Техническое задание на внедрение Системы SI и оказание услуг

Security Operation Center

Exported on Oct 10, 2024

Table of Contents

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 6

2 ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 7

3 ОБЩИЕ СВЕДЕНИЯ 8

3.1 Полное наименование АС и ее условное обозначение 8

3.2 Наименование организации 8

3.3 Плановые сроки начала и окончания работ по созданию Системы 8

3.4 Общие сведения об источниках и порядке финансирования работ 8

3.5 Порядок оформления и предъявления результатов работ 9

4 ЦЕЛИ И НАЗНАЧЕНИЕ СОЗДАНИЯ СИСТЕМЫ 10

4.1 Назначение Системы 10

4.2 Цели создания Системы 10

5 ХАРАКТЕРИСТИКА ОБЪЕКТА АВТОМАТИЗАЦИИ 11

6 ТРЕБОВАНИЯ К АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ 12

6.1 Требования к структуре ИС 12

6.1.1 К Системе применяются следующие требования: 12

6.1.2 САИВМ должна быть реализована на основе функциональных модулей: 12

6.1.3 Система должна функционировать в следующих режимах: 16

6.1.4 Требования по диагностированию Системы: 16

6.2 Требования к функциям, выполняемым ИС 18

6.3 Требования к видам обеспечения ИС 21

6.3.1 Требования к математическому обеспечению ИС 21

6.3.2 Требования к информационному обеспечению ИС 21

6.3.3 Требования к лингвистическому обеспечению ИС 21

6.3.4 Требования к программному обеспечению ИС 21

6.3.5 Требования к техническому обеспечению ИС 22

6.3.6 Требования к метрологическому обеспечению ИС 22

6.3.7 Требования к организационному обеспечению ИС 22

6.3.8 Требования к методическому обеспечению ИС 23

6.4 Общие технические требования к ИС 27

6.4.1 Требованиях к численности и квалификации персонала и пользователей ИС 27

6.4.2 Требования к показателям назначения 27

6.4.3 Требования к надежности 28

6.4.4 Требования по безопасности 29

6.4.5 Требования к эргономике и технической эстетике 29

6.4.6 Требования к транспортабельности для подвижных АС 29

6.4.7 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов ИС 30

6.4.8 Требования к защите информации от несанкционированного доступа 30

6.4.9 Требования по сохранности информации при авариях 31

6.4.10 Требования к защите от влияния внешних воздействий 32

6.4.11 Требования к патентной чистоте и патентоспособности 32

6.4.12 Требования по стандартизации 33

6.5 Дополнительные требования 33

7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ ИС 34

7.1 Предпроектное обследование 35

7.2 Проектирование 35

7.3 Внедрение Системы 36

7.4 Разработка аналитических приложений, дашбордов и отчетов 37

7.5 Опытная эксплуатация Системы 43

7.6 Приёмо-сдаточные испытания Системы 44

7.7 Перевод Системы в промышленную эксплуатацию 44

8 ПОРЯДОК РАЗРАБОТКИ ИС 46

9 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ИС 47

9.1 Общие требования к приемке работ: 47

10 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ ИС В ДЕЙСТВИЕ 48

10.1 Требования к подготовительным работам 48

10.2 Требования к обучению пользователей Системы 48

11 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ 49

* [ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ](#scroll-bookmark-2)
* [ПЕРЕЧЕНЬ СОКРАЩЕНИЙ](#scroll-bookmark-3)
* [ОБЩИЕ СВЕДЕНИЯ](#scroll-bookmark-4)
	+ [Полное наименование АС и ее условное обозначение](#scroll-bookmark-5)
	+ [Наименование организации](#scroll-bookmark-6)
	+ [Плановые сроки начала и окончания работ по созданию Системы](#scroll-bookmark-7)
	+ [Общие сведения об источниках и порядке финансирования работ](#scroll-bookmark-8)
	+ [Порядок оформления и предъявления результатов работ](#scroll-bookmark-9)
* [ЦЕЛИ И НАЗНАЧЕНИЕ СОЗДАНИЯ СИСТЕМЫ](#scroll-bookmark-10)
	+ [Назначение Системы](#scroll-bookmark-11)
	+ [Цели создания Системы](#scroll-bookmark-12)
* [ХАРАКТЕРИСТИКА ОБЪЕКТА АВТОМАТИЗАЦИИ](#scroll-bookmark-13)
* [ТРЕБОВАНИЯ К АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ](#scroll-bookmark-14)
	+ [Требования к структуре ИС](#scroll-bookmark-15)
		- [К Системе применяются следующие требования:](#scroll-bookmark-16)
		- [САИВМ должна быть реализована на основе функциональных модулей:](#scroll-bookmark-17)
			* [Модуль интеграции с источниками данных должен иметь автоматизированный функционал:](#scroll-bookmark-18)
			* [Модуль извлечения, обработки, преобразования, загрузки данных должен иметь автоматизированный функционал:](#scroll-bookmark-19)
			* [Модуль фильтрации и хранения данных (DWH) должен иметь автоматизированный функционал:](#scroll-bookmark-20)
			* [Модуль анализа и исследования должен иметь автоматизированный функционал:](#scroll-bookmark-21)
			* [Модуль визуализации данных и отчетности должен иметь автоматизированный функционал:](#scroll-bookmark-22)
			* [Модуль централизованного управления должен иметь автоматизированный функционал:](#scroll-bookmark-23)
		- [Система должна функционировать в следующих режимах:](#scroll-bookmark-24)
		- [Требования по диагностированию Системы:](#scroll-bookmark-25)
	+ [Требования к функциям, выполняемым ИС](#scroll-bookmark-26)
	+ [Требования к видам обеспечения ИС](#scroll-bookmark-27)
		- [Требования к математическому обеспечению ИС](#scroll-bookmark-28)
		- [Требования к информационному обеспечению ИС](#scroll-bookmark-29)
		- [Требования к лингвистическому обеспечению ИС](#scroll-bookmark-30)
		- [Требования к программному обеспечению ИС](#scroll-bookmark-31)
		- [Требования к техническому обеспечению ИС](#scroll-bookmark-32)
		- [Требования к метрологическому обеспечению ИС](#scroll-bookmark-33)
		- [Требования к организационному обеспечению ИС](#scroll-bookmark-34)
		- [Требования к методическому обеспечению ИС](#scroll-bookmark-35)
	+ [Общие технические требования к ИС](#scroll-bookmark-36)
		- [Требованиях к численности и квалификации персонала и пользователей ИС](#scroll-bookmark-37)
		- [Требования к показателям назначения](#scroll-bookmark-38)
		- [Требования к надежности](#scroll-bookmark-39)
		- [Требования по безопасности](#scroll-bookmark-40)
		- [Требования к эргономике и технической эстетике](#scroll-bookmark-41)
		- [Требования к транспортабельности для подвижных АС](#scroll-bookmark-42)
		- [Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов ИС](#scroll-bookmark-43)
		- [Требования к защите информации от несанкционированного доступа](#scroll-bookmark-44)
		- [Требования по сохранности информации при авариях](#scroll-bookmark-45)
		- [Требования к защите от влияния внешних воздействий](#scroll-bookmark-46)
		- [Требования к патентной чистоте и патентоспособности](#scroll-bookmark-47)
		- [Требования по стандартизации](#scroll-bookmark-48)
	+ [Дополнительные требования](#scroll-bookmark-49)
* [СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ ИС](#scroll-bookmark-50)
	+ [Предпроектное обследование](#scroll-bookmark-51)
	+ [Проектирование](#scroll-bookmark-52)
	+ [Внедрение Системы](#scroll-bookmark-53)
	+ [Разработка аналитических приложений, дашбордов и отчетов](#scroll-bookmark-54)
	+ [Опытная эксплуатация Системы](#scroll-bookmark-55)
	+ [Приёмо-сдаточные испытания Системы](#scroll-bookmark-56)
	+ [Перевод Системы в промышленную эксплуатацию](#scroll-bookmark-57)
* [ПОРЯДОК РАЗРАБОТКИ ИС](#scroll-bookmark-58)
* [ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ИС](#scroll-bookmark-59)
	+ [Общие требования к приемке работ:](#scroll-bookmark-60)
* [ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ ИС В ДЕЙСТВИЕ](#scroll-bookmark-61)
	+ [Требования к подготовительным работам](#scroll-bookmark-62)
	+ [Требования к обучению пользователей Системы](#scroll-bookmark-63)
* [ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ](#scroll-bookmark-64)

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

# ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

**Таблица 1** - Перечень сокращений

|  |  |  |
| --- | --- | --- |
| ИБ | – | Информационная безопасность |
| KPI | – | Ключевые показатели эффективности |
| АРМ | – | Автоматизированное рабочее место |
| ДМЗ | – | Демилитаризованная зона |
| ИС | – | Информационная система |
| ИТ | – | Информационные технологии |
| ОС | – | Операционная система |
| ПО | – | Программное обеспечение |
| ТЗ | – | Техническое задание |
| ПСИ | – | Приемо-сдаточные испытания |
| ПМИ | – | Программа и методика приёмо-сдаточных испытаний |
| СЗИ | – | Средства защиты информации |
| САИВМ | – | Система аналитики и визуализации метрик |
| СУБД | – | Система управления базами данных |
| ЕКХД/DWH | – | Единое Корпоративное хранилище данных |
| ЦОД | – | Центр обработки данных |
| PAM | – | Privileged Access Management |

# ОБЩИЕ СВЕДЕНИЯ

## Полное наименование АС и ее условное обозначение

Полное наименование АС: Система аналитики и визуализации метрик ИБ

Условное обозначение: САИВМ, Система

## Наименование организации

Заказчик: ООО «Группа копаний «Иннотех»

Ленинградский проспект, 36с41, Москва, 125167

Исполнитель: определяется по результатам проведения конкурсных процедур

## Плановые сроки начала и окончания работ по созданию Системы

Проект по созданию системы включает в себя следующие этапы:

|  |  |
| --- | --- |
| Наименование этапа | Срок |
| Предпроектное обследование | до 30 календарных дней |
| Проектирование | до 45 календарных дней |
| Внедрение системы | от 90 до 180 календарных дней |
| Разработка аналитических приложений дашбордов и отчетов | от 30 до 60 календарных дней |
| Функциональное тестирование | до 45 календарных дней |
| Опытная эксплуатация Системы | до 60 календарных дней |
| ПСИ Системы | от 7 до 30 календарных дней |
| Перевод в промышленную эксплуатацию | от 7 до 14 календарных дней |

## Общие сведения об источниках и порядке финансирования работ

Источником финансирования работ является Заказчик.

Порядок финансирования определяется условиями контракта.

Если в процессе создания системы Заказчик изменяет описанные в ТЗ требования, то они оформляются отдельным документом и влекут за собой изменение или дополнение существующего договора между Заказчиком и Исполнителем в части сроков выполнения и стоимости работ.

## Порядок оформления и предъявления результатов работ

ТЗ утверждается Заказчиком и является в основным регламентирующим документом при проведении работ по внедрению Системы и оказанию услуг.

# ЦЕЛИ И НАЗНАЧЕНИЕ СОЗДАНИЯ СИСТЕМЫ

## Назначение Системы

САИВМ предназначена для сбора, обработки и визуализации данных о состоянии ИБ в компании, поступающих от подключенных средств защиты информации, ИТ и бизнес систем/систем-источников, а также автоматизированного расчета метрик ИБ для повышения эффективности информационной безопасности посредством анализа, в режиме максимально приближенному к реальному времени или исторического поиска, состояния ИБ на оперативном, тактическом и стратегическом уровнях.

