование - в течение 5 (пяти) лет.

### **4. Состав выполняемых работ**

4.1 Место выполнения работ: Свердловская обл. г. Заречный пром. Зона Белоярской АЭС.

#### ***Этап 1. Предпроектное обследование.***

1.1. Разработка опросных листов, сбор и уточнение данных, необходимых для создания Системы:

- имеющиеся нормативно-методические и организационно-распорядительные документы по вопросам обеспечения информационной безопасности;
- актуальные сведения об архитектуре сети, составе и количестве технических и программных средств информационной системы;
- информацию о наличии требований к сбору и анализу событий информационной безопасности, расследованию инцидентов информационной безопасности, к срокам хранения данных о событиях информационной безопасности и инцидентах;
- планы по модернизации сети и информационной системы с указанием ориентировочных сроков проведения работ;
- другие особенности информационной системы, влияющие на архитектуру Системы.

Перечень исходных данных может уточняться и дополняться в ходе выполнения работ.

1.2. Разработка отчета о предпроектном обследовании:

- результаты предпроектного обследования должны оформляться, согласовываться и утверждаться в документе «Отчет о предпроектном обследовании».

#### ***Этап 2. Проектирование и создание Системы.***

2.1. Разработка и согласование Технического задания на создание Системы.

- Разработка, согласование и утверждение Технического задания на создание Системы.

2.2. Разработка и согласование Пояснительной записки к техническому проекту Системы.

- осуществляется разработка проектных решений по созданию Системы, включая общие решения по функциональной структуре и алгоритмам функционирования Системы, выявляемым типам инцидентов ИБ и источникам событий безопасности для их выявления, функциям персонала, обслуживающего Систему, параметрам настройки программных средств Системы, обеспечивающих реализацию функциональных возможностей Системы и мероприятия по подготовке объекта автоматизации для ввода Системы в действие.

#### 2.3. Разработка и согласование эксплуатационной документации Системы:

- регламент эксплуатации Системы;
- руководство администратора Системы;
- руководство пользователя Системы;
- инструкции по настройке программно-технических средств информационных систем для сбора событий безопасности из целевых журналов аудита и сведений об информационных ресурсах (активах) и уязвимостях информационных ресурсов;
- порядок взаимодействия персонала по ликвидации последствий инцидентов информационной безопасности.

#### 2.4. Комплектация Системы программными средствами.

Исполнитель при передаче программных средств предоставляет следующие документы:

- дистрибутивы программного обеспечения, техническая и эксплуатационная документация производителей программных средств Системы на бумажном или электронном носителе;

- комплекты документов, устанавливающих соответствующие формы правовых и финансово-экономических отношений (акты, товарные накладные, счета-фактуры и пр.).

#### 2.4. Пуско-наладочные работы по созданию Системы.

##### 2.4.1. Монтаж и первоначальная настройка

В ходе монтажа и первоначальной настройки Системы силами специалистов АО "Институт реакторных материалов" выполняются следующие работы:

- выделение свободного места в телекоммуникационных шкафах для установки оборудования Системы;

- выделение электроснабжения необходимой мощности, а также необходимого количества коммутационных разъемов для подключения оборудования Системы к сетям электропитания;

- установка средств виртуализации и создание виртуальных серверов с характеристиками согласно проектной документации на Систему, включение их в сетевую инфраструктуру АО "Институт реакторных материалов";

- предоставление дистрибутива и нужного количества лицензий ОС, необходимой для функционирования Системы.

В ходе монтажа и первоначальной настройки Системы силами специалистов Исполнителя выполняются следующие работы:

- установка и настройка ОС на виртуальных серверах Системы, согласно рекомендациям производителя ПО MaxPatrol SIEM или аналог;

- установка ПО MaxPatrol SIEM или аналог;

- первоначальная настройка серверов Системы.

##### 2.4.2. Подключение источников событий ИБ

В ходе подключения источников событий ИБ к Системе выполняются следующие работы:

- настройка программно-технических средств информационных систем АО "Институт реакторных материалов" для регистрации событий безопасности и сбора событий безопасности согласно разработанным на этапе технического проектирования

инструкциям (настройка осуществляется силами специалистов АО "Институт реакторных материалов" при консультационной поддержке Исполнителя);

- настройка Системы, включая:
  - создание в ПО MaxPatrol SIEM или аналог сервисных учетных записей для подключения к информационным ресурсам;
  - создание в ПО MaxPatrol SIEM или аналог профилей сбора событий безопасности (настройка портов подключения; названий и полей таблиц, из которых производится сбор; частоту сбора данных; корректировку времени события, количество передаваемых сообщений и т.п.);
  - создание в ПО MaxPatrol SIEM или аналог расписания задач по сбору событий безопасности.

