«СОГЛАСОВАНО»

Инженер КИПиА

Сыпиков А.

«08» июня 2024 ~~2022~~ года

«УТВЕРЖДАЮ»

ЗАО КГК

Заместитель менеджера ЗСФ

Касымбеков Т. Б

«08» июня 2024 ~~2022~~ года

ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА ПРИОБРЕТЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА (PIMS)

БИШКЕК, 2022

Содержание

СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

Термин	Определение
RPO	Recovery point objective - допустимый объём возможных потерь данных в случае сбоя (инцидента).
RTO	Recovery time objective - допустимое время восстановления информационной системы в случае сбоя (инцидента).
ЦОД	Центр Обработки Данных — это специализированное выделенное помещение для размещения серверного и сетевого оборудования, которое обеспечивает бесперебойную работу IT-Системам компании.
РКД	Резервная Копия Данных – консистентная копия данных на съёмном носителе (жёстком диске, дискете и т. д.), предназначенная для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

1. Общие сведения

1.1. Наименование

Полное наименование – «Техническое задание на приобретения системы управления информацией технологического процесса (PIMS-process information management system)»

1.2. Поставщик и исполнитель

Заказчик работ: ЗАО «Кумтор Голд Компани»

Поставщик программного обеспечения: организация, выбранная Заказчиком для поставки программного обеспечения по данному ТЗ.

2. Основание, назначение и цели проекта

2.1. Основание

Основанием приобретения системы PIMS является необходимость оперативного управления технологическими процессами в режиме реального времени- позволяющая вести оперативный учет данных, планирования и управления ресурсами производства, что позволит повысить эффективность и производительность.

2.1. Назначение и цели системы

Назначениями системы является следующее:

a. Единый источник достоверных данных, которое объединяет важную информацию и повышает возможности персонала для обеспечения безупречной, непрерывной работы предприятия;
b. Своевременно предоставить данные пользователям и смежным системам в необходимом объеме и наиболее подходящем формате;
c. Возможность анализировать сравнивать события;
d. Предоставление всем авторизованным пользователям удобный доступ к данным о состояние фабрики и ключевым элементы;
e. Возможность сжать и архивировать данных без потери полноты и качества;
f. Защита от потерь и искажения при хранении данных;
g. Удобная визуализация исторических трендов и данных в режиме реального времени;
h. Возможность безопасной эксплуатации, путем повышения качества и скорости реагирования в нештатных ситуациях.

3. Требования к PIMS системе

3.1. Требования к функционалу программного обеспечения

1. Возможность выгрузки данных (тегов) с РСУ (Foxboro DCS) посредством OPC сервера;
2. 2000 тэгов для онлайн просмотра и архива;
3. 5 лицензий для одновременной онлайн работы пользователей;
4. 1 лицензия для редактирования пользователей;
5. Генерирование различных отчетов (в формате excel, на электронную почту, на персональные устройства)
6. Приложение для трендов, с возможностью выбора тэгов из базы данных и просмотра, сравнения, хронологии изменений для анализа и поиска неисправности;
7. Возможность системы выдавать истории аварийных событий и сохранения для просмотра;
8. Доступ к системе через веб, для Руководства через мобильные приложения (Chrome, MS Edge, FireFox);
9. Логин контроль - если пользователь вошел в систему и произвел какие-либо изменения, должно быть сохранено и прослежено;
10. Предоставить 5 интерфейс страниц системы (мнемосхемы);
11. Предоставить тренинг для технического персонала для продолжения настройки и редактирования интерфейс страниц;
12. Опция ручного ввода данных.
13. Минимизировать интеграцию, в случае дальнейшего перехода на Foxboro EVO IDE software; обсудить в процессе предварительного согласования с заказчиком.

Тэг, должен содержать следующие данные:

- Название тэга
- Свойства метаданных (технические единицы, описания, ограничения и т.д.)
- Временные метки
- Значения (логические значения, числа с плавающей запятой, целые числа, строки и т.д)

3.2. Нефункциональные требования к программному обеспечению

3.2.1. Расположение данных

Решение системы SaaS / On Premise должно быть развернуто в Центрах обработки данных, арендуемых или приобретенных КГК.