## Цели создания Системы

Основными целями создания САИВМ являются:

1. Повышение качества принимаемых управленческих решений, благодаря доступу к хранилищу информации, организованной удобным способом для быстрого визуального анализа;
2. Увеличение скорости получения информации для принятия решений, которое достигается исключением из цепочки преобразования данных в информацию промежуточных звеньев в виде программ и сотрудников, занимающихся выгрузкой данных и их обработкой;
3. Валидация соответствия результатов деятельности ИБ бизнес-целям Компании и построение эффективных процессов информационной безопасности за счёт непрерывного анализа текущих процессов и состояния информационной безопасности в визуальном виде данных, получаемых из систем-источников на инфраструктуре Заказчика;
4. Контроль ключевых показателей эффективности благодаря ретроспективным и оперативным данным;
5. Автоматизированное формирование отчетов о деятельности ИБ;
6. Обеспечение неизменности данных при непреднамеренном выполнении операций по передаче, хранению и обработке.

# ХАРАКТЕРИСТИКА ОБЪЕКТА АВТОМАТИЗАЦИИ

1. Система должна эксплуатироваться на выделенном виртуальном сервере, подключенном к сети Интернет и установленном на специально подготовленной площадке Заказчика.
2. Объектом автоматизации являются данные систем-источников, которые обеспечивают процессы ИБ, выполняемые в структурных подразделениях Заказчика.
3. Перечень источников данных должен включать в себя Системы:
	* системы мониторинга событий ИБ – VolgaBlob Smart Monitor;
	* системы управления заявками – Jira ServiceDesk;
	* системы контроля и управления инцидентами ИБ – TheHive.

# ТРЕБОВАНИЯ К АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

## Требования к структуре ИС

### К Системе применяются следующие требования:

1. Система должна быть развернута на базе PIX BI.
2. Система должна обладать модульной архитектурой и позволять наращивать функционал Системы на базе единой технологической и архитектурной платформы. При добавлении новых компонент, равно как и новых сервисов, должно быть достаточно добавление нового модуля к Системе, либо внесение незначительных изменений в существующую конфигурацию без изменения архитектуры Системы;
3. Система должна обеспечивать возможность вертикального, горизонтального и функционального масштабирования средствами используемого базового программного обеспечения путем добавления дополнительных функциональных модулей без изменения архитектуры системы, наращивания вычислительных мощностей, централизации/децентрализации;
4. Должна быть обеспечена непрерывная доступность Системы на всем сроке её эксплуатации, возможные сбои не должны влиять на консистентность и полноту данных Системы;
5. Система должна обеспечивать возможность периодической синхронизации с интервалом не менее 5 минут с учетом равномерного распределения/балансировки нагрузки;
6. Должна быть предусмотрена возможность создания резервных копий Системы для восстановления в случае возникновения критических ситуаций;
7. Система должна обеспечивать визуализацию метрик ИБ и предоставлять отчеты;
8. Система должна предоставлять возможность предотвращения аварийных ситуаций;
9. Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных;
10. Подключение источников данных должно поддерживать интеграцию через API . Должны быть API для: выгрузки данных, изменения конфигураций, подключения источников (интеграций), выполнения поисковых запросов, управления сервисами/службами Системы;
11. Система должна быть реализована полностью на оборудовании Заказчика, исключающим необходимость расположения вне корпоративных сетей Заказчика;
12. Система должна быть построена на компонентах, исключающих отказ вендора и/или интегратора в их обслуживании в связи с санкционной деятельностью третьих лиц;
13. Функционал Системы, описанный в требованиях данного ТЗ, должен быть выполнен по технологии, исключающей необходимость разработки программного кода Заказчиком.

### САИВМ должна быть реализована на основе функциональных модулей:

1. Модуль интеграции с источниками данных;
2. Модуль извлечения, обработки, преобразования, загрузки данных в Систему;
3. Модуль фильтрации и хранения данных;
4. Модуль анализа и исследования данных;
5. Модуль визуализации данных и отчетности;
6. Модуль централизованного управления и распределения данных.

#### Модуль интеграции с источниками данных должен иметь автоматизированный функционал:

1. Подключения источников данных, включая реляционные, базы данных (SQL, NoSQL), файловые хранилища, облачные хранилища данных и другие, как напрямую к Системе, так и через хранилища данных;
2. Тестирования и отладки интеграции с источниками данных, для валидации данных;
3. Создания и хранения шаблонов настроек источников данных;
4. Обработки исключений и уведомления в случае возникновения ошибок или проблем при интеграции с источниками данных;
5. Обеспечения безопасности данных в процессе интеграции и извлечения, включая шифрование при передаче данных и управление доступом к данным и источникам данных;
6. Подключения новых источников данных по REST API с помощью универсального коннектора.

#### Модуль извлечения, обработки, преобразования, загрузки данных должен иметь автоматизированный функционал:

1. Управления, в том числе редактирование набора данных и обновление данными по требованию, и по расписанию;
2. Настройки и изменения параметров загрузки данных для каждого источника данных или типов источников;
3. Управления расписанием загрузки и обновления данных для каждого источника данных или типов источников;
4. Настройки инкрементальной загрузки данных для обновления только тех данных, которые изменились с момента предыдущей загрузки;
5. Восстановления данных в случае сбоев или ошибок, возникающих в процессе извлечения, преобразования и загрузки данных в Систему;
6. Извлечения данных из различных источников, включая базы данных, файлы, расположенные на корпоративных сетевых хранилищах (csv, xlsx, txt, pdf, html, qvd) и других структурированных, и неструктурированных источников;
7. Настройки параметров загрузки данных для каждой модели данных, дашборда и источника в отдельности;
8. Обработки данных различных форматов: текстовые, числовые, временные, графические JSON, XML и другие;
9. Формирования протоколов загрузки данных, отражающих полноту загруженных в систему данных, а так же отражающих проблемные или подозрительные записи, не прошедшие контроль качества, например: соответствие типов данных, разрядность, контрольные суммы;
10. Настройки уведомлений в случае возникновения ошибок или проблем в процессе преобразования данных, включая уведомления об аномалиях, отслеживание производительности и статусов обновления данных.

#### Модуль фильтрации и хранения данных (DWH) должен иметь автоматизированный функционал:

1. Обработки больших массивов данных в режиме реального времени и в режиме исторического поиска;
2. Хранения больших массивов данных в контуре Заказчика в течение не менее 3-х лет;
3. Настройки модели данных, отражающую структуру и связи разного вида между данными, в том числе в графическом представлении установленных связей;
4. Создания и настройки всевозможных сочетаний значений из двух и более таблиц;
5. Настройки форматов хранения данных, включая сырые, обработанные, агрегированные и иные форматы данных;
6. Выгрузки данных для хранения в JSON;
7. Создания настраиваемых фильтров и критериев для группировки данных;
8. Сквозной фильтрации и группировки данных при переходе на другой лист/в другой отчет, сохраняя установленные настройки;
9. Настройки слайдеров или окон ввода для количественной фильтрации;
10. Обнаружения информации в неструктурированной совокупности данных (Data Discovery);
11. Настройки механизма индексации данных для оптимизации запросов и ускорения доступа к информации;
12. Выявления, уведомления и устранения ошибок и исключений в процессе обращения к данным.

#### Модуль анализа и исследования должен иметь автоматизированный функционал:

1. Оценки эффективности ИБ (KPI), управления весовыми коэффициентами, целевыми и пороговыми значениями;
2. Настройки иерархической структуры KPI;
3. Создания и настройки сложных математических и логических вычислений, включая формулы с использованием функций, условных операторов и переменных;
4. Сохранения аналитических запросов, настроек и параметров пользователя для возможности их последующего использования и повторного анализа;
5. Экспорта результатов анализа в различные форматы для дальнейшего использования и обмена информацией.

#### Модуль визуализации данных и отчетности должен иметь автоматизированный функционал:

* Создания и настройки набора визуализаций. Должны быть доступны визуализации:
	1. графики;
	2. различные карты:
		+ карта сети,
		+ карта России с разбивкой по макрорегионам и регионам;
	3. матрицы;
	4. таблицы;
	5. диаграммы:
		+ столбчатые,
		+ точечные и пузырьковые различной плотности,
		+ каскадные,
		+ линейчатые,
		+ блочные,
		+ радарные,
		+ круговые,
		+ кольцевые диаграммы с возможностью вывода общей суммы в центре диаграммы;
	6. комбинированные диаграммы и гистограммы;
	7. воронковые диаграммы;
	8. диаграммы датчиков;
	9. светофоры и спидометры;
	10. диаграммы «дерево»;
	11. дерево декомпозиции;
	12. числовое табло;
	13. диаграмма Ганта;
	14. диаграмма Сэнкей;
	15. календарь событий;
	16. облако слов;
	17. графы связей;
	18. векторные диаграммы;
	19. лента времени;
	20. сортировщик;
	21. другие.
* Создания и изменения аналитических панелей, создания собственных и настройки встроенных метрик/KPI и визуализации, включая цветовую гамму, типы линий, шрифты, размеры и другие параметры, с целью создания индивидуализированных визуальных представлений под нужды разных пользователей;
* Применения фильтров и сохранения такой фильтрации при обновлении данных для конкретного пользователя;
* Добавления на дашборд и/или в отчет автономных изображений, логотипов, текстовых описаний;
* Совместной разработки метрик, визуализаций, историй и отчетов группой пользователей внутри Системы;
* Настройки параметров публикации отчетов:
на почту/мессенджер;
* Выгрузки визуализаций и отчетов в различные форматы: PNG, JPG, CSV, XLSX, PDF, PPTX, SVG и др. Должна быть возможность их встраивания в другие приложения и документы.

#### Модуль централизованного управления должен иметь автоматизированный функционал:

1. Обеспечения стабильной работы Системы, безопасности и целостности данных, удаленное централизованное управление и контроль за всеми распределенными модулями/компонентами Системы, в которых планируется развертывание Системы.
2. Управления модулями/компонентами Системы, редактирования и удаления пользовательских аккаунтов, определение и назначение ролей с различными уровнями доступа (Row Level Security);
3. Управления активными сеансами пользователей, а также отслеживания и прерывания подозрительных или длительных транзакций;
4. Настройки системных оповещений для мониторинга состояния Системы, важных событий и нарушений безопасности;
5. Мониторинга и контроля состояния модулей Системы и потоков данных с подключённых источников данных;
6. Централизованного управления источниками данных и настройками загрузок/интеграции;
7. Централизованного управления модулями, их конфигурациями и любыми дополнениями, включая их установку, удаление, обновление и изменение;
8. Централизованного управления данными в оперативном доступе, архивами (активация, деактивация, реиндексация), параметрами хранения данных, фильтрами, настройками сетевой конфигурации.