Перечень подключаемых к Системе информационных систем и средств защиты информации информационно-вычислительной инфраструктуры АО "Институт реакторных материалов" приведен в Разделе 2.2 данного ТЗ. Точный состав подключаемых к Системе источников событий безопасности уточняется на этапе технического проектирования.

#### 2.4.3. Настройка сбора сведений об информационных ресурсах

В ходе настройки сбора сведений об информационных ресурсах выполняются следующие работы:

- настройка программно-технических средств информационных систем АО "Институт реакторных материалов" для сканирования и сбора сведений согласно разработанным на этапе технического проектирования инструкциям (настройка осуществляется силами специалистов АО "Институт реакторных материалов" при консультационной поддержке Исполнителя);
- настройка программных средств Системы, включая:
  - создание в ПО MaxPatrol SIEM или аналог сервисных учетных записей для подключения к информационным ресурсам;
  - создание в ПО MaxPatrol SIEM или аналог расписания задач сканирования информационных ресурсов в режиме аудита и пентеста, обнаружения сетевых узлов;
  - построение топологии сети АО "Институт реакторных материалов" на уровне L3 сетевой модели OSI (Open Systems Interconnection Basic Reference Model) для просканированных информационных ресурсов.

Перечень сканируемых узлов сети уточняется и конкретизируется на этапе технического проектирования Системы.

#### 2.4.4. Настройка правил корреляции событий безопасности для выявления инцидентов ИБ

В ходе настройки правил корреляции (анализа) событий безопасности для выявления инцидентов ИБ выполняются следующие работы:

- разработка и настройка в ПО MaxPatrol SIEM или аналог правил корреляции событий безопасности в соответствии с перечнем выявляемых типов инцидентов ИБ. Перечень выявляемых типов инцидентов ИБ и возможных сценариев их выявления представлен в таблице ниже. Перечень выявляемых типов инцидентов ИБ и источников событий безопасности для их выявления, применимых в информационно-вычислительной инфраструктуре АО "Институт реакторных материалов" уточняется на этапе технического проектирования;
- создание и наполнение вспомогательных справочников и табличных списков необходимых для функционирования соответствующих правил (например, перечень известных вредоносных ресурсов в сети Интернет, списки исключений и т.д.);

№	Тип инцидента ИБ	Возможные сценарии выявления инцидентов	Возможный источник событий информационной безопасности
1.	Вредоносное программное обеспечение (ПО) (включая АРТ и бот-агент)	Массовое заражение узлов сети одним вирусом	Журналы регистрации событий системы антивирусной защиты
2.		Несколько вирусов на одном узле сети	
3.		Ошибка удаления вируса на узле	
4.		Подключения узла к бот-нет сети	Журналы регистрации событий проху-сервера или межсетевого экрана
5.		Обнаружение сетевых червей	
6.		Обнаружение признаков вредоносного ПО (запуск ПО, процесса или последовательности процессов)	Журналы регистрации событий ОС
7.	Несанкционированный доступ	Попытка входа в ОС под технологической учетной записью	Журналы регистрации событий службы каталогов Active Directory, ОС, сетевое оборудование, серверы виртуальной инфраструктуры
8.		Изменение критичных параметров системы (остановка критичных служб и приложений, очистка системных журналов)	
9.		Повышение привилегий пользователя, Изменение ключевых групповых политик, изменение состава привилегированных групп, создание/удаление учетных записей	
10.		Работа пользователя в ночное время, выходной или праздничный день во внутренней сети компании	
11.		Большое количество блокировок пользователей в системе	
12.		Попытка несанкционированного доступа к информационным ресурсам	Журналы регистрации событий службы каталогов Active Directory, ОС, прикладного ПО, систем управления

