

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ПРИОБРЕТЕНИЕ
ITSM СИСТЕМЫ**

БИШКЕК, 2022

Содержание

1.	Общие сведения	7
1.1.	Наименование	7
1.2.	Поставщик и исполнитель	7
2.	Основание, назначение и цели приобретения ITSM системы	8
2.1.	Основание	8
2.1.	Назначение системы	8
2.2.	Цели проекта	8
3.	Требования к ITSM системе	10
3.1.	Функциональные требования	10
3.1.1.	УПРАВЛЕНИЕ ИНЦИДЕНТАМИ	10
3.1.1.1.	Задачи модуля	10
3.1.1.2.	Жизненный цикл инцидентов	11
3.1.1.3.	Необходимые функции	13
3.1.1.4.	Взаимодействие с другими модулями	15
3.1.2.	УПРАВЛЕНИЕ ЗАПРОСАМИ НА ОБСЛУЖИВАНИЕ	15
3.1.2.1.	Задачи модуля	15
3.1.2.2.	Жизненный цикл заявок на обслуживание	15
3.1.2.3.	Необходимые функции	17
3.1.2.4.	Взаимодействие с другими модулями	18
3.1.3.	УПРАВЛЕНИЕ ПРОБЛЕМАМИ	19
3.1.3.1.	Задачи модуля	19
3.1.3.2.	Необходимые функции	19
3.1.3.3.	Взаимодействие с другими модулями	20
3.1.4.	УПРАВЛЕНИЕ ЗНАНИЯМИ	20
3.1.4.1.	Задачи модуля	20
3.1.4.2.	Необходимые функции	21
3.1.4.3.	Взаимодействие с другими модулями	21
3.1.5.	УПРАВЛЕНИЕ СЕРВИСНЫМИ АКТИВАМИ И КОНФИГУРАЦИЯМИ	22
3.1.5.1.	Задачи модуля	22
3.1.5.2.	Необходимые функции	22
3.1.5.3.	Взаимодействие с другими модулями	24

3.1.6.	УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ	24
3.1.6.1.	Задачи.....	24
3.1.6.2.	Необходимые функции.....	24
3.1.6.3.	Взаимодействие с другими модулями.....	26
3.1.7.	УПРАВЛЕНИЕ КАТАЛОГОМ СЕРВИСОВ (УСЛУГ)	26
3.1.7.1.	Необходимые функции.....	26
3.1.8.	УПРАВЛЕНИЕ УРОВНЕМ УСЛУГ	27
3.1.8.1.	Задачи.....	27
3.1.8.2.	Необходимые функции.....	27
3.1.8.3.	Взаимодействие с другими модулями.....	28
3.1.9.	УПРАВЛЕНИЕ СОБЫТИЯМИ.....	28
3.1.9.1.	Задачи.....	28
3.1.9.2.	Необходимые функции.....	28
3.1.9.3.	Взаимодействие с другими модулями.....	29
3.1.10.	УПРАВЛЕНИЕ ЗАДАЧАМИ И НАРЯДАМИ.....	29
3.1.10.1.	Задачи.....	29
3.1.10.2.	Необходимые функции.....	29
3.1.11.	УПРАВЛЕНИЕ ФИНАНСАМИ	30
3.1.11.1.	Задачи.....	30
3.1.11.2.	Необходимые функции.....	30
3.2.	Нефункциональные требования к программному обеспечению.....	30
3.2.1.	Расположение данных	30
3.2.2.	Требования к производительности	30
3.2.3.	Требования к интеграции с существующими системами	31
3.2.4.	Требования к отчетности системы.....	31
3.2.5.	Требования к технологическому стеку.....	31
3.2.5.1.	Использование веб браузеров, «тонких» клиентов, мобильные приложения на iOS, Android	31
3.2.5.2.	Модульность прикладного программного обеспечения	31
3.2.5.3.	Основные компоненты технологического стека приложений.....	32
3.2.5.4.	Среда разработки	32
3.2.5.5.	Технология подключения к базе данных	32
3.2.5.6.	Тестирование приложений.....	32
3.2.5.7.	Требования к протоколам обмена данными при интеграции информационных систем	33

3.2.5.8.	Фреймворки	33
3.2.5.9.	Система контроля версий	33
3.2.5.10.	ETL процессы	33
3.2.5.11.	SDLC процесс	34
3.2.5.12.	Пользовательский интерфейс	35
3.2.5.13.	Язык интерфейса и данных	35
3.2.5.14.	Кеширование и сохранение данных	35
3.2.5.15.	Дружелюбность и удобство пользовательского интерфейса	35
3.2.5.16.	Модуль справочников	36
3.2.6.	Класс системы по времени восстановления и доступности за год	36
3.2.7.	Класс системы по приоритету восстановления	36
3.2.8.	Типовой архитектурный шаблон для Medium Speed (RC4) системы	36
3.2.9.	Класс Системы по режиму поддержки	39
3.2.10.	Требования к документации системы	39
3.2.11.	Требования к ролевой модели системы	39
3.2.12.	Требования к информационной безопасности	40
3.2.12.1.	Идентификация и аутентификация	40
3.2.12.2.	Управление доступом субъектов доступа к объектам доступа	40
3.2.12.3.	Ограничение программной среды	41
3.2.12.4.	Защита машинных носителей информации	41
3.2.12.5.	Регистрация событий безопасности	41
3.2.12.6.	Антивирусная защита	42
3.2.12.7.	Обнаружение вторжений	42
3.2.12.8.	Контроль (анализ) защищенности информации	42
3.2.12.9.	Обеспечение целостности информационной системы и информации	42
3.2.12.10.	Обеспечение доступности информации	43
3.2.12.11.	Защита среды виртуализации	43
3.2.12.12.	Защита технических средств	44
3.2.12.13.	Защита информационной системы, ее средств, систем связи и передачи данных	44