3.2.2. Требования к производительности

№	Параметр	Значение
1.	Количество пользователей, одновременно использующих систему в единицу времени	5-10
2.	Количество пользователей, одновременно редактирующих данные в единицу времени	1-2
3.	Среднее время отклика для операций навигации по экранным формам	500 мс
4.	Среднее время отклика для операций поиска/фильтрации данных	Не должна превышать 30 секунд

3.2.3. Требования к интеграции с существующими системами

Необходима возможность реализовать автоматизированный обмен данными с любых PLC, DCS, SCADA, HMI, LIMS систем для их гарантированной доставки в единое хранилище. Также, необходима поддержка обмена информацией с системами управления верхнего уровня (SAP/R3, Oracle Application, Baan и др.)

3.2.4. Требования к отчетности системы

Должны быть доступны следующие параметры отчетности:

a. Возможность анализа информации и генерации отчетов на базе web для доступа к отчетной информации, ключевым показателям и технологическим данным, посредством современных методов анализа трендов и сбора исторической информации в режиме реального времени.

b. Данные должны формироваться автоматически (по расписанию, по событиям) и в интерактивном (ручном) режиме и обеспечивать выборку информации по заданным параметрам

c. Должна быть опция выгрузки отчетов в Excel, PDF, XML, CSV без ограничения по количеству строк

d. Возможность создания электронного файла-документа с отчетом, вводом документа на печать и возможностью рассылки данного отчета на почту

e. Просмотр сравнительных отчетов (произведя выборку по датам, по состоянию и по другим необходимым фильтрам)

3.2.5. Использование мобильного приложения на IOS Android

Отдается предпочтение архитектурным решениям «тонким клиентским» мобильным приложениям на iOS, Android.

Для использования приложения с «тонким клиентским» на рабочей станции пользователя должны быть установлены только стандартные ПО, не требующие последующего сопровождения.

3.2.6. Модульность прикладного программного обеспечения

Архитектура системы должна строиться из максимально независимых модулей, интегрированных между собой через универсальные интерфейсы (API) и сервисы, реализующие функционал и прием/передачу данных.

3.2.7. Политики пользователя

Система должна предусматривать отображение необходимой информации для каждых ролей авторизованного пользователя по их части. В системе должна иметься возможность настройки прав пользователя по изменению ролей, по правам доступа к определенным сегментам данных.

3.2.8. Дружелюбность и удобство пользовательского интерфейса

Интерфейс системы должен обеспечивать наглядное, интуитивно понятное представление структуры размещенной информации, быстрый и логичный переход к соответствующим разделам системы.

Навигационные элементы интерфейса системы должны обеспечивать однозначное понимание пользователем их смысла и обеспечивать навигацию по всем доступным пользователю разделам системы и отображать соответствующую информацию

Пользовательский интерфейс должен быть дружелюбным и удобным для пользователей. Интерфейс системы должен учитывать контекст использования: где, при каких обстоятельствах, с помощью каких устройств пользователь будет взаимодействовать с системой. Интерфейс должен быть адаптивным, т.е. обеспечивать высокую степень удобства использования не только на широких настольных экранах, но и на портативных (мобильные версии приложения на IOS и Android), планшетных и веб устройствах (Mac OS, Android, Linux, Windows). Интерфейс системы, включая графики и диаграммы, должен адаптироваться под разрешение экрана.

Элементы интерфейса (пункты меню, кнопки, поля ввода в формах, раскрывающиеся списки, и т.д.) должны адаптироваться по размеру под устройство, на котором просматривается система, и под основной сценарий использования данного устройства.

Он также должен иметь подсказки и указатели на функциональные компоненты. Система, предназначенные для обработки данных, должны иметь функции ручной и автоматической обработки данных, например такие как копирование, дублирование, импорт/экспорт в форматах Excel, PDF, XML, CSV. Данные должны выводиться с использованием широких графических и функциональных возможностей, обеспечивающие пользователям функции взаимодействия, мониторинга, анализа и управления производственными процессами. При возникновении ошибки или сбоя, ПО должно выдавать соответствующее информационное сообщение/уведомление, понятное конечному пользователю.

3.2.9. Язык интерфейса и данных

Система должна поддерживать отображении интерфейса на русском и английском языках. При входе в систему она должна выводить опцию выбора подходящего для пользователя языка.

