«СОГЛАСОВАНО»

_____

«_____» _____ 2021 года

«УТВЕРЖДАЮ»

ЗАО КГК

Конищев .И.Н

«17» декабря 2021 года

ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА ПРИОБРЕТЕНИЕ СИСТЕМЫ ПЛАНИРОВАНИЯ ПОДЗЕМНЫХ ГОРНЫХ РАБОТ

БИШКЕК, 2021

Содержание

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Планирование горных работ	Система процессов по определению направлений и последовательности ведения горных работ, носящая цикличных характер, на основе имеющихся и прогнозируемых и периодически актуализируемых горно-геологических, технических и технологических условий, с учетом целевых показателей предприятия в долгосрочной, среднесрочной и краткосрочной перспективах.
Долгосрочное планирование	Планирование горных работ на пять лет и боле с детализацией первого года отработки по кварталам, остальных лет по годам. Цель – формирование стратегии отработки Задачи: определение объемно-качественных показателей, планируемых к добыче полезных ископаемых с выделением в них содержаний полезных компонентов и вредных примесей, формирование порядка ведения вскрышных работ для своевременной подготовки и отработки запасов месторождения, определение стратегических направлений горных работ, определение необходимого количества технико-материальных ценностей, количества оборудования.
Среднесрочное планирование	Планирование горных работ на срок 1 год с разбивкой по месяцам Цель – определение объемно-качественных показателей, планируемых к добыче полезных компонентов, уточнение порядка ведения вскрышных работ для своевременной подготовки и отработки запасов месторождения, определение направлений горных работ по месяцам.
Краткосрочное планирование	Планирование горных работ на Месяц разбивкой по суткам Цель: создание плана горных работ для оперативной деятельности предприятия на последующий месяц. Задачи: определение объемно-качественных показателей, планируемых к добыче полезных компонентов, определение последовательности отработки выемочных единиц.
Система планирования горных работ	Программное обеспечение, регламентирующие документы и унифицированные шаблоны для входных и выходных данных, позволяющие создавать стандартизированные горные планы в требуемые сроки и периоды деятельности предприятия.
Объемно-качественные показатели	Численные показатели к объему, тоннажу и содержанию полезного компонента в горной массе, извлекаемой в процессе проведения горных работ, на основе геологической блочной модели.

Термин	Определение
Сценарий плана горных работ	Совокупность горно-геологических, технических, технологических данных и результатов планирования, отраженных в совокупности файлов определённого программного обеспечения.

СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

Термин	Определение
БВР	Буровзрывные работы
БД	База данных
ГГИС	Горно-геологическая информационная система
ГОК	Горно-обогатительный комбинат
ГРР	Геологоразведочные работы
ИТР	Инженерно-технические работники
ИТ	Информационные технологии
КПЭ	Ключевые показатели эффективности
ПГР	Подземные горные работы
ПК	Персональный компьютер
ПЭ	Промышленная эксплуатация
ПО	Программное обеспечение
САПР	Система автоматизированного проектирования
УК	Управляющая компания
RPO	Recovery point objective - допустимый объём возможных потерь данных в случае сбоя (инцидента).
RTO	Recovery time objective - допустимое время простоя 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.),

Термин	Определение
	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 приобретение системы планирования подземных горных работ».

Условное обозначение – Приобретение системы планирования.

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 приобретения системы планирования

2.1. Основание

Основанием внедрения системы планирования служит запрос от менеджмента компании на развитие информационной прозрачности планирования подземных горных работ, повышение качества принятия стратегических и оперативных решений, работу в едином информационном пространстве, использование единых инструментов, повышение производительности труда ИТР и достоверности результатов горного планирования.

2.2. Назначение

Внедрение единого контура информационной системы для планирования подземных горных работ.

Система планирования горных работ должна:

1. Обеспечивать автоматизацию технологических процессов Компании в части планирования подземных горных работ;
2. Обеспечивать возможность планирования горных работ на различные периоды (пятилетнее, годовое, месячное), на основании геологических блочных моделей, трехмерных моделей проектных горных выработок, ресурсов, привил и ограничений.