№	Тип инцидента ИБ	Возможные сценарии выявления инцидентов	Возможный источник событий информационной безопасности
13.		Запись конфиденциальных документов на съемные носители информации	базами данных (далее – СУБД) DLP-системы, средств защиты от несанкционированного доступа и пр.
14.		Использование утилит удаленного управления <sup>97</sup> (TeamViewer и пр.)	Журналы регистрации проху-сервера, межсетевых экранов или маршрутизаторов
15.		Подключение к узлу периметра по административным портам с внешнего узла	
16.	Эксплуатация уязвимости	Обнаружение вредоносного ПО	Журналы регистрации событий системы антивирусной защиты
17.			
18.		Подключение к ИС с нетипичного узла	Журналы регистрации межсетевых экранов
19.		Подключение к ИС по нетипичным портам	
20.	DoS/DDoS	DoS-атака на сетевой узел	Журналы регистрации событий средства защиты от DDoS, системы мониторинга состояния служб и серверов или межсетевого экрана
21.		Всплеск входящего сетевого трафика	
22.		Недоступность сервиса, узла или канала связи	
23.		Всплеск нагрузки на сетевое оборудование, критические ошибки в работе сетевого оборудования	
24.	Перебор паролей	Подбор пароля пользователя с последующим успешным входом	Журналы регистрации действий пользователей в службе каталогов Active Directory, ОС, прикладном ПО, СУБД и пр.
25.		Подбор учетной записи	
26.		Большое количество блокировок пользователей в системе	
27.	Центр управления бот-сети	Подключения к вредоносным ресурсам в	Журналы регистрации

№	Тип инцидента ИБ	Возможные сценарии выявления инцидентов	Возможный источник событий информационной безопасности
28.		сети Интернет (ботнет сети)	событий проху-сервера, межсетевого экрана или средства Anti-bot защиты
		Обнаружение аномального исходящего трафика	
29.	Фишинг (мошенничество)	Подключение к фишинг-ресурсам	Журналы регистрации событий проху-сервера, межсетевого экрана
30.		Нелегитимное подключение носителей информации и мобильных устройств	Журналы регистрации событий системы контроля периферийных устройств и DLP-систем
31.	Вредоносный ресурс	Подключения систем к IP-адресам и доменам из черного списка	Журналы регистрации событий проху-сервера, межсетевого экрана
32.		Обнаружение сигнатур вредоносного ПО в файлах, получаемых из сети Интернет	Журналы регистрации событий системы антивирусной защиты и средств проактивной защиты («песочниц»)
33.	Сканирование ресурсов	Сканирование портов на узле из сети Интернет	Журналы регистрации событий проху-сервера, межсетевого экрана
34.		Поиск из Интернет открытого порта на узлах сети	
35.		Сканирование портов из внутренней сети	
36.		Поиск из внутренней сети открытого порта на узлах	
37.		Поиск открытых сетевых файловых ресурсов	
38.		Большое количество блокировок сетевого	



№	Тип инцидента ИБ	Возможные сценарии выявления инцидентов	Возможный источник событий информационной безопасности
		взаимодействия для узла сети	
39.	Спам	Получение на почтовый ящик большого объема писем, отмеченных как спам	Журналы регистрации событий системы электронной почты, DLP-системы, средства спам-фильтрации
40.		Наличие ссылок в письмах от внешних адресатов	
41.		Отправка большого количества писем на внутренние или внешние почтовые адреса	
42.		Возможная рассылка вредоносного ПО (аномальная активность в почте)	

#### 2.4.5. Прочая настройка Системы

В ходе прочей настройки Системы выполняются следующие работы:

- настройка программных средств Системы для реализации ролевой модели доступа пользователей к данным в Системе на базе настроенных прав доступа;
- заведение учетных записей пользователей, интеграция с контроллерами домена службы каталогов Microsoft Active Directory для авторизации пользователей;
- настройка программных средств Системы для представления сведений об информационных ресурсах, событиях безопасности и зарегистрированных инцидентах ИБ:
  - фильтры событий безопасности по типам подключенных в Системе источников событий безопасности;
  - группировка информационных ресурсов в Системе по следующим признакам:
    - территориальной, организационной и функциональной принадлежности сетевых узлов информационных ресурсов, например - принадлежность узлов к зонам сети или подсети (АРМ пользователей, сегмент ДМЗ, сегмент управления и пр.);
    - версия установленной операционной системы;
    - наличие уязвимостей;
    - роли или типа узла (например, сетевое оборудование, серверное оборудование или рабочие станции, файловый сервер, сервер СУБД и т.д.);
- настройка Системы для почтового оповещения ответственных сотрудников АО "Институт реакторных материалов" о собранных событиях безопасности и зарегистрированных инцидентах ИБ;
- настройка Системы для рассылки отчетов по расписанию ответственным сотрудникам АО "Институт реакторных материалов" по электронной почте;
- оформление, согласование и утверждение документа «Акт завершения предварительной настройки».