### Система должна функционировать в следующих режимах:

1. Штатный режим – основной режим функционирования, при котором Система и смежные системы работают без сбоев и выполняют обмен данными, Система реализует свою функциональность в полном объеме без потерь производительности.
2. Сервисный режим – режим, при котором в Системе по запланированному графику проводится обслуживание, реконфигурация или обновление модулей. В данном режиме все модули Системы функционируют в полном объеме и обеспечивают информационный обмен между модулями, не затронутыми работами на обновляемом модуле. В данном режиме допускается частичная потеря производительности, возможна кратковременная недоступность Системы с целью проведения функциональных изменений или необходимых технологических работ.
3. Аварийный режим – режим, при котором Система продолжает работу в случае выхода из строя одного из функциональных модулей. В данном режиме все модули Системы, кроме вышедшего из строя модуля, функционируют в полном объеме и обеспечивают информационный обмен между системами, не затронутыми сбоем вышедшего из строя модуля.

### Требования по диагностированию Системы:

Система должна удовлетворять следующим требованиям по диагностированию:

1. Централизованная регистрация/журналирование и отслеживание всех событий интеграции, системных ошибок и других ИБ/ИТ событий в Системы.
2. Должно быть реализовано логирование действий пользователей Системы при выполнении работ, включая логирование запросов с указанием детальной информации, должна быть возможность отслеживать время выполнения транзакций/запросов и определять их инициатора.
3. В журнале аудита должны фиксироваться события создания, удаления, блокирования и разблокирования УЗ пользователя (в том числе встроенных УЗ), а также изменения аутентификационных данных.
4. Должны фиксироваться как входы пользователей в Систему, так и выходы (при наличии технической возможности) из нее.
5. Должны фиксироваться неуспешные попытки аутентификации.
6. Должна фиксироваться информация по устройству, с которого осуществлен вход (попытка входа), например, IP-адрес или имя устройства.
7. Должно фиксироваться назначение пользователю прав доступа к данным и функциям Системы, а также изменение прав доступа.
8. Должны фиксироваться изменения параметров и системных настроек компонентов Системы с указанием новых значений параметров и настроек.
9. Должно фиксироваться изменение системного времени или настроек синхронизации системного времени.
10. Должны фиксироваться все случаи недоступностиов составных частей Системы.
11. Должна осуществляться регистрация событий, связанных с созданием, копированием, в том числе резервным, и/или удалением ресурсов (баз данных, систем-источников).
12. Должна осуществляться регистрация событий, связанных с внесением изменений/удалением журналов аудита.
13. Должна осуществляться регистрация событий сетевых подключений как входящих, так и исходящих.
14. Должны регистрироваться события создания/запуска программных процессов и исполнение команд интерпретаторами.
15. Сообщения об ошибках должны предоставляться в формате, доступным для чтения человеком и автоматизированной системой, содержать в себе уникальный идентификатор события, по которому возможен поиск в журнале Системы, дата и время возникновения ошибки, информацию о причине возникновения ошибки. Действия по обработке и устранению ошибок должны быть описаны в документации на Систему.
16. В журнале Системы для каждого типа события, как минимум, должна быть зарегистрирована информация, состав и содержание которой включает:
	* дата и время (timestamp в формате UTC с точностью до секунды);
	* идентификатор (представляет собой уникальный идентификатор события, который должен позволять однозначно идентифицировать событие в электронном журнале аудита событий компонента Системы);
	* наименование действия в Системе, повлекшее к его регистрации или причина возникновения события;
	* субъект доступа (имя учётной записи пользователя или иные идентификационные данные, позволяющие сопоставить субъект доступа с событием);
	* тип ИБ или ИТ события, подлежащего регистрации;
	* уровень важности: влияет на приоритетность обработки события: аварийный/фатальный/критический/высокий/средний/низкий/отладочный/информационный и другие приоритеты.
17. В Системе должен быть предусмотрен функционал передачи событий посредством стандартных протоколов.
18. Журналы аудита не должны содержать конфиденциальную информацию, в частности, пароли пользователей, данные платежных карт и другие конфиденциальные данные.
19. Должна быть реализована ротация журналов событий. Журналы событий компонентов Системы должны иметь средства для очистки журнала аудита за определенный промежуток времени с фиксацией данного события в журнале аудита.
20. Журналы аудита должны обеспечивать хранение событий, регистрируемых в течение не менее трех суток.

## Требования к функциям, выполняемым ИС

1. В системе должен быть реализован механизм хранения «очереди» входящих и исходящих данных во внешние системы в случае временной недоступности.
2. Система должна обеспечивать 100% загрузку данных. Загрузка данных должна быть обеспечена при любом режиме функционирования Системы в том числе с помощью очереди отложенных данных, в случае недоступности Системы, и запросов, в случае недоступности систем-источников.
3. Система не должна нарушать работоспособность систем-источников.
4. В Системе должна быть возможность настройки параметров подключения источников данных, включая учетные данные, порты, протоколы и другие параметры.
5. Система должна обеспечивать централизованную регистрацию и отслеживание состояния модулей Системы посредством дашборда для мониторинга метрик производительности всех модулей.
6. Модуль загрузки данных должен обеспечивать выполнение следующего набора функций:
	1. Загрузка первоначального массива данных в Систему;
	2. Загрузка обновлений данных, накопленных с последней загрузки;
	3. Формирование протоколов загрузки данных отражающих полноту загруженных в Систему данных и проблемные или подозрительные записи, не прошедшие контроль качества, например: соответствие типов данных, разрядность, контрольные суммы;
	4. Настройка и изменение параметров загрузки данных: периодичности, зависимости одного потока загрузки от другого;
	5. Ручная инициация загрузки/обновления данных;
	6. Сохранение данных в формате Системы, для последующего использования;
	7. Формирование логов загрузки данных.
7. Система должна обеспечивать загрузку данных без потери данных с соблюдением показателей назначения.
8. Система должна обеспечивать автоматическое обнаружение структуры данных в источниках и предоставлять пользователю удобные средства для выбора необходимых полей.
9. В Системе должна быть предусмотрена возможность загрузки тестовых данных в формате xlsx, csv, а также возможность указывать id измерений/мер в тестовых данных напрямую из тестового файла.
10. В системе должен быть реализован механизм преобразования данных. Механизм преобразования данных должен обеспечивать преобразование данных, включая изменение формата, агрегацию, фильтрацию, вычисления новых полей и другие манипуляции.
11. Система должна обеспечивать возможность дополнительного категорирования данных, загруженных из систем-источников, а также возможность редактирования данных, внесения дополнительной информации для расширения сведений о событиях , получаемых от систем-источников.
12. Система должна обеспечивать автоматическое обновление данных, с возможностью настройки расписания для каждой группы данных на любом этапе: сбор, визуализация, рассылка.
13. Система должна обеспечивать поддержку языка запросов и трансформаций данных, предоставляя пользователям возможность использования различных операций и преобразований.
14. Система должна обеспечивать простоту в написании запросов для преобразования таблиц данных посредством использования конструктора запросов.
15. В системе должен быть реализован механизм автоматической инкрементальной загрузки обработанных данных в хранилище данных.
16. Система должна обеспечивать возможность гибко настроить фильтры: задать несколько параметров в условия работы одного фильтра, ограничить распространение/действие фильтра на конкретные визуализации, задать значения по умолчанию, ограничить набор значений, предлагаемых для фильтрации.
17. В системе должны быть фильтры и параметры по времени, дате, значениям, позволяя пользователям динамически настраивать условия анализа.
18. В системе должна быть строка поиска для контекстного поиска с возможностью определения глубины поиска, например: по всем дашбордам/конкретному дашборду/конкретной визуализации/по типу визуализаций/по источнику/по всему хранилищу данных.
19. В системе должен быть встроенный календарь для поиска за произвольный отрезок времени.
20. В системе должен быть реализован механизм автоматической оптимизации и поддержки хранилища данных с учетом требований к производительности.
21. Система должна предоставлять возможность самостоятельного исследования данных пользователями (Self-service BI).
22. Система должна обеспечивать простоту написания поисковых запросов. Например, обычный html запрос или SQL-подобный язык запросов, поддерживающий стандартные операторы, подзапросы, агрегацию, использование индексов, оптимизацию запросов и расширенный набор аналитических функций.
23. При формировании поисковых запросов Система должна обеспечивать обработку ошибок и исключений, предоставляя информацию об ошибках и предлагая возможности их устранения.
24. В системе должна быть возможность подстановки параметров и передача параметров в запросы к данным.
25. Система должна предоставлять возможность любому пользователю прервать выполнение транзакции/запроса, не дожидаясь ее завершения.
26. Система должна предоставлять возможность агрегирования данных с использованием стандартных функций, таких как SUM, AVG, MIN, MAX, COUNT, а также поддерживать пользовательские агрегатные функции.
27. Система должна предоставлять возможность отмечать запросы для переноса их в топ-лист поисковых запросов, для каждого пользователя в отдельности.
28. Система должна предоставлять возможность группировки данных по различным измерениям, включая временные, и возможность создания сводных таблиц, визуализаций и отчетов из результатов поискового запроса.
29. Система должна предоставлять инструменты для визуализации результатов анализа, включая графики, диаграммы и таблицы, для более наглядного представления информации.
30. В системе должна быть возможность реализовать оконные функции для проведения анализа данных в рамках определенных временных или логических интервалов, таких как расчет скользящих средних или накопительных сумм.
31. В системе должны быть сценарии для проведения сравнительного анализа, включая анализ изменений, сопоставление различных периодов и выявление ключевых отличий.
32. Запросы пользователя, преобразования в визуализациях и другие операции с данными не должны приводить к изменению данных.
33. В Системе должны быть визуальные конструкторы интерактивных дашбордов и отчетности, а также возможность в один клик заменить тип визуализации.
34. В Системе должна быть сетка с настраиваемой размерностью для равномерного распределения и выравнивания элементов на листе.
35. В Системе должна быть возможность задавать размер/положение в виде фиксированного числа пикселей и в процентном соотношении.
36. Система должна предоставлять возможность создания связанных дашбордов, которые используют общие данные.
37. Система должна предоставлять возможность использования динамических параметров.
38. В Системе должны быть интерактивные элементы управления, такие как фильтры, выпадающие списки и переключатели для динамической адаптации данных на дашборде под требования пользователя.
39. Система должна предоставлять возможность пользователям создание собственных представлений/ историй (data storytelling).
40. Система должна обладать инструментами для удобной навигации по дашборду, включая возможность настроить actions на дашбордах, создание гиперссылок с открытием в новом окне, закладок и интерактивных панелей управления, всплывающих подсказок (tooltip).
41. Система должна быть интегрирована с аналитическим движком для получения и оперативного обновления данных на дашборде.
42. В Системе должна быть возможность анализировать информацию в рамках «единого окна»свозможностью изменения глубины выборки (drill-down, drill-up).
43. Система должна предоставлять возможность прямого доступа к источникам данных из визуализаций для детального анализа и получения контекста.
44. В Системе должен быть встроенный набор настраиваемых отчетов и разработанных метрик с учетом возможности создания пользователем Системы отчетов в корпоративном стиле Заказчика.
45. В Системе должна быть возможность настройки общих стилей и стилей для конкретного листа.
46. Система должна предоставлять возможность автоматически формировать, в том числе при достижении KPI пороговых значений и, при необходимости рассылать, отчеты разного вида для заданного набора адресатов.
47. Система должна предоставлять возможность отправлять один и тот же шаблон/макет отчета с разными параметрами, например, фильтры, расписание, получатели.
48. Система должна предоставлять возможность обмениваться визуализациями внутри Системы.
49. В системе должен быть реализован механизм аудита и логирования всех событий для отслеживания состояний системы, ошибок в работе, действий пользователей, изменений в данных.
50. В системе должны вестись записи в журнал изменений для отслеживания изменений и возможности отката к предыдущим конфигурациям.
51. Система должна обеспечивать управление конфигурацией Системы, включая настройки подключения к базам данных, параметры безопасности и настройки производительности.