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 ИТ-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.
ITIL	IT Infrastructure Library - библиотека инфраструктуры информационных технологий.
ITSM	IT Service Management, управление ИТ-услугами — подход к управлению и организации ИТ-услуг, направленный на удовлетворение потребностей бизнеса.
Инцидент	Незапланированное прерывание или снижение качества ИТ-услуги.
Запрос на обслуживание	Запрос от пользователя на предоставление чего-либо.
ID	Идентификационный номер
RFC	Requests for Change – запрос на изменение
БЗ	База знаний
KE	Конфигурационная единица
CMDB	Configuration Management Data Base - база данных управления конфигурацией; репозиторий, который содержит необходимую информацию об аппаратных и программных компонентах ИТ-инфраструктуры.
Baseline	Конфигурация, выбранная и закреплённая на любом этапе жизненного цикла разработки как основа для дальнейшей работы.
CAB	Change Advisory Board, Консультативный совет по изменениям, который авторизует изменения и помогает управлению изменениями оценивать и определять приоритеты изменений.
Dashboard	Панель управления, отображающая данные в реальном времени
IVR	Interactive Voice Response - интерактивный голосовой отклик

Термин	Определение

1. Общие сведения

1.1. Наименование

Полное наименование – «Техническое задание на приобретение системы ITSM (IT Service Management, управление ИТ-услугами)».

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 ITSM системы

2.1. Основание

Основанием приобретения ITSM системы является необходимость выстроить эффективную систему контроля работы корпоративных сервисов — от проектирования сервисного подхода к автоматизации бизнес-процессов различных подразделений компании до автоматизации ключевых функций на базе единой платформы, тем самым сокращая затраты на поддержку ИТ инфраструктуры и минимизируя количество используемых ИТ систем.

2.1. Назначение системы

Основным назначением системы являются:

- a. Создание портала самообслуживания, который позволит пользователям самостоятельно решать такие задачи как: создавать запросы на предоставление услуг и сервисов, отслеживать прогресс исполнения заявок, находить решения в Базе знаний.
- b. Автоматизация процесса назначения запросов и инцидентов исполнителю, а также контроль исполнения путем уведомления ответственных лиц;
- c. Контроль за процессом предоставления услуг и всей ИТ-инфраструктурой; информационные панели с данными об инцидентах и запросах в реальном времени.
- d. Эффективное управление процессами для снижения затрат на материальные активы и рабочие ресурсы.
- e. Создание отчетов на основе любой из метрик с представлением информации о прогрессе и результате работы.
- f. Контроль за ИТ-активами (оборудование, ПО) для повышения эффективности их использования, модернизации и развития.
- g. Комплексный подход к оказанию услуг, устранению инцидентов, поддержке пользователей и изменению ИТ-инфраструктуры.
- h. Управление финансовыми процессами ИТ-подразделения: закупками, бюджетом, стоимостью услуг.
- i. Сбор обратной связи от пользователей для улучшения качества обслуживания.
- j. Назначение приоритетов запросам в зависимости от типа запроса, конкретного пользователя или других параметров.
- k. Эскалация запросов и инцидентов, оповещение соответствующих администраторов.
- l. Хранение базы знаний по прошлым запросам, позволяющей специалистам быстро разрешать проблемы, схожие с уже возникавшими.
- m. Снижение рисков за счет внедрения элементов управления процессами, которые отслеживают все связанные действия.

2.2. Цели проекта

Основными целями проекта являются:

- a. Централизованное управление ИТ-инфраструктурой, стратегически сфокусированное на предоставлении услуг и ориентированное на потребителя этих сервисов.
- b. Сокращение времени на обработку запросов и инцидентов пользователей;

с. Предоставление управленческой информации и выработка предложений по улучшению сервисов.

d. Сокращение времени устранения неполадок путем охвата всех самостоятельных организационных подразделений, что позволяет через единую панель получать доступ к нужной информации о заявках, инцидентах, проблемах, изменениях и ресурсах.