### **Этап 3. Ввод Системы в эксплуатацию.**

3.1. Разработка и согласование программы и методик предварительных испытаний, программы опытной эксплуатации, протокола проведения предварительных испытаний и акта приемки в опытную эксплуатацию, журнала опытной эксплуатации, программы и методик приёмочных испытаний протокола проведения приёмочных испытаний и акта приемки в постоянную эксплуатацию.

#### **3.2. Проведение предварительных испытаний**

В ходе предварительных испытаний Системы выполняются следующие работы:

- проведение предварительных испытаний в соответствии с документом «Программа и методика предварительных испытаний»;
- оформление и согласование документа «Протокол проведения предварительных испытаний».

По результатам предварительных испытаний осуществляется приемка Системы в опытную эксплуатацию, оформляется и утверждается документ «Акт ввода Системы в опытную эксплуатацию».

#### **3.3. Проведение опытной эксплуатации**

Продолжительность опытной эксплуатации Системы должна составлять не менее 1-ой (одной) недели и не более 4-х (четырех) недель. Условием начала опытной эксплуатации является утверждение документов «Программа опытной эксплуатации» и «Акт ввода Системы в опытную эксплуатацию». Опытная эксплуатация Системы проводится силами специалистов АО "Институт реакторных материалов" при консультационной поддержке Исполнителя. В ходе проведения опытной эксплуатации осуществляются:

- проверка корректности функционирования Системы в реальных условиях эксплуатации в АО "Институт реакторных материалов";
- доработка настроек и документации Системы (производится Исполнителем при необходимости).

На этапе опытной эксплуатации предоставляется следующая документация:

- документ «Рабочий журнал опытной эксплуатации», с выявленными в период проведения опытной эксплуатации замечаниями. В журнале фиксируются произошедшие сбои и/или отказы Системы и результат их устранения, дополнительные настройки Системы, внесенные в систему по итогам опытной эксплуатации.

#### **3.4. Проведение приёмочных испытаний**

В ходе проведения приёмочных испытаний выполняются следующие работы:

- проведение приёмочных испытаний в соответствии с документом «Программа и методика приёмочных испытаний Системы»;
- оформление и согласование документа «Протокол проведения приёмочных испытаний»

и передача Системы в постоянную эксплуатацию. Условием начала проведения приёмочных испытаний является утверждение документа «Акт завершения опытной эксплуатации».

По результатам приёмочных испытаний осуществляется приемка Системы в постоянную эксплуатацию, оформляется и утверждается документ «Акт ввода Системы в постоянную эксплуатацию» и «Акт сдачи-приемки выполненных работ».

## **5. Система мониторинга событий информационной безопасности**

Система мониторинга событий информационной безопасности предназначена для сбора, хранения, преобразования и выдачи пользователям информации об объектах информационной инфраструктуры и событиях в рамках этой инфраструктуры,

автоматизации процесса выявления инцидентов информационной безопасности и управления ими.

Система должна иметь сертификацию, подтверждающую о том, что функции безопасности системы предотвращают несанкционированный доступ к результатам сканирования, настройкам и иной важной информации, обрабатываемой системой на уровне детального изучения процессов разработки и тестирования, а также поиска уязвимостей в файлах дистрибутива системы. (Сертификация, предусмотренная ISO 15408)

## 5.1 Требования к структуре и функционированию Системы

5.1.1 Функциональные компоненты Системы должны поддерживать развертывание как на физическом, так и на виртуальном оборудовании.

5.1.2 Система должна быть построена по модульному принципу и позволять использование и установку ее в различной конфигурации.

5.1.3 В состав Системы должны входить следующие компоненты:

- Управляющий сервер;
- Агент;
- Модуль анализа сетевого трафика;
- Модуль сбора событий с конечных узлов.

В состав компонента «Управляющий сервер» должны входить следующие функциональные модули:

- модуль управления;
- модуль обработки;
- модуль развертывания и конфигурирования;
- база знаний с экспертизой вендора;
- хранилище событий (исходных и нормализованных).

В состав компонента «Агент» должны входить следующие функциональные модули:

- сканирующий модуль;
- модуль сбора событий.