## Требования к видам обеспечения ИС

### Требования к математическому обеспечению ИС

Требования отсутствуют.

### Требования к информационному обеспечению ИС

Информационный обмен между модулями Системы должен удовлетворять следующим положениям:

1. Все взаимодействия должны контролироваться подсистемой безопасности;
2. Все модули должны использовать общую базу данных с учетом хранения больших массивов данных, защищая их от системных сбоев и случайной порчи;
3. Все модули должны использовать общие конфигурационные файлы;
4. Все модули должны обеспечить резервное копирование в объеме, достаточном для восстановления модулей Системы в состояние, предшествующее переходу системы в аварийный или сервисный режим функционирования;
5. Все модули должны поддерживать возможность эксплуатации с использованием технологии виртуализации;
6. Обмен между компонентами системы должен быть выполнен с использованием зашифрованных протоколов.

### Требования к лингвистическому обеспечению ИС

1. Интерфейсы пользователей Системы, сообщения, генерируемые Системой в процессе установки и работы, должны обеспечивать поддержку русского языка.
2. У каждого пользователя должна быть возможность выбора/переключения языкаа: русский/английский.
3. Основной язык интерпретации событий журналов Системы – английский, дополнительный – русский.
4. Системное и прикладное ПО, которое используется при реализации проекта должно быть локализовано (русскоязычные версии).
5. Встроенная справка должна быть на русском и английском языке.
6. Все документы должны готовиться и представляться пользователю на русском языке.

### Требования к программному обеспечению ИС

1. Исполнитель, на стадии технического проектирования, должен определить количественный и качественный состав программных средств. Программное обеспечение Системы должно позволять эффективно решать поставленные задачи.
2. Прикладное программное обеспечение, требуемое для реализации Системы, предоставляется Исполнителем в соответствии с разработанной проектной документацией и должно поддерживать работу на виртуальных машинах.
3. Система не должна предъявлять ограничения, включая лицензионные, на:
	1. объемы обрабатываемых, индексируемых и хранимых данных,
	2. на количество подключаемых источников данных и/или их тип.
4. Система должна обеспечивать независимость от коммерческого программного обеспечения сторонних производителей, не входящих в комплект поставки.

### Требования к техническому обеспечению ИС

1. Исполнитель на стадии технического проектирования должен определить количественный и качественный состав технических средств. Техническое обеспечение Системы должно позволять эффективно решать поставленные задачи. Поставка технического обеспечения не предусмотрена.
2. Требования к серверному оборудованию, программным и аппаратным средствам, системам хранения данных должны быть определены и уточнены на этапе предпроектного обследования и отражены в «Пояснительной записке к техническому проекту».
3. Количество серверов и их мощностные характеристики должны быть рассчитаны в зависимости от планируемого или фактического потока событий от систем-источников с запасом в 20%.

### Требования к метрологическому обеспечению ИС

1. Точность вычисления в САИВМ должна соответствовать стандарту IEEE 754-2008.
2. Система должна обеспечивать возможность отслеживания затраченного времени на выполнение математических операций и преобразований.
3. Система должна обеспечивать возможность отслеживания затраченного времени на получение, загрузку и предоставление данных.

### Требования к организационному обеспечению ИС

1. Организационное обеспечение системы должно быть достаточным для эффективного выполнения персоналом возложенных на него обязанностей при осуществлении автоматизированных и связанных с ними неавтоматизированных функций системы.
2. Заказчиком должны быть определены должностные лица, ответственные за:
	1. обработку информации АС;
	2. администрирование АС;
	3. обеспечение безопасности информации АС;
	4. управление работой персонала по обслуживанию АС.
3. Настройку существующей системы мониторинга Заказчика выполняет Исполнитель под контролем экспертов Заказчика.
4. В рамках проекта Исполнителем должны быть:
	1. доработаны и согласованы с Заказчиком основные метрики мониторинга производительности и доступности Системы и ее модулей;
	2. все модули Системы поставлены на мониторинг в соответствии с разработанными метриками.
5. Система должна поставляться с поддержкой Вендора, включая возможность технически доработать Систему под нужды Заказчика и оперативно выпускать пакеты изменений.
6. Расширенная поддержка должна соответствовать следующим требованиям:
	1. Круглосуточная доступность услуги подачи обращений – 24х7.
	2. Время реакции на новое обращение в рабочее время от 30 мин до 24 часов в зависимости от приоритета.
	3. Время обработки критичных обращений, до устранения проблемы или подтверждения Заказчика – до 48 часов.
	4. Различные способы подачи обращений: email/telegram/телефон с регистрацией на портале.
	5. Выделенный специалист.
	6. Отсутствие ограничений по числу обращений.
	7. Возможность дистанционных или выездных работ по диагностике, настройке и отладке специалистом поддержки Вендора.

### Требования к методическому обеспечению ИС

1. В рамках проекта Исполнителем должны быть разработаны и согласованы с Заказчиком документы «Пояснительная записка к техническому проекту (Техническое решение)», «Инструкция пользователя системы», «Инструкция администратора системы».
2. Документ «Пояснительная записка к техническому проекту (Техническое решение)» должен описывать полный ландшафт технической инфраструктуры комплекса технических средств Системы, содержать детальные схемы, их описания, настройки для каждого модуля Системы, перечень и описание всех функций, описывать информационные потоки между системами и подсистемами, содержать структуру Системы, схемы взаимодействия и описание каждой интеграции, детальные требования к межсетевому взаимодействию, описывать разметку систем хранения данных, ключевые настройки системы виртуализации, описание технических решений. Документ «Пояснительная записка к техническому проекту (Техническое решение)» должен содержать обязательные разделы:
	* Описание процесса деятельности
	* Основные технические решения:
		+ Перечень функций
		+ Структура системы
	* Описание технических решений:
		+ Источники данных
		+ Модели данных
		+ Хранение данных
		+ Поиск по данным
		+ Оповещения и отчетность
		+ База знаний
		+ REST API
	* Мероприятия по подготовке системы к вводу в эксплуатацию:
	* Мероприятия по подготовке персонала
	* Мероприятия по первоначальному конфигурированию системы
	* Мероприятия по внесению изменений системы
3. Документ «Инструкция пользователя Системы» должен описывать все необходимые инструкция, действия и операции доступные пользователю Системы. Документ «Инструкция пользователя системы» должен содержать обязательные разделы:
	* Введение
		+ Область применения
		+ Документы и справочные материалы
		+ Определения и аббревиатуры
	* Обзор продукта
		+ Описание продукта
		+ Функции и возможности
	* Регистрация и аутентификация
		+ Процесс входа в систему
		+ Восстановление забытого пароля
	* Интерфейс пользователя
		+ Главный экран
		+ Меню и навигация
		+ Пользовательские настройки
		+ Использование виджетов и плагинов
	* Основные функции
		+ Управление данными
		+ Загрузка и сохранение данных
		+ Поиск и фильтрация данных
	* Работа с проектами
		+ Создание нового проекта
		+ Редактирование и управление проектами
		+ Совместная работа
		+ Настройка прав доступа
		+ Создание и использование шаблонов
		+ Применение шаблонов к проектам
	* Расширенные функции
		+ Автоматизация задач
		+ Настройка автоматических действий
		+ Использование макросов
		+ Кастомизация функционала
		+ Настройка пользовательских виджетов
		+ Модификацияа
		+ Расширенная аналитика и отчетность
		+ Создание комплексных отчетов
4. Документ «Инструкция администратора Системы» должен описывать все инструкция, действия и операции необходимые администратору Системы. Документ «Инструкция администратора системы» должен содержать обязательные разделы:
	* Введение
		+ Область применения
		+ Документы и справочные материалы
		+ Определения и аббревиатуры
	* Архитектура системы
		+ Общий обзор архитектуры
		+ Компоненты системы
		+ Взаимодействие компонентов
	* Установка и первоначальная настройка
		+ Требования к системе и серверному оборудованию
		+ Процесс установки
		+ Первоначальная конфигурация системы
	* Управление пользователями
		+ Создание и управление учетными записями
		+ Назначение ролей и прав доступа
		+ Мониторинг активности пользователей
	* Настройки безопасности
		+ Конфигурация параметров безопасности
		+ Управление сетевыми правилами
		+ Журналирование и аудит
	* Резервное копирование и восстановление
		+ Планирование резервного копирования
		+ Восстановление данных
		+ Тестирование плана восстановления
	* Мониторинг системы
		+ Мониторинг производительности системы
		+ Анализ логов
		+ Оптимизация ресурсов
	* Обновление и обслуживание
		+ Планирование и реализация обновлений
		+ Управление версиями
		+ Техническое обслуживание
	* Интеграция с другими системами
		+ Конфигурация интеграции
		+ Управление API
		+ Совместимость и тестирование
5. Процедура резервного копирования разрабатывается Исполнителем в рамках документа «Пояснительная записка к техническому проекту (Техническое решение)» и должна описывать сценарии выполнения резервного копирования, расписание, объемы, глубину хранения и сущности, которые необходимо резервировать в Системе.
6. Исполнителем должен быть разработан раздел «Матрица разграничения ответственности при эксплуатации системы» документа «Пояснительная записка к техническому проекту (Техническое решение)».
7. Исполнителем должен быть разработан раздел «Комплекс программно-технических средств» документа «Пояснительная записка к техническому проекту (Техническое решение)». Раздел должен описывать техническую и системную инфраструктуру: серверная платформа, операционные системы, системы хранения данных, каналы передачи данных и других значимых модулей, и объектов инфраструктуры.
8. Исполнителем должен быть разработан раздел «Ролевая модель системы» документа «Пояснительная записка к техническому проекту (Техническое решение)», включающий в себя список ролей управления, содержащий следующие сведения о каждой роли:
	1. наименование роли;
	2. полномочия роли в Системе;
	3. описание действий, выполняемых данной ролью.
9. Исполнителем должен быть разработан раздел «Обеспечение информационной безопасности системы» документа «Пояснительная записка к техническому проекту (Техническое решение)», который должен описывать применяемые организационно-технические методы и средства защиты Системы.
10. Перечень проверок, позволяющий оценить производительность Системы, разрабатывается Исполнителем в рамках документа «Программа и методика приёмо-сдаточных испытаний» и согласовывается с Заказчиком.
11. Для обеспечения взаимодействия между пользователями Системы должен быть сформирован «Регламент эксплуатации Системы», в котором должны быть зафиксированы процессы Заказчика с четким распределением зон ответственности и отражены:
	1. решения административных вопросов, например, предоставление допусков, оформление заявок подразделениями;
	2. решения инженерно-технических вопросов, например, согласование технических аспектов эксплуатации и администрирования Системы, определение наличия и размещения технических средств, коммуникаций;
	3. порядок разработки или изменения аналитических ответов\дашбордов\отчетов\визуализаций\метрик и других аналитически ресурсов;
	4. согласования и принятия оперативных решений по вопросам эксплуатации.
12. Для защиты от ошибочных действий пользователей Системы необходимо в «Регламенте эксплуатации Системы» зафиксировать процесс резервного копирования и восстановления модулей Систем в случае их преднамеренного или непреднамеренного удаления/повреждения. Под процессом понимается порядок взаимодействия, последовательность действий с указанием ключевых участников, сроков, частоты, входными и выходными данными на каждом этапе.
13. В рамках разработки Системы должны быть определены и задокументированы в «Регламенте эксплуатации Системы» подходы и правила контроля, разработаны инструменты управления доступом создаваемой Системы.
14. «Инструкция администратора» должна содержать раздел, описывающий процесс интеграции с Системой, включая описание REST API и инструкцию, описывающую, как проводить интеграцию и что необходимо учесть для успешного завершения интеграции.