3.2.10. Модуль справочника

Система должна иметь отдельный модуль или режимы для редактирования справочника системы. Модуль/режим редактирования справочников должен быть способным добавлять новые справочники при необходимости без вмешательства или привлечения дополнительной разработки на уровне кода.

3.2.11. Класс системы по времени восстановления и доступности за год

Код шаблона отказоустойчивости	Имя шаблона отказоустойчивости	Описание шаблона	Код класса Системы использующий данный шаблон	Регламентированный % доступности Системы за год (SLA)	Макс. допустимое время простоя Системы за год	*Восстановление в случае локального сбоя системы		*Восстановление в случае падения основного ЦОДа		Количество необходимых комплектов оборудования для обеспечения заявленной отказоустойчивости	
						RTO	RPO	RTO	RPO		
<RC4>	Medium Speed	Системы, недоступность которых влияет на невозможность получения доходов в долгосрочной перспективе, или существенно влияет на эффективность работы большого количества сотрудников компании			BO	99,5%	до 1д 19ч 50м	1-12ч	1-12ч	до 5 дней	До 24 ч	Два комплекта серверов и один СХД в основном ЦОДе

3.2.12. Класс системы по приоритету восстановления

Код класса Системы	Имя класса Системы	Описание классификаторов
BO	Business Operational	Системы, недоступность которых влияет на невозможность получения доходов в долгосрочной перспективе, или существенно влияет на эффективность работы большого количества сотрудников компании КГК. Т.е. это системы, обеспечивающие поддержку различных операций компании КГК. Недоступность этих Систем в течение 1 суток не приводит к существенным финансовым потерям.

3.2.13. Типовой архитектурный шаблон для Medium Speed (RC4) системы

Код шаблона отказоустойчивости	Имя шаблона отказоустойчивости	Описание шаблона	Восстановлениев случае локального сбоя Системы		Восстановление в случаепадения основного ЦОДа	
			RTO	RPO	RTO	RPO
RC4	Medium Speed	Системы, недоступность которых влияет на невозможность получения доходов в долгосрочной перспективе, или существенно влияет на эффективность работы большого количества сотрудников компании	1-12ч	1-12ч	До 5дней	До 24ч

Системы класса RC4 по приоритету восстановления - это Системы **BO (Business Operational)**, а по типу обработки отказов – **HA (High Availability)**.

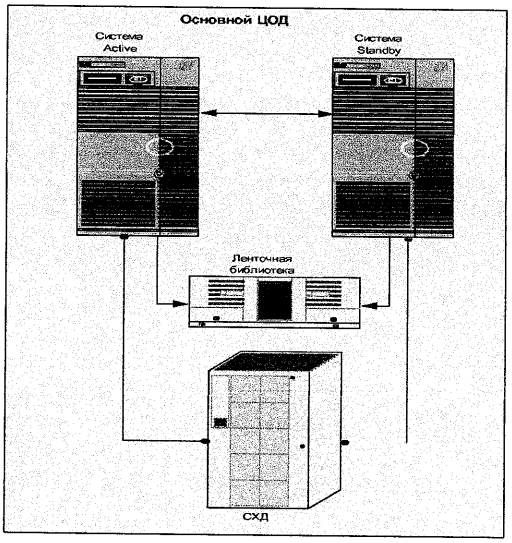
ТЕХНОЛОГИЧЕСКОЕ РЕШЕНИЕ ДЛЯ RC4 IT-СИСТЕМ:

Для защиты данных от потери и логического искажения будет применяться стратегия РКД и восстановления с магнитных лент и/или дисков. При этом необходимо будет еженедельно выполнять полное РКД на магнитную ленту и каждый день проводить инкрементное РКД (а не просто архивировать резервные копии журнала) на магнитную ленту.

Могут применять следующие технологии резервирования данных:

1) РКД по сети LAN или SAN;
2) РКД данных на дисковую память;
3) РКД на магнитные ленты.