Таблица 1 — Требования к функциям модулей Системы

Наименование		Требования к функциям модуля
п/п	е модуля/компонента	
<b>Управляющий сервер</b>		
1.	Модуль управления	Модуль управления должен выполнять следующие функции: <ul style="list-style-type: none"> <li>• централизованное хранения конфигурации активов;</li> <li>• централизованное управление компонентами системы;</li> <li>• оперативное реагирование на инциденты ИБ и обеспечение взаимодействия подразделений организации при расследовании этих инцидентов;</li> <li>• генерация отчетов;</li> <li>• предоставление графического интерфейса пользователя;</li> <li>• управление лицензиями;</li> <li>• привязку событий к активам;</li> <li>• построение и работа с сетевой топологией уровня 3 OSI.</li> </ul>
	Модуль обработки	Модуль обработки должен осуществлять функции по

п/п	Наименование модуля/компонента	Требования к функциям модуля
2.		обработке и хранению событий: <ul style="list-style-type: none"> <li>• централизованное хранение информации о событиях ИБ и сетевом трафике;</li> <li>• агрегацию, фильтрацию, нормализацию и корреляцию событий;</li> <li>• автоматическое создание инцидентов;</li> <li>• привязку событий к активам</li> </ul>
3.	Модуль развертывания и конфигурирования	Модуль развертывания и конфигурирования должен обеспечивать доступ к системе через сервис единого входа и журналирование действий пользователей, а также осуществлять доставку обновлений для всех компонентов Системы
4.	База знаний с экспертизой вендора	База знаний с экспертизой вендора РТ КВ должна обеспечивать получение данных о новых уязвимостях и эксплойтах, автоматическое обновление правил корреляции и применение их в IT-инфраструктуре предприятия без ручной перенастройки. База знаний устанавливается совместно с модулем управления
5.	Хранилище событий	Компонент должен осуществлять централизованное хранение информации о событиях как исходных («сырых»), так и нормализованных
6.	Сканирующий модуль	<b>Агент</b> Сканирующий модуль должен осуществлять сбор, в том числе, следующей информации о конфигурации актива: версия и производитель ОС, установленные обновления ОС, список установленного ПО, настройки ОС и ПО, пользователи и группы пользователей, аппаратное обеспечение, запущенные сетевые сервисы и службы ОС, настройки сети, настройки средств защиты
7.	Модуль сбора событий	Модуль сбора событий должен обеспечивать сбор событий от различных источников и позволять осуществлять активный и пассивный сбор событий
8.	Модуль анализа сетевого трафика	<b>Модуль анализа сетевого трафика</b> Модуль должен выполнять комплексный анализ сетевого трафика на уровнях L2-L7 сетевой модели OSI и позволять выявлять сетевые сессии, новые активы, серверное и клиентское программное обеспечение, передаваемые файлы
<b>Модуль сбора событий с конечных узлов</b> Модуль сбора событий с конечных узлов		<b>Модуль сбора событий с конечных узлов</b> Модуль должен запускаться на оконечных вычислительных узлах под управлением ОС Windows. Модуль должен обеспечивать сбор системных событий, мониторинг сетевых служб на конечных узлах, отслеживать сетевую активность узла, активность пользователей, связанную с созданием, чтением, изменением и удалением файлов

5.1.4 Система с использованием функциональных модулей должна обеспечивать реализацию следующих функциональных возможностей:

- сбор событий;
- управление активами;
- обнаружение уязвимостей;
- обработка событий;
- управление инцидентами;
- визуализация и построение отчетов;
- хранение событий;
- обновление;
- разграничение доступа пользователей Системы.

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

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

5.1.6 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 неподдерживаемых;
- модернизации и оптимизации логики обработки собираемых событий ИБ.

## **5.2 Требования к функциям Системы**

### **5.2.1 Общие требования**

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

### **5.2.2 Требования к функциям сбора событий**

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

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

5.2.2.3 Компоненты Системы должны обеспечивать возможность сбора событий в режиме, близком к реальному времени.

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

5.2.2.5 Учётные данные, необходимые для активного подключения к источникам, должны храниться в единой базе.

5.2.2.6 Должна быть обеспечена возможность использования одной записи с учётными данными для подключения к различным источникам с целью минимизации трудозатрат на корректировку учётных данных.

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

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

5.2.2.9 В Системе должны быть предусмотрены предустановленные системные профили для сбора данных.

5.2.2.10 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; частоту забора данных; количество передаваемых сообщений и т.п.).