## Общие технические требования к ИС

### Требованиях к численности и квалификации персонала и пользователей ИС

1. Система должна обеспечивать одновременную работу не менее 50 пользователей в веб-интерфейсе без потери функциональности;
2. Эксплуатация САИВМ должна осуществляться группой технических специалистов Заказчика, прошедших соответствующую подготовку.
3. Обучение специалистов Заказчика должно быть обеспечено Исполнителем в рамках реализации проекта до внедрения Системы.

### Требования к показателям назначения

По результатам проекта должны быть обеспечены целевые показатели:

* Одновременная работа в Системе не менее 50 пользователей.
* Время отклика на действия пользователя в веб-интерфейсе не более 5 секунд.
* Среднее время обработки поискового запроса в часы наибольшей нагрузки – не более 10 секунд.
* Время зависания при работе с дашбордами при использовании фильтров, drill-down, drill-up не более 3 секунд.
* Первичная полная загрузка дашборда/аналитического приложения не более 10 секунд.
* Время полного восстановления данных не должно превышать 20 минут/ТБ, время восстановления из последней резервной копии не должно превышать 30 минут.
* Время простоя Системы не более 10 дней в год.
* Ресурсы Системы должны быть утилизированы не более, чем на 80% на момент завершения этапа ПСИ.
* Хранения детализированных данных не менее 90 дней, преобразованных данных не менее 3-х лет.
* Индексация десятков\сотен ТБ в сутки, со скоростью не менее 20 мин/ТБ.
* Интервал создания резервных копий БД, функциональных компонентов и их конфигураций – не реже одного раза в две недели.
* Система должна обеспечивать высокую доступность. Время доступности системы должно составлять не менее 97%.
* Система должна выполнять действия и операции для эталонного набора данных (23.02.2024-29.02.2024), не дольше чем:
 **Таблица 2** - Время выполнения операций

|  |  |
| --- | --- |
| Наименование операции | Максимальное время, сек |
| Выгрузка данных в формат pdf | 9,04 |
| Выгрузка данных в формат pdf | 6,88 |
| Загрузка данных в UI | 4,44 |
| Время загрузки таблицы в UI | 3,08 |
| Время загрузки столбчатой диаграммы в UI | 3,06 |
| Время загрузки круговой диаграммы в UI | 3,37 |
| Время загрузки числового значение в UI | 3,29 |
| Время полной загрузки данных из источника | 2148 |

### Требования к надежности

1. Надежность Системы должна быть не менее 97%, время простоя не более 10 дней в год. Данное требование распространяется на все модули Системы.
2. Время полного восстановления данных не должно превышать 8 часов (20 мин/ТБ), среднее время обработки поискового запроса в часы наибольшей нагрузки – не более 10 секунд.
3. При сбоях, приводящих к перезагрузке ОС, в течение 30 мин должно происходить автоматическое восстановление работы Системы, включая перезапуск ОС автоматический старт компонентов системы, подгрузку данных за период простоя.
4. Разработка и релиз новых метрик, аналитических приложений, отчетов и других действий в рамках эксплуатации системы не должны приводить к простою или деградации существующих приложений, функционала или Системы.
5. Сохранность информации в Системе должна быть обеспечена в случаях отказов и аварий сетевого оборудования, серверного оборудования и системного программного обеспечения.
6. Сохранность информации в Системе должна обеспечиваться дублированием серверного и сетевого оборудования - «горячий резерв», резервированием, разработкой и реализацией плана резервного копирования и восстановления работоспособности Системы после сбоев согласно разработанному документу «Регламент эксплуатации Системы».
7. Для аварийных ситуаций, связанных с отказом других телекоммуникационных компонентов, каналов связи, требования надежности должны быть не ниже требований, предъявляемых к разрабатываемой Системе.
8. Для выполнение указанных требований Заказчик предоставляет соответствующие аппаратное и программное обеспечение.
9. На случай полного отказа любого модуля Системы Исполнителем должен быть предоставлен DRP (disaster recover plan).
10. Система может быть развернута на нескольких независимых друг от друга серверах, запросы к которым должны автоматически распределяться с помощью сетевого балансировщика, настроенного на режим active-active. Серверы баз данных так же должны быть настроены в отказоустойчивой конфигурации, в кластерном исполнении. У администраторов системы должна быть возможность, при необходимости, вручную перераспределить нагрузку или снять нагрузку с активной ноды;
11. При внесении изменений в конфигурацию Системы, перед подтверждением действий, Система должна проводить анализ и выдавать предупреждение с указанием, на что повлияет запрашиваемое изменение.

### Требования по безопасности

1. Система должна быть реализована полностью на оборудовании Заказчика, исключающим необходимость использования облачных решений, расположенных вне корпоративных сетей Заказчика.
2. Система должна быть построена на компонентах, исключающих отказ вендора и/или интегратора в их обслуживании в связи с санкционной деятельностью третьих лиц.
3. Специальных требований к безопасности при монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств Системы не предъявляется. Сотрудники Заказчика и Исполнителя должны руководствоваться действующими в соответствующих организациях регламентирующими технику безопасности документами.
4. Должна быть предусмотрена возможность автоматизированного и ручного создания резервных копий: Системы, БД и журналов событий для восстановления в случае возникновения критических ситуаций. Интервал создания резервных копий БД, функциональных компонент и их конфигураций – не реже одного раза в две недели с доступом до 90 дней.
5. Система должна выполнять все требования нормативной документации в области ИБ Заказчика.
6. Система должна обладать возможностью интеграции с глобальным каталогом, роли в системе должны предоставляться через группы пользователей в глобальном каталоге Заказчика - Microsoft AD.

### Требования к эргономике и технической эстетике

1. Система должна быть ориентирована на графическое представление информации.
2. Должен быть единый интуитивно понятный с возможностью выбора каждым пользователем языкаа: русский/английский.
3. Система должна предоставлять возможность подстроиться под задачи каждого пользователя без необходимости программировать (гибкий с drag-and-drop).
4. Должна быть возможность просмотра информации на различных устройствах, Системы и разработанные дашборды/отчеты должны подстраиваться под печатные формы, различные размеры экранов и работать на мобильных устройствах. Наличие мобильных клиентов. работающих на основных операционных системах (Android, iPhone и другие) будет являться преимуществом.
5. Должно быть предусмотрено информирование и обмен данными между пользователями Системы, включая встроенные механизмы информирования об изменениях, например с помощью всплывающих информационных сообщений, как самой Системы, так и разрабатываемых метрик, визуализаций и отчетов (Release notes).
6. Однотипные наименования блоков, полей, кнопок во всех экранных формах Системы должны быть унифицированы.
7. Интерфейс пользователя Системы должен способствовать уменьшению вероятности совершения им случайных ошибочных действий. Недоступный той или иной роли функционал не должен отображаться пользователю с соответствующей ролью.

### Требования к транспортабельности для подвижных АС

Требования отсутствуют.

### Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов ИС

1. Функции Системы должны предоставляться в круглосуточном бесперебойном режиме. Регламентные работы по обслуживанию оборудования и программного обеспечения должны выполняться обслуживающим персоналом согласно режиму работы обслуживающей организации.
2. При проведении регламентных работ в рабочее время пользователи системы должны быть предупреждены путем перенаправления на веб-страницу с указанием факта регламентных работ.
3. В системе должна быть обеспечена возможность, в случае отказа оборудования или ПО, восстановления ее функционирования с резервной копии.
4. Должны поддерживаться режимы полного, инкрементального и дифференциального копирования.
5. Все работы по интеграции и разработке новых метрик, дашбордов, отчетов и других действий по изменению системы должны проводиться на тестовом сегменте - точная копия Системы, которая должна быть развернута в рамках внедрения основной Системы.

### Требования к защите информации от несанкционированного доступа

1. В САИВМ должны быть реализованы следующие основные механизмы защиты информации от несанкционированного доступа:
	1. Модуль САИВМ, выполняющий функции управления, должен поддерживать возможность задания парольной политики для локальных учетных записей с административными правами.
	2. Для информационного обмена между модулями САИВМ должен использоваться протокол защищенной передачи данных.
2. Система должна поддерживать средства идентификации пользователей и многоуровневый доступ к информационным ресурсам Системы, определяемый функциональными обязанностями пользователя.
3. Доступ к информации, хранимой в Системе, должен предоставляться только авторизованным пользователям.
4. Система должна обеспечивать разграничение полномочий пользователей в Системе в соответствии с ролевой моделью.
5. Система должна предоставлять возможность реализовать разграничение доступов для локальных копий приложений отдельно от доступов к приложению.
6. В Системе должна быть возможность предоставления пользователю доступа только к данным от определенных источников на основании назначенных данному пользователю ролей. При формировании поискового запроса не должны выдаваться данные, доступ к которым ограничен ролевой моделью.
7. При формировании некорректного поискового запроса или запроса по индексу/строке данных, к которым у пользователя отсутствует доступ, поисковый запрос не должен запускаться, должна появляться подсказка для корректировки запроса или предупреждение, что доступ ограничен.
8. В Системе должна быть возможность предоставления пользователю доступа только к определенным функциям, дашбордам, отчетам и другим ресурсам Системы, на основании назначенных данному пользователю ролей.
9. В Системе должна быть сконфигурирована ролевая модель доступа ко всем функциям Системы. Настройка полномочий пользователей Системы должна быть выполнена в соответствии с согласованной с Заказчиком, на этапе реализации проекта, матрицей доступа. Роли должны иметь возможность быть выданы путем добавления учетной записи пользователя в группу Microsoft Active Directory.
10. Использование LDAPS совместимой службы каталогов, в том числе Active Directory, в качестве источника списка зарегистрированных пользователей.
11. Возможность работы в режиме Single Sign-On (SSO) по протоколу Windows Native Authentication (Kerberos) и OpenID Connect, что бы не вводить пароль для доступа к системе, если пользователь уже был аутентифицирован в домене.
12. Идентификация пользователя при входе в Систему должна осуществляться на основе уникального имени его учетной записи в Microsoft Active Directory.
13. Аутентификация пользователя при входе в Систему должна осуществляться на основе пароля его учетной записи в Microsoft Active Directory.
14. Авторизация пользователя при входе в Систему должна осуществляться на основе назначенных данному пользователю ролей средствами Системы.
15. Пользователи Системы не должны иметь прав на удаление данных из журнала событий.
16. Защита информации от несанкционированного доступа регулируется внутренними документами Заказника, существующими политиками и разграничением прав доступа, а также настройками стороннего ПО. В процессе реализации проекта нарушение действующей системы защиты от НСД не должно быть нарушено.
17. Система должна предоставлять документированный REST интерфейс для взаимодействия с внешними системами.
18. Система должна быть обеспечена механизмами защиты интеграций через API, включая вызов API key из защищённых хранилищ при подключении к внешним системам и шифрования данных для обеспечения их защиты от несанкционированного доступа при обращении от/к серверу.
19. Требования по безопасности информации, предъявляемые к Системе, распространяются на все ее компоненты: от серверной части до конечных автоматизированных рабочих мест пользователей системы, включая каналы передачи данных.
20. Система должна отвечать действующей у Заказчика политике разграничения доступа, парольной политике и др.
21. Должен быть возможность настроить аудит выданных доступов.
22. Должен быть предусмотрен принудительный выход из Системы при бездействии в течение заданного времени и блокировка доступа на определенный период при превышении допустимого количества неуспешных попыток входа.
23. Дополнительно должны быть реализованы следующие меры:
	1. разграничение доступа на сетевом уровне - сегментирование;
	2. ограничение физического доступа к программно-техническим средствам Системы в соответствии с принятым порядком;
	3. предоставление прав/ролей в соответствии с принятым у Заказчика порядком с проведением соответствующего инструктажа - обучения;
	4. для контроля доступа администраторов и регистрации их действий использование решение класса Privileged Access Management.