2.3. Задачи проекта

Задачи проекта:

1. Непрерывное совершенствование производственных процессов.
2. Повышение профессиональных компетенций сотрудников в рамках использования программных продуктов планирования горных работ.
3. Оптимизация работ горной служб предприятия с целью повышения производительности труда и достоверности принимаемых решений.
4. Снижение влияния «человеческого фактора» за счет автоматизации горно-геологических производственных процессов планирования, проектирования и учета результатов деятельности предприятия.
5. Обеспечить автоматизацию нижеперечисленных процессов планирования подземных работ (на данный момент нет возможности планирования подземных работ из-за отсутствия ПО с необходимым функционалом).

*анализ исходных данных, таких как: геологические модели, каркасы открытых горных работ, каркасы подземных горных работ предыдущих периодов. Используется официальная блочная модель, предоставляемая геологами.
*построение каркасов камер в соответствии с геомеханическими, технологическими и экономическими параметрами, на основании данных консалтинговой компании.
*проектирование вскрывающих и очистных горных выработок.
*определение последовательности строительства выработок и отработки камер, график работ.
*симуляция продвижения горных выработок с их возможной производительностью (сколько метров в сутки или год, за необходимый период времени), для решения тактических задач планирования, например: буровое оборудование для проходки

горизонтальных и вертикальных выработок, также для откатки горной массы погрузочно-доставочные машины из очистных и подготовительных выработок.

6. Повышение качества контроля и анализ ведения горных работ.
7. Повышение точности прогнозирования извлекаемых запасов на всех стадиях разработки месторождения.
8. Снижение вариации между планом и фактом за счет повышения вариативности и качества планирования.
9. Снижение издержек от несвоевременного принятия решений.
10. Своевременная идентификация рисков.
11. Повышение безопасности ведения горных работ.
12. Снижения операционных затрат за счет автоматизации процессов планирования горных работ.
13. Достижение главных стратегических целей компании за счет повышения вариативности и качества долгосрочного планирования.

3. Требования к системе планирования подземных горных работ

1. Разработка долгосрочных, среднесрочных и краткосрочных планов горных работ в контурах проектной отработки с возможностью внесения корректировок
2. Планирование проходческих, очистных и вспомогательных работ (бурение, взрывание)
3. Разработка сценариев планов горных работ на основании блочных геологических моделей и трёхмерных моделей выработок.
4. Производить планирование ресурсным методом с учетом производительности оборудования или комплексов оборудования
5. Производить планирование с учетом целевых показателей качества руды, подаваемой на фабрику
6. Производить планирование с учетом приоритетов, геометрических и логических ограничителей последовательности отработки участков и работы комплексов оборудования.
7. Анализ результатов планирования с использованием 3D мультипликации последовательности отработки, визуализация таблиц, диаграмм, диаграмм Ганта и графиков по результатам планирования, с возможностями настройки их визуализации в интерактивном режиме.

3.1. Требования к функционалу программного обеспечения

Система должна содержать следующие модули:

1. Планирование добычи подземных горных работ с расстановкой оборудования;
2. Планирование подготовительных работ подземных горных работ с расстановкой оборудования;
3. Планирование складов (шихтование) с расстановкой оборудования;
4. Администрирование системы для разграничения прав доступа пользователей.

Перечень требований к функционалу ПО приведен ниже.

1.	Наличие функциональности 3D визуализации объектов планирования (каркасов, выработок, сечений, штреков) и анимации последовательности отработки на основании введенных правил последовательности выработок.
2.	Наличие возможности установить фильтр для выбора штреков и выработок по имени, части имени, z отметке, названию назначенного оборудования, пользовательским атрибутам при 3Д моделировании.
3.	Хранение настроек планировании и результатов работы ПО в виде сценариев.
4.	Использование объёмно качественных характеристик из атрибутов каркасных моделей (удельный вес руды, запасы полезных ископаемых).
5.	Расчет объемно качественных показателей на основании введенных блочных моделей и каркасов: количество руды, содержание полезных компонентов, объём добываемой руды (сечение*длина). Необходим справочник параметров блочных моделей.
6.	Возможность использовать несколько блочных моделей в одном сценарии.
7.	Возможность использование блочных моделей с суб-блокировкой.