Схема восстановления Систем класса RC4 (Medium Speed)



Для Систем класса RC4 должны быть учтены следующие требования:

1) не менее одного раза в неделю следует производить полное РКД, а также не реже одного раза в сутки проводить инкрементальное РКД;

2) РКД следует осуществлять на локальный медиа-сервер в локальной сети;

3) резервный образ должен существовать как минимум в двух экземплярах;

4) необходимо проводить тестирование восстановления данных Систем, согласно утверждённого и подписанного плана тестирования РКД;

5) выделение одного сетевого подключения, используемого для целей РКД для серверов приложений >2 Tb (для физических серверов);

6) возможна использование технологии «кластеризации»;

7) могут использовать подключенные через SAN дисковые накопители 2-3 уровня (более вероятно - внутренние жесткие диски);

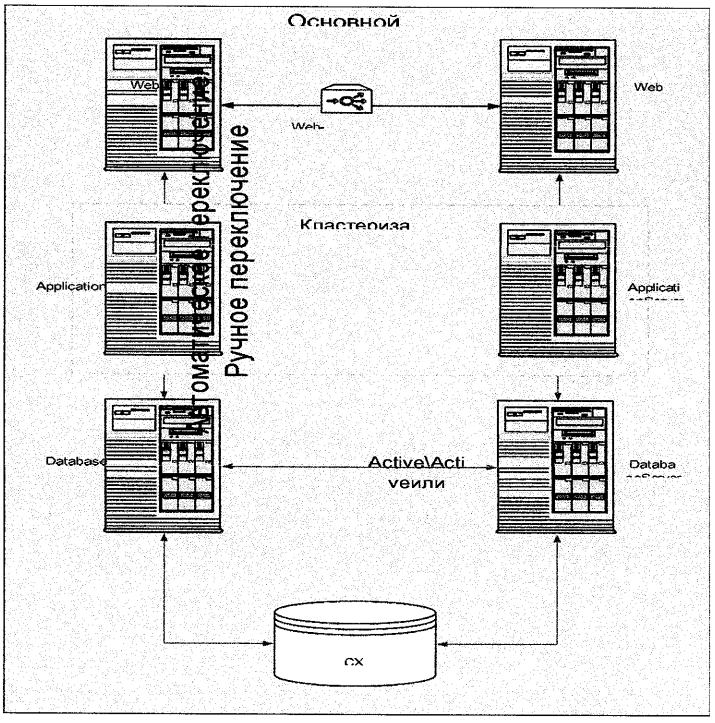
8) серверное и сетевое оборудование находится в пределах одного ЦОДа;

9) обязательное использование Web-балансировщика в схеме НА;

10) необходим действующий контракт(техподдержка) на обслуживание ПО и аппаратных средств со стороны Вендора ПО\оборудования (время реагирования 24 часа или меньше).

Резервирование в пределах основного ЦОДа:

High Availability



3.2.14. Класс Системы по режиму поддержки

Код	Имя	Описание
S11x7	S11x7	IT-Система, сопровождаемая IT в режиме 11 часов в сутки и 7 дней в неделю.

3.2.15. Требования к документации системы

По результатам реализации проекта Исполнитель должен разработать, согласовать и передать Заказчику следующие документы:

- Техническое задание (функциональные и нефункциональные требования с описанием сервисов по интеграции с др. системами)
- Описание наиболее часто использующихся правил обработки внешней корреспонденции - внешней и внутренней (best practice), возможно с применением программно-аппаратного комплекса. Возможный план нормативной части по внешней корреспонденции.
- Спецификация (Состав и описание программы. Сведения о логической структуре и функционировании программы. Техническая архитектура. Описание применения: Сведения о назначении программы, области применения, применяемых методах, классе решаемых задач, ограничениях для применения). Архитектура решения (логическая структура приложения, с разбивкой на модули; функциональная архитектура; структура и схема базы данных; сценарий интеграции приложений; схема развертываний системы в отказоустойчивой архитектуре, в разбивке сред-разработка, тест, препрод, прод).
- Сайзинг на аппаратное обеспечение системы, в разбивке сред (обработка, тест, препрод, прод);
- Программа и методика испытаний (объект испытаний; цель испытаний; требования к программе; требования к программной документации; состав и порядок испытаний с указанием технических и программных средств, используемых во время испытаний, а также порядок проведения испытаний; методы испытаний с указанием результатов проведения испытаний (перечней тестовых примеров)).
- Протоколы тестирования (юнит, интеграционные, производительность, стресс – тесты, на уязвимости).
- Руководство разработчика (Сведения для проверки, обеспечения функционирования и настройки программы, API библиотеки классов и функций с описанием сигнатур, семантики функций).
- Требования к системному администрированию (Установка, обновление версий и т.д)
- Руководство администратора приложения.
- Руководство пользователя.