### Требования по сохранности информации при авариях

1. В Системе должна быть обеспечена сохранность информации при наступлении следующих событий:
	1. отключение сетевого электропитания;
	2. отказ или авария отдельных модулей САИВМ, сетевого или серверного оборудования;
	3. завершение работы Системы
	4. стихийные бедствия, например: пожар, наводнение, взрыв, землетрясение;
	5. хищение носителей информации, других систем комплекса;
	6. ошибки в программных средствах;
	7. неверные действия сотрудников.
2. Должны быть учтены возможные причины простоя Системы, предусмотрены и описаны в разрабатываемой документации механизмы сохранения работоспособности и обеспечения восстановления своих функций:
	1. Плановые отключения модуля или Системы. Для выполнения профилактических мероприятий, наращивания аппаратного обеспечения, установки пакетов обновлений и других значимых событий.
	2. Отказы программных средств Системы, например ОС и драйверы устройств. Возможность и последствия возникновения данных нарушений должны быть проанализированы для всех функциональных модулей Системы.
	3. Отказы сетевых и аппаратных средств Системы кроме носителей данных. Для минимизации времени простоя Системы по причине отказа аппаратных средств необходимо предусмотреть избыточность и резервирование компонентов аппаратного обеспечения.
	4. Отказы внутренних каналов связи. Для минимизации времени простоя по причине отказа внутренних каналов связи необходимо разработать резервную схему связи.
	5. Вмешательство злоумышленников. Для минимизации времени простоя по причине воздействия со стороны злоумышленников, необходимо разработать защитные и упреждающие мероприятия, позволяющие защитить Систему от известных видов атак.
3. Для выполнения операции отката и повышения надёжности хранения базы данных предусмотреть раздельное хранение двух дополнительных копий.
4. Должна быть обеспечена сохранность информации в Системе при авариях, отказе технических средств, потери питания.

### Требования к защите от влияния внешних воздействий

Требования отсутствуют.

### Требования к патентной чистоте и патентоспособности

1. Проектные, программные и технические решения по созданию Системы должны отвечать требованиям действующего законодательства Российской Федерации об авторском праве и смежных правах по патентной чистоте.
2. При реализации САИВМ должно применяться только лицензионное системное и программное обеспечение.
3. На все приобретаемое ПО должны быть закуплены и зарегистрированы лицензии, по составу и количеству соответствующие количеству пользователей и вычислительной мощности серверного оборудования, в соответствии с лицензионными соглашениями.
4. Права на ПО и Систему должны быть переданы Заказчику, за исключением прав на ПО, предоставление которых регулируется отдельным лицензионным соглашением с правообладателем/разработчиком ПО.

### Требования по стандартизации

1. Система должна использовать стандартные решения, базирующиеся на применении типовых протоколов иов взаимодействия, предусматривающих возможность сопряжения и совместной работы оборудования и программного обеспечения разных производителей, а также для сопряжения с информационными системами других организаций.
2. Все технические решения, используемые в Системе, должны соответствовать требованиям национальных стандартов РФ или международных стандартов, например EEE 754-2008. Технические средства, применяемые в составе САИВМ, должны иметь сертификаты или другие документы Исполнителя, подтверждающие их соответствие техническим условиям.

## Дополнительные требования

Требования отсутствуют.

# СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ ИС

План-график работ должен включать:

**Таблица 3** - График работ

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование этапа | Результат | Срок |
| 1 | Предпроектное обследование | Выполнены работы по сбору информации об инфраструктуре, процессах, системах-источниках.Собраны показатели по производительности. Произведен расчет целевого ресурсного потребления системы. Предоставлены технические требования и требования к инфраструктуре Заказчика.Разработана соответствующая документация на Систему. | до 30 календарных дней |
| 2 | Проектирование | Проработана архитектура решения и проведено техническое проектирование.Подготовлен план-график работ по внедрению системы.Разработаны макеты дашбордов, метрики/KPI.Разработаны модели данных и ТЗ на реализацию дашбордов.Проведено обучение сотрудников Заказчика.Разработано «Техническое задание на разработку и внедрение Системы» | до 45 календарных дней |
| 3 | Внедрение системы | Успешно пройдены предварительные испытания.Разработана документация. | от 90 до 180 календарных дней |
| 4 | Разработка аналитических приложений дашбордов и отчетов | Завершены необходимые интеграции, загрузки и настройки Системы.Перенесены дашборды, реализованные в других Системах, проработаны ТЗ на разработку дополнительных дашбордов в соответствии с п.7.4 ТЗ. | от 30 до 60 календарных дней |
| 5 | Функциональное тестирование | Выполнены работы по валидации данных. Расхождения устранены. | до 45 календарных дней |
| 6 | Опытная эксплуатация Системы | По результатам опытной эксплуатации системы Исполнителем должен быть оформлен протокол, утвержденный Заказчиком, с выводами и рекомендациями по каждому пункту программы.Замечания устранены.Матрица разграничения прав доступа разработана.Завершена разработка дополнительных дашбордов в соответствии с п.7.4 ТЗ. | до 60 календарных дней |
| 7 | ПСИ Системы | ПСИ проводится согласно ПМИ на соответствие требованиям Технического задания, а также включает проверку устранения недостатков, выявленных в ходе опытной эксплуатации Системы.Полный пакет документов разработан Исполнителем и согласован Заказчиком. | от 7 до 30 календарных дней |
| 8 | Перевод в промышленную эксплуатацию | Система, а также документы, дашборды, отчеты, аналитические приложения переданы в эксплуатацию Заказчику. | от 7 до 14 календарных дней |

## Предпроектное обследование

По результатам обследования Исполнителем должны быть направлены Заказчику рекомендаций по дополнительной настройке систем-источников, расчет состава программно-аппаратных компонентов решения с учётом запаса роста, сайзинг на Систему с указанием количества необходимых серверов, их мощностные характеристики, требования к типу и версиям ОС, техническое задание и макеты на разработку аналитических приложений, дашбордов и отчетов, иерархии метрик/KPI для оценки эффективности процессов ИБ.

На данном этапе будут проведены следующие работы:

1. Аудит бизнес-процессов Заказчика. Сбор исходных данных о процессах, процедурах, функциональных обязанностях работников ИБ и системах-источниках для формирования метрик/KPI.
2. Анализ систем-источников: определение и проверка наличия данных, необходимых для сбора информации, а также анализ и формирование рекомендаций по дополнительной настройке систем для подключения их в качестве источника.
3. Уточнение количества/состава разрабатываемых дашбордов/аналитических приложений/отчетов.
4. Разработка Технического проекта Системы;
5. Разработка первой рабочей версии программной части Системы. Итоговыми результатами по первому этапу являются:
	1. Технический проект и первой рабочей версии программной части Системы;
	2. Предоставлен комплекс рабочей документации, в соответствии с разделом 11 ТЗ;
	3. Предоставлено описание API и часто встречаемых и наиболее критичных ошибок Системы как на этапе настройки, так и на этапе сопровождения/эксплуатации. У каждой ошибки/проблемы в перечне должен быть свой ID, описание и рекомендации по устранению;
	4. Согласование дат обучения персонала Заказчика на аккредитованных курсах.

## Проектирование

На данном этапе будут проведены следующие работы:

1. Проработка архитектуры решения и техническое проектирование Системы включая:
	1. уточнение описания каждого функционального модуля;
	2. уточнение требований к программным и аппаратным средствам;
	3. описание требований к интеграции функциональных модулей;
	4. детализацию требований к интеграции с информационными системами и системами-источниками;
	5. детализацию способов и механизмов подключения, извлечения, загрузки данных;
	6. уточнение состава и структуры данных, необходимых для разработки новых и переноса существующих аналитических приложений, дашбордов и отчетов;
	7. согласование с Заказчиком способов обеспечения желаемого уровня отказоустойчивости, надежности, равномерного распределения нагрузки/балансировки и других значимых параметров.
2. Подготовку план-графика работ по внедрению системы и согласование сроков по каждому этапу с Заказчиком.
	1. Проект по созданию Системы должен быть разбит на этапы. Результат выполненных работ на каждом этапе должен полностью соответствовать целям, определенным ТЗ;
	2. При подготовке плана-графика проекта Исполнитель обязан выполнить синхронизацию по срокам с зависимыми проектами и проектами, оказывающими влияние на реализацию данного проекта.

## Внедрение Системы

Все работы выполняются Исполнителем по согласованию с Заказчиком и в присутствии представителей Заказчика.
При необходимости изменения настроек существующих компонентов инфраструктуры и информационных систем Заказчика, такие изменения планируются и прорабатываются Исполнителем, согласуются с Заказчиком, выполняются силами Заказчика.
Заказчик определяет и уведомляет Исполнителя о возможных технологических временных «окнах» для проведения работ, требующих выполнения Исполнителем действий, затрагивающих инфраструктуру Заказчика, находящуюся в промышленной эксплуатации.

На данном этапе будут проведены следующие работы:

1. Подготовка объекта автоматизации к вводу Системы в эксплуатацию.
	1. произвести работы по настройке серверной аппаратной части, включая установку операционной системы и программного обеспечения;
	2. произвести работы по наполнению справочников;
	3. произвести работы по подготовке конфигурационных файлов.
2. Настройку информационных систем и систем-источников по рекомендациям Исполнителя. При необходимости дополнительной настройки систем-источников или внесения изменений в интегрируемые системы для реализации возможности автоматического получения из них необходимого набора данных, настройка выполняется Заказчиком в рамках внедрения Системы на этапе подключения систем-источников под руководством и по рекомендациям Исполнителя. Исполнитель предоставляет Заказчику перечень необходимых изменений и предполагаемые средства реализации на стороне САИВМ.
3. Работы по доработке программной части Системы.
4. Подготовка и согласование с Заказчиком документа «Программа проведения опытно-промышленной эксплуатации» и «Инструкция пользователя системы».
5. Проведение тестирования функциональности и работоспособности всех модулей Системы согласно методике приёмо-сдаточных испытаний.
6. Проведение предварительных испытаний:
	1. Предварительные испытания проводятся с целью определения готовности Системы к вводу в опытную эксплуатацию.
	2. В ходе предварительных испытаний оценивается соответствие Системы требованиям Технического задания и ее работоспособность.
	3. Для проведения предварительных испытаний Исполнителем должна быть подготовлена Программа и методика испытаний, утверждаемая Заказчиком.
	4. Результаты предварительных испытаний должны быть оформлены Исполнителем в виде протоколов предварительных испытаний. По результатам предварительных испытаний Исполнителем должен быть оформлен «Акт ввода системы в опытную эксплуатацию», утвержденный Заказчиком.
	5. В Акте должны быть отражены результаты проведенных проверок по каждому пункту программы, выводы и рекомендации по ним.
7. Доработка Исполнителем в согласованные с Заказчиком сроки функциональности Системы по результатам тестирования и предварительных испытаний в соответствии с требованиями ТЗ.