8.	Возможность использование блочных моделей с частичным процентом.
9.	Возможность создавать пользовательские вычисления путем составления формульных выражений из обязательных и пользовательских параметров.
10.	Пользовательский интерфейс и справка о ПО на русском и английских языках.
11.	Возможность разработки долгосрочных (стратегический план, life of mine), среднесрочных (год, месяц) и краткосрочных (день, неделя) планов горных работ. Исходные данные: установки блочной модели. Подготовительные работы: Оси выработок, оптимизация каркасов. Установки планирования: установки параметров очистных выработок. Настройка последовательности вспомогательных работ. Принципиальная схема движения материалов. Настройка последовательности отработки. Технология отработки – камерная система разработки (проведение разрезного штрека, отбойка очистной камеры, закладка разрезного штрека и камеры, отработанная панель после закладки). Установка производительности оборудования. Установка вспомогательных операций. Установка календарей работы оборудования. Визуализация плана горных работ.
12.	Планирование проходческих работ. Возможность наименования проходческих выработок и назначения группирующих атрибутов. Возможность настройки направления проходческих работ в выработке (возможность задать направление, последовательность выработок, приоритетность). Возможность назначения последовательности проходки выработок вручную.
13.	Функциональность расчёта объёмно-качественных показателей в проходческой выработке при заранее заданных сечениях разных объемов (сечение*длину=объем, объем*удельный вес= масса).
14.	Функциональность внесения факта проходки выработок (метры проходки, процент выполнения) для определения положения, от которого начинается формирование плана.
15.	Планирование очистных работ (возможность введения последовательности горных работ по камерам и производительности оборудования).
16.	Возможность присваивание имен очистных выработок и назначения группирующих атрибутов (заданный период выработки, направление очистных работ).
17.	Возможность настройки вспомогательных работ: бурение, взрывание, закладочные работы.
18.	Возможность схематичного изображения рудопотоков предприятия по цепочке движения материалов от участков добычи до фабрики.
19.	Возможность настройки мягких приоритетов распределения производительности между выработками.
20.	Возможность добавления добычного и вспомогательного оборудования или комплексов оборудования с параметрами их производительности. Необходим справочник по оборудованию.
21.	Возможность настройки назначения оборудования (основного и вспомогательного) по выработкам как интерактивно в 3D интерфейсе, так и в табличной форме.
22.	Возможность настройки рабочих календарей оборудования.

23.	Функциональность настройки дат и событий, в случае наступления которых изменяются входные промеры планирования.
24.	Функциональность внесения факта выполнения очистных работ (извлеченные тонны, процент выполнения) для определения положения, от которого начинается формирование плана.
25.	Производить планирование ресурсным методом с учетом введенной производительности оборудования или комплексов оборудования.
26.	Планирование шихтования руды с учетом промежуточных складов и поступление руды непосредственно из участков добычи.
27.	Производить планирование с учетом целевых показателей качества руды, подаваемой на фабрику.
28.	Визуализация результатов планирования-3д модель.
29.	Возможность мультипликации в 3D последовательности отработки участков и вспомогательных работ, разработанного календарного плана.
30.	Версионность изменений.

3.2. Нефункциональные требования к программному обеспечению

3.2.1. Требования к производительности

№	Параметр	Значение
1.	Количество пользователей, одновременно работающих с системой в единицу времени	5
2.	Среднее время отклика для операций навигации по экранным формам	<= 8 сек.
3.	Среднее время отклика для операций поиска/фильтрации данных	<= 60 сек.

3.2.2. Требования к интеграции с существующими системами

Необходима возможность реализовать автоматизированный обмен данными (блочная модель, каркасные модели очистных выработок, оси выработок, сечения проходческой выработки на основании стринг файла) с существующими системами через RESTful API.

Необходима возможность реализовать автоматическую загрузку графических результатов планирования: в виде полигональных моделей выработок с идентификаторами периодов, в виде каркасных моделей с идентификаторами периодов, в виде числовых данных в соответствующие блока геологической блочной модели в форматы DXF, DWG, SURPAC, DATAMINE, MICROMINE, VULKAN.

3.2.3. Требования к отчетности системы

Визуализация отчетов по выработке, добыче, результатам планирования за заданный промежуток времени (от 1 часа).

Визуализация графиков по выработке, добыче, результатам планирования, с возможностями настройки форматов графиков (столбчатые диаграммы, штабельные диаграммы, линейные диаграммы, площадные диаграммы).

Визуализация последовательности работ в виде диаграммы Ганта.

3.2.4. 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 загод	*Восстановление в случае локального сбоя системы		*Восстановление в случае падения основного ЦОДа		Количество необходимых комплектов оборудованиядля обеспечения заявленной отказоустойчивости
						RTO	RPO	RTO	RPO	
RC5	Low Speed	Все остальные системы не попадающие под классификацию RC1, RC2, RC3, RC4	OP, TE	99%	до 3д 15ч 40м	до 72 часов	до 24 часов	до 4-х недель	до 24 часов	Один комплект серверов иСХД в основном ЦОДе

3.2.5. Класс системы по приоритету восстановления

Код класса Системы	Имя класса Системы	Описание классификаторов
OP	Office Productivity	Офисные приложения, обеспечивающие эффективную работу персонала компании.