3.2.16. Требования к ролевой модели системы

В ходе реализации проекта в системе должна быть реализована матрица CRUD (Create, Read, Update, Delete). При имплементации системы роли, действия и доступы будут пересматриваться.

Действие / Роль	Создание справочников, конфигурация бизнес-процессов	Резолюция Утверждение	Исполнение	Контроль	Отчетность
Руководитель		RU	R	R	R
Делопроизводитель			CRU		CRU
Исполнитель			U		R
Контроллер		R	R	RU	R
Администратор	CRU				
Офицер ИБ		CRU			

3.2.17. Требования к информационной безопасности

3.2.17.1. Идентификация и аутентификация

Идентификация и аутентификация субъектов доступа и объектов доступа посредством интеграции с Active Directory.

Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.

Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

Защита обратной связи при вводе аутентификационной информации (Процесс обмена и подтверждения кодов аутентификации, подтверждение авторизации обратной стороной) для внешних контрагентов.

Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа.

3.2.17.2. Управление доступом субъектов доступа к объектам доступа

Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей.

Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.

Управление (фильтрация (ограничение набора данных), маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.

Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).

Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации.

Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы.

Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.

Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки.

Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

Регламентация и контроль использования в информационной системе технологий беспроводного доступа.

Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

Обеспечение доверенной загрузки средств вычислительной техники.

3.2.17.3. Ограничение программной среды

Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения.

Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения.

Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.

Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов.

3.2.17.4. Защита машинных носителей информации

Учет машинных носителей информации.

Управление доступом к машинным носителям информации.

Контроль перемещения машинных носителей информации за пределы контролируемой зоны (в случае надобности).

Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах.

Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации. Контроль ввода (вывода) информации на машинные носители информации.

Контроль подключения машинных носителей информации.

Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания).

3.2.17.5. Регистрация событий безопасности

Определение событий безопасности, подлежащих регистрации, и сроков их хранения.

Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.

Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

Генерирование временных меток и (или) синхронизация системного времени в информационной системе.

Защита информации о событиях безопасности.

Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе.

3.2.17.6. Антивирусная защита

Реализация антивирусной защиты или интеграция с существующими системами защиты.

3.2.17.7. Обнаружение вторжений

При обнаружении вторжений (Dos атаки) сигнализирование и блокировка действий.

Обновление базы решающих правил (при наличии верхнего уровня обнаружения, опционально).

3.2.17.8. Контроль (анализ) защищенности информации

Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей.

Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

Контроль состава технических средств, программного обеспечения и средств защиты информации.

Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

3.2.17.9. Обеспечение целостности информационной системы и информации

Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

Контроль целостности информации, содержащейся в базах данных информационной системы.

Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы.

Ограничение прав пользователей по вводу информации в информационную систему.

Контроль точности, полноты и правильности данных, вводимых в информационную систему.

Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях.

3.2.17.10. Обеспечение доступности информации

Использование отказоустойчивых технических средств.

Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы.

Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

Периодическое резервное копирование информации на резервные машинные носители информации.

Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала.

Кластеризация информационной системы и (или) ее сегментов.

Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации.

3.2.17.11. Защита среды виртуализации

Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.

Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин.

Регистрация событий безопасности в виртуальной инфраструктуре.

Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры.

Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией.

Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

Контроль целостности виртуальной инфраструктуры и ее конфигураций.

Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры.

Реализация и управление антивирусной защитой в виртуальной инфраструктуре.

Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

3.2.17.12. Защита технических средств

Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам.

Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

3.2.11.13. Защита информационной системы, ее средств, систем связи и передачи данных

Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы.

Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом.

Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации).

Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств.

Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами.

Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода.

Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи.

Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации.

Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам.

Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов.

Исключение возможности отрицания пользователем факта отправки информации другому пользователю.

Исключение возможности отрицания пользователем факта получения информации от другого пользователя.

Использование устройств терминального доступа для обработки информации.

Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации.

Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов.

Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы.

Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения.

Изоляция процессов (выполнение программ) в выделенной области памяти.

Защита беспроводных соединений, применяемых в информационной системе.

Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы.

Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы.

Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.

Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды).

Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем.

Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации.

Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы.

Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы.

Защита мобильных технических средств, применяемых в информационной системе.