## Разработка аналитических приложений, дашбордов и отчетов

1. В ходе разработки аналитических приложений, дашбордов и отчетов у Заказчика должна быть возможность вносить изменения и корректировки, но не более 2-х итераций для каждого дашборда.
2. В рамках проекта должно быть перенесено не менее десяти дашбордов/аналитических приложений/отчетов, реализованных в других Системах. Дополнительно должны быть разработаны дополнительные дашборды/аналитические приложения/отчеты по следующим процессам:
**Таблица 4** - Визуализации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование процесса** | **Описание метрики** | **Источники данных** | **Частота измерения (день/неделя/месяц/год)** |
| 1 | Управление источниками SIEM | Время решения заявок | Jira (SSS) | День |
| 2 | Управление источниками SIEM | Размер очереди событий | VolgaBlob Smart Monitor | 5 мин |
| 3 | Услуги по выявлению нарушений политик информационной безопасности в части контроля утечек конфиденциальной информации | Количество инцидентов (утечка/ВНД) | TheHive  | Неделя |
| 4 | Администрирование системы защиты от утечек Конфиденциальной Информации (Решение обращений пользователей на проблемы) | Количество заявок, направленных на ЦЗКИ, в т.ч. по СНИ | Jira (ISD) | Неделя |
| 7 | Процесс разработки и настройки сценариев угроз ИБ | Топ сработок правил корреляции по кол-ву событий с указанием процента FP Technical, TP | TheHive  | 15 мин |
| 8 | Процесс разработки и настройки сценариев угроз ИБ | Среднее время доработки сценариев | Jira (UCM) | 15 мин |
| 9 | Процесс разработки и настройки сценариев угроз ИБ | Процент заявок на доработку, обработанных в срок | Jira (UCM) | 15 мин |
| 10 | Процесс разработки и настройки сценариев угроз ИБ | Добавлено новых идей | Jira (UCM) | 15 мин |
| 11 | Процесс разработки и настройки сценариев угроз ИБ | Правила корреляции без сработок  | VolgaBlob Smart MonitorTheHiveJira | 1 час |
| 12 | Процесс управления правилами корреляции | Количество разработанных правил | Jira (UCM) | 15 мин |
| 13 | Процесс управления правилами корреляции | Среднее время разработки | Jira (UCM) | 15 мин |
| 14 | Процесс управления правилами корреляции | Процент заявок на разработку, обработанных в срок | Jira (UCM) | 15 мин |
| 15 | Процесс управления правилами корреляции | Среднее время настройки | Jira (UCM) | 15 мин |
| 16 | Процесс управления правилами корреляции | Процент заявок на настройку, обработанных в срок | Jira (UCM) | 15 мин |
| 17 | Процесс управления правилами корреляции | Количество всех настроек | Jira (UCM) | 15 мин |
| 18 | Процесс управления правилами корреляции | Среднее время всех настроек | Jira (UCM) | 15 мин |
| 19 | Процесс управления правилами корреляции | Среднее время согласования правила | Jira (UCM) | 15 мин |
| 20 | Процесс управления правилами корреляции | % правил, разработанных с ошибкой оформления | VolgaBlob Smart Monitor | 15 мин |
| 21 | Сбор информации об угрозах ИБ | Среднее время обработки внешних источников угроз | Jira (CTI) | 15 мин |
| 22 | Сбор информации об угрозах ИБ | Количество заявок на обогащение информации по индикаторам | Jira (CTI) | 15 мин |
| 23 | Сбор информации об угрозах ИБ | Среднее время на обогащение информации по индикаторам | Jira (CTI) | 15 мин |
| 24 | Сбор информации об угрозах ИБ | Процент заявок на обогащение информации по индикаторам, обработанных в срок | Jira (CTI) | 15 мин |
| 25 | Сбор информации об угрозах ИБ | Количество внешних заявок | Jira (CTI) | 15 мин |
| 26 | Сбор информации об угрозах ИБ | Среднее время обработки внешних заявок | Jira (CTI) | 15 мин |
| 27 | Сбор информации об угрозах ИБ | Процент внешних заявок, обработанных в срок | Jira (CTI) | 15 мин |
| 28 | Сбор информации об угрозах ИБ | Процент кейсов, закрытых как TP на основании добавленных IoC | TheHive | 15 мин |
| 29 | Сбор информации об угрозах ИБ | Кол-во заявок на добавление IoC | Jira (CTI) | 15 мин |
| 30 | Сбор информации об угрозах ИБ | Среднее время обработки заявок на добавление IoC | Jira (CTI) | 15 мин |
| 31 | Сбор информации об угрозах ИБ | Процент заявок на добавление IoC, обработанных в срок | Jira (CTI) | 15 мин |
| 32 | Моделирование угроз ИБ | Кол-во внесенных изменений в Ландшафт угроз | Jira (CTI) | День |
| 33 | Анализ угроз ИБ | Кол-во разработанных продуктов аналитики | Jira (CTI) | 15 мин |
| 34 | Анализ угроз ИБ | Процент заявок на разработку продуктов аналитики, обработанных в срок | Jira (CTI) | 15 мин |
| 35 | Анализ угроз ИБ | Среднее время разработки продукта аналитики | Jira (CTI) | 15 мин |
| 36 | Анализ угроз ИБ | Количество созданных заявок на разработку/настройку сценариев на основании продуктов аналитики | Jira (UCM) | 15 мин |
| 37 | Управление инцидентами ИБ (Реагирование на инциденты) | Длительность решения инцидента | VolgaBlob Smart Monitor TheHive  | Час |
| 38 | Управление инцидентами ИБ (Реагирование на инциденты) | Время обработки алерта | TheHive  | Час |
| 39 | Управление инцидентами ИБ (Реагирование на инциденты) | Время обработки кейса | TheHive  | Час |
| 40 | Управление инцидентами ИБ (Реагирование на инциденты) | % алертов по которым заведены кейсы с разбивкой по UC | TheHive  | день |
| 41 | Управление инцидентами ИБ (Реагирование на инциденты) | Соотношение инцидентов по их критичности | TheHive  | День/неделя |
| 42 | Управление инцидентами ИБ (Реагирование на инциденты) | % Инцидентов, обработанных с критичной ошибкой | TheHive  | Неделя |
| 43 | Управление инцидентами ИБ (Пост-анализ) | % обработанных алертов/кейсов | TheHive  | День |
| 44 | Автоматизация процессов и процедур ИБ | Количество заявок на автоматизацию с отклонениями | Jira (OUSR) | Месяц/квартал/год |
| 45 | Процесс разработки планов реагирования | Среднее время разработки плана реагирования | Jira (OUSR) | Месяц |
| 46 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение инцидентов по статусу закрытия | TheHive | 15 мин |
| 47 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение событий по критичности | TheHive | 15 мин |
| 48 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение событий по UC | TheHive | 15 мин |
| 49 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение событий по источникам | TheHive | 15 мин |
| 50 | Управление инцидентами ИБ (Реагирование на инциденты) | Наименование инцидента/Топ 10 инцидентов ИБ в работе по времени обработки | TheHive | 15 мин |
| 51 | Управление инцидентами ИБ (Реагирование на инциденты) | Срезовое значение количества закрытых инцидентов ИБ | TheHive | 15 мин |
| 52 | Управление инцидентами ИБ (Реагирование на инциденты) | Конвертированные в инциденты события | TheHive | 15 мин |
| 53 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение событий по статусу | TheHive | 15 мин |
| 54 | Управление инцидентами ИБ (Реагирование на инциденты) | Процент False Positive Technical | TheHive | 15 мин |
| 55 | Управление инцидентами ИБ (Реагирование на инциденты) | Наименование правил корреляции | TheHive | 15 мин |
| 56 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение FP alerts по правилам корреляции | TheHive | 15 мин |
| 57 | Управление инцидентами ИБ (Реагирование на инциденты) | Количество обработанных инцидентов ИБ | TheHive | 15 мин |
| 58 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение True Positive инцидентов ИБ по приоритетам | TheHive | 15 мин |
| 59 | Управление инцидентами ИБ (Реагирование на инциденты) | Количество маркерных инцидентов ИБ | TheHive | 15 мин |
| 60 | Процесс управления правилами корреляции | Эффективность правил корреляции | TheHive | 15 мин |
| 61 | Процесс разработки и настройки сценариев угроз ИБ | Распределение событий по правилу корреляции | TheHive | 15 мин |
| 62 | Процесс разработки и настройки сценариев угроз ИБ | Распределение True Positive инцидентов по правилам корреляции | TheHive | 15 мин |
| 63 | Процесс разработки и настройки сценариев угроз ИБ | Распределение FP technical событий по правилам корреляции | TheHive | 15 мин |
| 64 | Процесс управления правилами корреляции | Среднее время разработки  | Jira (UCM) | 15 мин |
| 65 | Процесс управления правилами корреляции | Время разработки  | Jira (UCM) | 15 мин |
| 66 | Процесс управления правилами корреляции | Количество идей UCM на основании продуктов аналитики TI | Jira (UCM) | 15 мин |
| 67 | Процесс управления правилами корреляции | Время обработки | Jira (UCM) | 15 мин |
| 68 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение инцидентов/событий по исполнителю | TheHive | 15 мин |
| 69 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение инцидентов по статусу пост-анализа | TheHive | 15 мин |
| 70 | Процесс управления правилами корреляции | Процент вовремя закрытых заявок на разработку | Jira (UCM) | 15 мин |
| 71 | Процесс управления правилами корреляции | Среднее время в разработке | Jira (UCM) | 15 мин |
| 72 | Процесс управления правилами корреляции | Среднее время согласования | Jira (UCM) | 15 мин |
| 73 | Процесс управления правилами корреляции | Просроченные заявки на разработку | Jira (UCM) | 15 мин |
| 74 | Процесс управления правилами корреляции | Среднее время настройки сценария | Jira (UCM) | 15 мин |
| 75 | Процесс управления правилами корреляции | Среднее время доработки сценариев | Jira (UCM) | 15 мин |
| 76 | Процесс управления правилами корреляции | Среднее время всех настроек сценариев  | Jira (UCM) | 15 мин |
| 77 | Процесс управления правилами корреляции | Просроченные заявки на настройку | Jira (UCM) | 15 мин |
| 78 | Процесс управления правилами корреляции | Среднее время обработки заявки по сотрудникам | Jira (UCM) | 15 мин |
| 79 | Процесс управления правилами корреляции | Просроченные заявки на доработку | Jira (UCM) | 15 мин |
| 80 | Автоматизация процессов и процедур ИБ | Количество задач в том или ином статусе с распределением по процессам отдела | Jira (OUSR) | 15 мин |
| 81 | Автоматизация процессов и процедур ИБ | Среднее время выполнения задач с распределением по процессам отдела | Jira (OUSR) | 15 мин |
| 82 | Автоматизация процессов и процедур ИБ | Процент задач отправленных на доработку с распределением по процессам отдела | Jira (OUSR) | 15 мин |
| 83 | Автоматизация процессов и процедур ИБ | Процент задач сотрудников с распределением по компонентам | Jira (OUSR) | 15 мин |
| 84 | Автоматизация процессов и процедур ИБ | Просроченные задачи с распределением по процессам отдела | Jira (OUSR) | 15 мин |
| 85 | Автоматизация процессов и процедур ИБ | Количество выполненных целевых задач из числа запланированных за выбранных период | Jira (OUSR) | 15 мин |
| 86 | Автоматизация процессов и процедур ИБ | Количество не закрытых в спринт задач с распределением по компонентам/процессам отдела | Jira (OUSR) | 15 мин |
| 87 | Автоматизация процессов и процедур ИБ | Количество обновленных задач вне спринта за выбранный период | Jira (OUSR) | 15 мин |
| 88 | Автоматизация процессов и процедур ИБ | Среднее время ожидания задач в бэклоге с распределением по процессам отдела | Jira (OUSR) | 15 мин |
| 89 | Автоматизация процессов и процедур ИБ | Количество задач по процессам с распределением по приоритетам | Jira (OUSR) | 15 мин |
| 90 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение событий по правилам корреляции | TheHive | 15 мин |
| 91 | Управление инцидентами ИБ (Реагирование на инциденты) | Количество инцидентов (число/%) за период | TheHive | 15 мин |
| 92 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение инцидентов по критичности | TheHive | 15 мин |
| 93 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение по статусу закрытия | TheHive | 15 мин |
| 94 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение инцидентов/событий по дате | TheHive | 15 мин |
| 94 | Управление инцидентами ИБ (Реагирование на инциденты) | Распределение по источникам | TheHive | 15 мин |