5.2.2.11 Система должна обеспечивать сбор событий с использованием следующих механизмов и протоколов:

- сенсор в терминах протокола Cisco NetFlow;
- сообщения стандарта Syslog по протоколам TCP и UDP;
- SNMP;
- WMI;
- текстовые файлы в форматах 1CEnterprise8, AccordSucuCsvLog, FtpFileLog, Oracle Listener Log, SharePointServer, WindowsFileLog;
- отслеживание изменений в БД следующих схем данных: DeviceLockLog, Dr Web Database, ForefrontEndpointProtectionLog, InfoWatchTrafficMonitor6.1, InfoWatchTrafficMonitorLog, KasperskySecurityCenter, Kontinent\_ServerAccessLog, LinterVS\_SAVZ, LinterVS\_SOA, LinterVS\_UD\_NSD, LumensionEndpointSecurity, McAfeeEpoLog, McAfeeEpoLog4.5, OdbcLog MSSQL, OdbcLog Oracle, OracleAuditTrail, SCCMDetectSoftware, SCCMDetectUSBDevices, SCCMEvents, SecretNetLog, SecretNeLog\_Oracle, SymantecEPMSecurityEvents, SymantecEPMSystemEvents, SymantecEPMVirusAlert, SystemCenterOperationsManager, Vipnet\_StateWatcher, ZecurionZGate;
- OPSEC LEA;
- Windows Event Log;
- результаты выполнения команд на сервере по протоколу SSH;
- события платформы виртуализации VMware vSphere;
- сбор сведений о сетевых соединениях на основе анализа сетевого трафика;
- мониторинг активности в файловой системе на удаленных узлах посредством размещения специального агента.

5.2.2.12 Система должна поддерживать получение данных из источников, указанных в таблице ниже (Таблица 2).

Таблица 2 — Перечень поддерживаемых источников событий

п/п	Наименование системы	Версия
<b>Системы аутентификации, авторизации, учета</b>		
1.	Код безопасности vGate	2.7, 2.8
2.	Cisco ACS	5.x
3.	RSA Authentication Manager	8.2
<b>Системы предотвращения утечек информации</b>		
4.	InfoWatch Traffic Monitor	4.1, 6.1
5.	Zecurion zGate (основной журнал)	7
6.	Zecurion zGate (журнал Zgate Proxy)	7
7.	SmartLine DeviceLock DLP	7.3
<b>Системы защиты приложений</b>		
8.	Cisco Email Security Appliance	7
9.	Cisco Web Security Appliance	8.0
10.	McAfee Web Gateway	7.5
<b>Бизнес-приложения</b>		

п/п	Наименование системы	Версия
11.	Microsoft SharePoint Server	2013
12.	1С:Предприятие	8.2
13.	New Security Technologies SafeInspect	2.1
<b>Системы управления базами данных</b>		
14.	Microsoft SQL Server	2005, 2008, 2012
15.	Oracle Audit Trail	10g, 11g, 12c
16.	Oracle Net Listener	10g, 11g, 12c
<b>Системы защиты конечных узлов</b>		
17.	Kaspersky Administration Kit	8.x
18.	Symantec Endpoint Protection	12.1
19.	Код Безопасности Secret Net Studio	7.6
20.	Lumenson Endpoint Security	4.4
21.	Kaspersky Security Center	10.x
<b>Системы электронной почты</b>		
22.	Microsoft Exchange Server	2003, 2007, 2010, 2013
23.	Postfix	2, 3
<b>Сетевые устройства</b>		
24.	Avaya ERS	5500
25.	QTech QSW	3450-28T-AC6500-52F8300-52F
26.	Cisco IOS	12, 15
27.	Коммутатор Cisco Nexus 1000v	4.x
28.	Коммутатор Cisco Nexus 5000, 7000	5.x, 6.x
29.	Cisco WLC	Cisco WLC 7.x
30.	HPE Comware Software	5.20
31.	Palo Alto Networks PAN-OS	6.1, 7
32.	FortiNet Fortigate	5.4.x
<b>Системы защиты сети</b>		
33.	Cisco ASA	8.x, 9.x
34.	Forcepoint StoneSoft Next Generation Firewall	5.3
35.	S-Terra VPN Gate	4.1
36.	Kerio KerioControl	9.0
37.	Check Point GAiA OS	76, 77.10, 77.20, 77.30
38.	Kaspersky Security for Linux Mail Server	8.0
39.	Open Source Suricata	3.1
<b>Операционные системы</b>		
40.	FreeBSD	FreeBSD 4.9-9.2
41.	Microsoft Windows	XP (только WMI), Vista+, 2003 (только WMI), 2008, 2008R2, 2012