3.2.6. Типовой архитектурный шаблон для Low Speed (RC5) системы

Код шаблона отказоустойчивости	Имя шаблона отказоустойчивости	Описание шаблона	Восстановлениев случае локального сбоя Системы		Восстановление в случаепадения основного ЦОДа	
			RTO	RPO	RTO	RPO
RC5	Low Speed	Все остальные системы, не попадающие под классификацию RC1, RC2, RC3 или RC4	до 72 часов	до 24 часов	до 4-х неделль	до 24 часов

Системы класса RC4 по приоритету восстановления - это Системы OP (Office Productivity) или TE (Test).

Технологическое решение для RC5 IT-Систем:

Может быть использована та же стратегия защиты данных, что и для данных с приоритетом восстановления RC4.

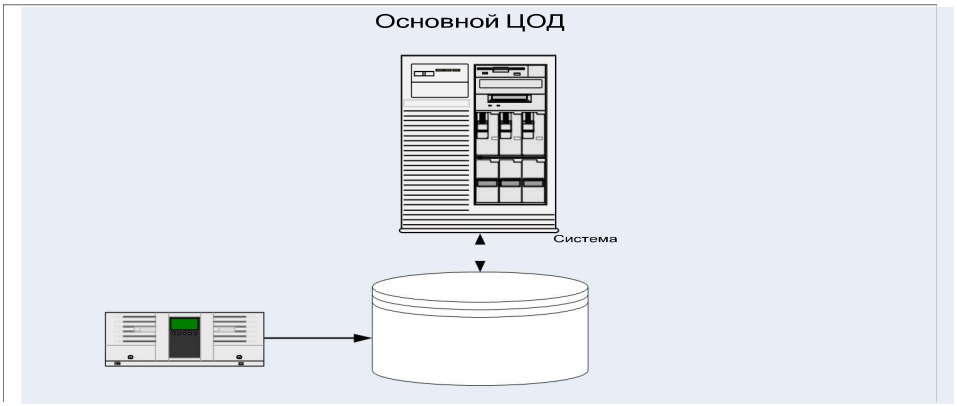
Могут применять следующие технологии резервирования данных:

1. РКД по сети LAN или SAN;
2. РКД на магнитные ленты.

Для Систем класса RC4 должны быть учтены следующие требования:

1. разрешено использовать подключенные через SAN\DAS СХД среднего\начального уровня, а также могут использоваться внутренние диски, собранные в RAID группу;
2. следует выполнять полное РКД на ленту как минимум один раз в неделю;
3. вероятно, приложения не будут кластеризованы;
4. для Систем этого класса резервирование аппаратного обеспечения не используется

Конфигурация без резервирования



3.2.7. 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.

3.2.8. Требования к документации системы

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

- Техническое задание
- 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).
- 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).
- Руководство администратора приложения.
- Руководство пользователя.

3.2.9. Требования к ролевой модели системы

В ходе реализации проекта в системе должна быть реализована матрица CRUD (Create, Read, Update, Delete).

Действие / Роль	Создание справочников пользователей	Управление доступом	Планирование	Отчетность
Планировщик 1			CRU	CRU
Планировщик 2			CR	CR
Администратор	CRU			
Офицер ИБ		CRU		

3.2.10. Требования к информационной безопасности

3.2.10.1. 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.

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.

3.2.10.2. 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, 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.

Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему.

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.

3.2.10.3. 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.

3.2.10.4. Защита машинных носителей информации

Учет машинных носителей информации.

Управление доступом к машинным носителям информации.

Контроль перемещения машинных носителей информации за пределы контролируемой зоны.

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).

3.2.10.5. 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.

3.2.10.6. Антивирусная защита

Реализация антивирусной защиты или интеграция с существующими.

Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

3.2.10.7. Обнаружение вторжений

Обнаружение вторжений.

Обновление базы решающих правил.

3.2.10.8. 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.

3.2.10.9. 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.

3.2.10.10. 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.

3.2.10.11. 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.

3.2.10.12. 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).

3.2.10.13. 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.