## Опытная эксплуатация Системы

1. Первая версия Системы должна пройти предварительные испытания, состоящие из функционального и нагрузочного тестирования. Должны быть проведены испытания Системы, продолжительностью не менее трех недель, с целью сбора перечня предложений и выявленных недостатков. В результате должен быть представлен протокол испытаний.
2. По итогам предварительных испытаний в Систему должны быть внесены исправления, учитывающие замечания, полученные в ходе предварительных испытаний.
3. Для проверки результата внесенных изменений должны быть проведены повторные предварительные испытания по ранее разработанной программе.
4. Опытная эксплуатация должна проводиться персоналом Заказчика при техническом сопровождении Исполнителя.
5. Опытная эксплуатация возможна при успешном завершении предварительных ПСИ, соответствии Системы требованиям ТЗ и наличии эксплуатационной документации.
6. В период опытной эксплуатации Исполнителем ведется журнал опытной эксплуатации, в котором отмечаются обнаруженные недоработки и проблемы, возникающие в процессе эксплуатации ИС.
7. По результатам опытной эксплуатации Исполнителем должен быть оформлен протокол, утвержденный Заказчиком, с выводами и рекомендациями по каждому пункту программы.
8. В случае наличия отрицательных выводов и заключений по результатам опытной эксплуатации Исполнителем должна быть проведена доработка Системы по указанным в протоколе пунктам в согласованные с Заказчиком сроки.
9. В случае отсутствия отрицательных выводов по результатам опытной эксплуатации Исполнителем должны быть проведены по согласованию с Заказчиком ПСИ.

## Приёмо-сдаточные испытания Системы

1. К моменту проведения финальных ПСИ должен быть подготовлен и согласован с Заказчиком полный пакет документов.
2. ПСИ должны проводиться согласно ПМИ на соответствие требованиям Технического задания, а также включать проверку устранения недостатков, выявленных в ходе опытной эксплуатации Системы.
3. Для проведения ПСИ Заказчиком по инициативе Исполнителя должна быть сформирована приемочная комиссия по передаче Системы в промышленную эксплуатацию, в которую должны быть включены специалисты Заказчика и Исполнителя.
4. По результатам проведения ПСИ Исполнителем должен быть подготовлен «Протокол приёмо-сдаточных испытаний», в случае отсутствия отрицательных выводов, «Акт о вводе системы в промышленную эксплуатацию».
5. Объем, последовательность и этапы, на которых проводятся предварительные или финальные приёмо-сдаточные испытания должны быть согласованы с Заказчиком.

## Перевод Системы в промышленную эксплуатацию

1. Промышленная эксплуатация возможна при успешном завершении финальных ПСИ, соответствии Системы требованиям ТЗ и наличии технической поддержки пользователей.
2. Факт ввода ИС в промышленную эксплуатацию должен быть отражен в соответствующем акте «Акт о вводе системы в промышленную эксплуатацию»
3. «Акт о вводе системы в промышленную эксплуатацию» должен быть подписан уполномоченными представителями Заказчика и Исполнителя.

# ПОРЯДОК РАЗРАБОТКИ ИС

Порядок разработки ИС должен быть уточнен на этапах предпроектного обследования и проектирования.

# ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ИС

## Общие требования к приемке работ:

1. Испытания Системы должны проводиться в соответствии с ГОСТ Р 59792-2021
2. Испытания Системы должны проводиться на основании программы и методики приёмо-сдаточных испытаний. Проведение предварительных испытаний заканчивается оформлением акта о приемке Системы с приложением к нему протокола испытаний.
3. Испытания должны проводиться на полном объеме реальных данных, которые вводятся Заказчиком посредством разработанного в Системеа. В процессе приёмо-сдаточных испытаний должен вестись журнал, в котором будут фиксироваться результаты выполненных работ, замечания по работе программного обеспечения и предложения по изменению работы программного обеспечения.
4. Предварительные испытания и эксплуатация проводятся на инфраструктуре Заказчика.
5. По результатам испытаний возможны доработки и исправления. Выявленные в ПО и документации недостатки Исполнитель исправляет за свой счет в специально оговоренные после проведения испытаний сроки.

# ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ ИС В ДЕЙСТВИЕ

## Требования к подготовительным работам

Требования к условиям должны быть скорректированы на этапе предпроектного обследования.

До момента начала работ по внедрению должны быть обеспечены следующие условия:

* Предоставление Заказчиком серверов под нужды проекта.
* Предоставление удаленного доступа Исполнителю к серверам
* Предоставление Заказчику необходимых дистрибутивов и ключей к ним.
* Создание Исполнителям учетных записей в Active Directory.

## Требования к обучению пользователей Системы

* обеспечить обучение работе с Системой на аккредитованных курсах не менее 5 администраторов Заказчика;
* обеспечить обучение работе с Системой не менее 20 пользователей (в том числе разработчиков аналитических приложений) Заказчика.

# ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

1. В рамках проекта должны быть разработаны и уточнены документы, регламентирующие работу с Системой.
2. Документирование Системы в рамках реализации проекта должно производиться в соответствии с требованиями международных, государственных и, по возможности, корпоративных стандартов Заказчика в части создания корпоративных информационных систем и порядком их описания/разработки.
3. По результатам реализации проекта Исполнитель должен разработать, согласовать и передать Заказчику документы в соответствии с государственными стандартами и требованиями Заказчика в **Таблице 5**.
4. Требования к составу и содержанию документации определяются на этапе формирования «Технического задания на разработку и внедрение Системы».
5. Комплект документации должен быть передан Исполнителем как на бумажных, так и на машинных носителях в службу эксплуатации Заказчика. Допускается разработка документации в ИС на инфраструктуре Заказчика.
6. Основной формат документов на носителях – Microsoft Office 2019 и выше, дополнительно для текстовых документов – формат «Adobe Acrobat Document» – «pdf»;
7. Для графических документов – формат «Файлы MS Visio»- «VSDX» и «VSDM» для исходных файлов на носителях, для печатных форм продублировать в PDF.
8. Все документы должны быть оформлены на русском языке, однако могут содержать записи латинскими буквами, например наименование функциональных модулей, тексты скриптов.
9. Факт передачи документации фиксируется Актом передачи проектной документации.
10. Каждый документ является неотъемлемой частью процедуры передачи Системы на сопровождение. Без передачи всего комплекта документации службе эксплуатации Заказчика проект не может считаться завершенным.

**Таблица 5** - Перечень документации

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование документа | Тип документации | ГОСТ |
| 1. | Техническое задание на разработку и внедрение Системы | Рабочая документация, русский | * ГОСТ Р 59795-2021
 |
| 2 | Регламент эксплуатации Системы | Эксплуатационная документация, русский | * ГОСТ Р 59795-2021
 |
| 3. | Пояснительная записка к техническому проекту (Техническое решение) с детальным описанием реализации Системы на инфраструктуре Заказчика:Общая, логическая, сетевая схемы,Схема функциональной структуры,Структуры баз данных,Логические/физические модели данных. | Технический проект, русский | * ГОСТ 34.321-96
* ГОСТ Р 59795-2021
 |
| 4. | Инструкция администратора Системы | Эксплуатационная документация, русский | * ГОСТ 19.503-79
* ГОСТ 19.504-79
 |
| 5. | DRP (disaster recover plan) | Эксплуатационная документация, русский | * ГОСТ Р ИСО/МЭК 27001-2021
* ГОСТ Р 57580.1-2017
 |
| 6. | Подробное описание API для: выгрузки данных, изменения конфигураций, подключения источников (интеграций), выполнения поисковых запросов, управления сервисами/службами Системы. | Эксплуатационная документация, русский |  |
| 7. | Детальное описание часто встречаемых и наиболее критичных ошибок Системы | Эксплуатационная документация, русский |  |
| 8. | Инструкция разработчика | Эксплуатационная документация, русский | * ГОСТ 19.503-79
* ГОСТ 19.504-79
* ГОСТ Р ИСО/МЭК 24668-2022
* ГОСТ 34.201-2020
* ГОСТ Р 59795-2021
 |
| 9. | Инструкция пользователя Системы | Эксплуатационная документация, русский | * ГОСТ Р ИСО/МЭК 24668-2022
* ГОСТ 34.201-2020
* ГОСТ Р 59795-2021
 |
| 10. | Программа и методика приёмо-сдаточных испытаний | Рабочая документация, русский | * ГОСТ 34.603-92
 |
| 11. | Программа проведения опытно-промышленной эксплуатации | Рабочая документация, русский | * ГОСТ Р 59795-2021
 |
| 12. | ТЗ на реализацию каждого дашборда/аналитического приложения или отчета в Системе с описанием:* набора данных для каждой визуализации,
* моделей данных и интеграций с системами-источниками для каждого дашборда/аналитического приложения или отчета,
* взаимосвязей между метриками/KPI и аналитическими элементами,
* системы группировок и фильтрации,
* периодичность обновления данных,
* общий вид/макет, логика работы dashboard и/или каждой визуализации.
 | Рабочая документация, русский | * ГОСТ Р 59795-2021
 |