п/п	Наименование системы	Версия
42.	Debian	7
43.	IBM AIX	5.3, 6.1, 7.1
44.	SUSE Linux Enterprise Service	10
45.	CentOS	4.x, 5.x, 6.x, 7.x
<b>Прокси-серверы</b>		
46.	Squid	3.0-3.5
47.	Microsoft Forefront TMG	7.0
<b>Системы виртуализации</b>		
48.	VMware ESXi	5.x, 6.x
49.	VMware vCenter	5
<b>Веб-серверы</b>		
50.	Apache HTTP Server	2
51.	Nginx	1.8, 1.9
52.	Microsoft Internet Information Services	6.0, 7.5, 8.5
<b>Системы динамической адресации</b>		
53.	Microsoft DHCP Server	2008, 2012
54.	Microsoft DHCP Client	2008, 2012
55.	Microsoft Windows DNS Server	2008, 2012
<b>Системы управления обновлениями и конфигурацией</b>		
56.	Microsoft Windows Server Update Services (WSUS)	Windows Server 2008, 2008R2, 2012, 2012 R2
<b>Удостоверяющий центр</b>		
57.	Microsoft Certification Authority (CA)	Windows Server 2008, 2008R2, 2012, 2012 R2
58.	RSA Certificate Manager	6.9
<b>Системы мониторинга серверов</b>		
59.	Microsoft System Center Operations Manager (SCOM)	2012R2
<b>Системы мониторинга сети</b>		
60.	Infotecs ViPNet StateWatcher	3.2
<b>Системы организации терминального доступа</b>		
61.	Windows Terminal Server	3.2

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

5.2.2.14 Система должна позволять разрабатывать пользовательские модули сбора для работы с неподдерживаемыми поставщиками программных средств Системы протоколами передачи событий на скриптовом языке Python версии 2.7. Разработка и работа с такими модулями должна осуществляться через интерфейс Системы.



5.2.2.15 Пользовательские модули сбора должны храниться непосредственно во внутренней базе Системы в целях предотвращения подмены или несанкционированного изменения.

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

### 5.2.3 Требования к функциям управления активами

5.2.3.1 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 ящиков;
- анализа сетевого трафика;
- добавления актива пользователями («вручную»).

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

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

5.2.3.4 Система должна обеспечивать сбор идентификационных данных об активах (IP-адрес, hostname/FQDN). Механизм идентификации должен обеспечивать выявление и корректную работу с кластерными конфигурациями активов.

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

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

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

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

5.2.3.9 Система должна обеспечивать построение и управление иерархией групп активов.

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

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

5.2.3.12 Система должна обеспечивать поиск активов в браузере активов и на топологии.

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

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

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

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

5.2.3.17 Система должна обеспечивать отслеживание изменений конфигурации активов и предоставлять возможность просмотра состояния актива на заданный момент времени в прошлом.

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

5.2.3.19 Система должна позволять пользователю настраивать правила оповещения по электронной почте об изменении состава выбранных динамических групп (включение/исключение активов).

#### 5.2.4 Требования к функциям обработки событий

5.2.4.1 Система должна обеспечивать нормализацию событий с использованием встроенных формул.

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

5.2.4.3 Система должна обеспечивать агрегацию событий с использованием встроенных правил.

5.2.4.4 Система должна обеспечивать категоризацию событий.

5.2.4.5 Система должна поддерживать возможность создания пользователями собственных формул нормализации.

5.2.4.6 Система должна обеспечивать поддержку мультиязычных событий.

5.2.4.7 Система должна позволять отфильтровать события по заданным пользователем критериям и сохранять результаты фильтрации для последующего быстрого доступа к интересующим событиям. При этом должна быть предусмотрена возможность создания иерархии фильтров с помощью папок.

5.2.4.8 Система должна обеспечивать возможность корреляции событий в режиме, близком к реальному времени.

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

5.2.4.10 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 корпоративных информационных систем, 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.

5.2.4.11 Система должна предоставлять пользователю интерфейс создания пользовательских правил корреляции в т.ч. на основе встроенных системных правил.

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

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

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

5.2.4.15 Функционал табличных списков должен позволять:

- реализовывать 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.

5.2.4.16 При обращении к табличным спискам из правил корреляции должен быть доступен функционал:

- 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.

5.2.4.17 Система должна обеспечивать возможность задания правил обогащения событий, поступающих в систему, данными из табличных списков (например, добавление данных из репутационных баз).

## 5.2.5 Требования к функциям управления инцидентами

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

5.2.5.2 Система должна обеспечивать импорт инцидентов из специально подготовленных файлов.

5.2.5.3 Система должна обеспечивать категорирование инцидентов.

5.2.5.4 Система должна обеспечивать управление автоматической генерацией инцидентов.

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

5.2.5.6 Система должна обеспечивать отправку уведомлений, содержащих данные по инцидентам (по электронной почте).

5.2.5.7 Система должна обеспечивать просмотр и редактирование карточки инцидента.

5.2.5.8 Система должна предоставлять возможность поиска инцидентов в реестре инцидентов.

5.2.5.9 Система должна обеспечивать фильтрацию инцидентов с использованием системных и пользовательских фильтров. При этом должна быть предусмотрена возможность создания иерархии фильтров с помощью папок.

5.2.5.10 Система должна обеспечивать сортировку инцидентов: по времени создания, статусу, критичности, категории, названию.

5.2.5.11 Система должна обеспечивать возможность построения процесса расследования инцидента: формирование поручений для расследования, определение порядка реагирования и устранения последствий инцидентов, назначение ответственных за их решение лиц.

5.2.5.12 Система должна обеспечивать хранение истории расследования инцидента.

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

## 5.2.6 Требования к функциям визуализации и построения отчетов

5.2.6.1 Система должна обеспечивать наличие оперативных графиков (дашбордов) по событиям, инцидентам и мониторингу функционирования Системы.

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

5.2.6.3 Система должна обеспечивать отображение следующих данных по инцидентам в графическом формате (дашборды):

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

5.2.6.4 Система должна обеспечивать возможность создания и конфигурирования пользовательских дашбордов.

5.2.6.5 Система должна обеспечивать возможность формирования и отправки уведомлений (по электронной почте) в случае попадания событий или инцидентов под системный или пользовательский фильтр.

5.2.6.6 Система должна обеспечивать формирование отчетов по фильтрам (системным и пользовательским).

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

- по конфигурации,
- по событиям,
- по инцидентам,
- по мониторингу функционирования Системы.

5.2.6.8 Система должна обеспечивать построение следующих отчетов по анализу конфигурации:

- 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.

5.2.6.9 Система должна обеспечивать построение следующих отчетов по инцидентам:

- распределение новых инцидентов по времени,
- распределение утвержденных инцидентов по времени,
- распределение инцидентов в работе по времени,
- распределение разрешенных инцидентов по времени,
- распределение закрытых инцидентов по времени,
- распределение актуальных инцидентов по времени,
- распределение неактуальных инцидентов по времени,
- новые инциденты с распределением по времени, сгруппированные по критичности,

- утвержденные инциденты с распределением по времени, сгруппированные по критичности,
- инциденты в работе с распределением по времени, сгруппированные по критичности,
- разрешенные инциденты с распределением по времени, сгруппированные по критичности,
- закрытые инциденты с распределением по времени, сгруппированные по критичности,
- актуальные инциденты с распределением по времени, сгруппированные по критичности,
- неактуальные инциденты с распределением по времени, сгруппированные по критичности.

5.2.6.10 Графический интерфейс пользователя должен быть реализован по технологии Web.

5.2.6.11 Графический интерфейс пользователя должен поддерживать русский язык.

5.2.6.12 Графический интерфейс пользователя должен позволять пользователю фильтровать, группировать и сортировать события в выдаче на экран по всем доступным полям.

5.2.6.13 Система должна позволять автоматически обновлять список событий и инцидентов в выдаче на экран через определённые промежутки времени.

#### 5.2.7 Требования к функциям хранения событий

5.2.7.1 Система должна обеспечивать хранение исходных и нормализованных событий.

5.2.7.2 Пользователю Системы должна быть доступна возможность формирования поисковых запросов в БД событий.

#### 5.2.8 Требования к функциям обновления

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

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

#### 5.2.9 Требования к функциям разграничения доступа пользователей Системы

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

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

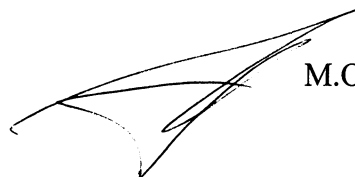
5.2.9.3 В Системе должна быть реализована модель ролевого доступа, обеспечивающая возможность разрешения или запрета доступа пользователей к информации по определённым узлам (активам) системы.

### 5.3. Требования по совместимости

Программные средства системы мониторинга событий информационной безопасности должны иметь возможность функционирования на компьютерах, работающих под управлением следующих 64-битных операционных систем:

- Ubuntu 16.04 LTS;
- Ubuntu 18.04 LTS;
- Debian GNU / Linux 8.6- 8.x;
- Debian GNU / Linux 9.4 – 9.x;
- ОСнова всех версий;
- SUSE Linux Enterprise Server 15
- Astra Linux Special Edition 1.5 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
- Astra Linux Special Edition 1.6 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды) ;
- ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем;
- ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем.

Разработал: Инженер 1 кат. ГИБ



М.О. Татаринова