е. Повышение уровня обслуживания пользователей путем контроля SLA для созданных услуг.

f. Повысить прозрачность бизнес-процессов различных подразделений компании.

g. Снизить затраты на обработку типовых заявок и инцидентов.

h. Планировать нагрузку для сотрудников различных подразделений компании.

i. Измерять удовлетворенность потребителей услуг.

j. Повысить надежность наиболее важных для бизнеса систем за счет сокращения времени на решение проблемы или устранение инцидента.

k. Сократить продолжительность и количество звонков от пользователей.

l. Повысить продуктивность персонала службы поддержки пользователей.

3. Требования к ITSM системе

3.1. Функциональные требования

В системе должны быть предусмотрены возможности реализации следующих процессов ITIL 4:

Service Strategy

Стратегическое управление ИТ Сервисами (Strategy Management for IT Services)

Взаимодействие с Бизнесом (Business Relationship Management)

Управление портфелем сервисов (Portfolio Management)

Управление финансами ИТ (Financial Management)

Service Design

Управление каталогом сервисов (Catalogue Management, SCM)

Управление уровнем сервиса (Service Level Management, SLM)

Управление мощностью (Capacity Management)

Управление доступностью (Availability Management)

Управление поставщиками (Supplier Management)

Service Transition

Управление изменениями (Change Management)

Управление сервисными активами и конфигурациями (SACM)

Управление знаниями (Knowledge Management)

Service Operation

Управление инцидентами (Incident Management)

Управление проблемами (Problem Management)

Управление событиями (Event Management)

Удовлетворение запросов (Request Fulfillment)

Управление доступом (Access Management)

Continual Service Improvement

Предоставление отчётов о сервисах (Reporting Management)

3.1.1. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

3.1.1.1. Задачи модуля

- a. Построение функциональной структуры службы для дальнейшего автоматического или ручного распределения ответственности специалистов за решением инцидентов и задач / нарядов на работы;
- b. Обеспечение контроля загрузки сотрудников различных линий поддержки и функциональных команд;
- c. Контроль хода выполнения всех обращений;
- d. Отслеживание временных характеристик выполнения всех обращений согласно параметрам качества, определенным на уровне SLA;

- e. Повышение прозрачности всех процессов решения инцидентов посредством гибкого механизма оповещений и эскалации (иерархической и функциональной);
- f. Использование Базы знаний при разрешении обращений пользователей;
- g. Использование CMDB для отслеживания связей между КЕ;
- h. Формирование персонализированной отчетности с целью непрерывного контроля ключевых показателей работы службы поддержки;
- i. Коммуникация с пользователями, в том числе, получение от них обратной связи различными способами: комментарии и переписка по запросам и оценки обслуживания.

3.1.1.2. Жизненный цикл инцидентов

Система должна иметь инструмент для реализации всего жизненного цикла инцидентов (*Приложение 1*).

Выявление инцидентов

- a. Ручной и автоматический режим формирования записей инцидентов;
- b. Записи могут создаваться пользователями ИТ-услуг с помощью портала самообслуживания.
- c. Записи могут создаваться сотрудниками ИТ от имени пользователя.
- d. Источники исходящего запроса через Telegram bot, Чат бот
- e. Автоматическая регистрация обращений, поступающих на электронный адрес службы поддержки;
- f. Регистрация инцидентов по телефону (см. пункт Интеграция);
- g. С помощью настраиваемых web-форм;
- h. Автоматическая регистрация инфраструктурных инцидентов и событий посредством встроенного модуля мониторинга и инвентаризации;
- i. Регистрация обращений из корпоративных порталов, сайтов и внешних бизнес-систем посредством интеграции.

Регистрация инцидентов

Присвоение каждой записи инцидента уникального ID;

Фиксация времени и даты создания записи и ее последующего изменения;

Сохранение в записи полной контактной информации (ФИО инициатора, способ обратной связи);

Фиксация информации об источнике сообщения об инциденте (человек, событие, группа).

Категоризация и приоритезация

Разделение обращений на инциденты и запросы на обслуживание;

Определение категории инцидентов на основе настраиваемого справочника с иерархической структурой;

Приоритезация инцидентов в соответствии с установленными приоритетами в ручном режиме либо преднастроенными условиями;

Автоматический расчет приоритета на основе информации о SLA, типе конфигурационной единицы, вышедшего из строя сервиса, степени нарушения его работоспособности и др.;

Возможность корректирования приоритета в процессе обработки инцидента с фиксацией изменений для последующего аудита и отражения в отчетах;

Возможность изменения типа заявки с инцидента на другой тип заявки (запрос на обслуживание, проблема, запрос на изменение);

Инструменты для службы поддержки и руководства, позволяющие устанавливать порядок обработки инцидентов в соответствии с задачами бизнеса.

Первичная диагностика

Фиксация признаков сбоя и результатов диагностики его причин;

Поддержка применяемых при регистрации инцидентов шаблонов, которые могут включать в себя список необходимых этапов обработки. Они могут быть определены для услуг, SLA, типов конфигурационных единиц и категорий инцидентов;

Автоматическое сравнение записей инцидентов с данными о выявленных проблемах и известных ошибках;

Уведомление пользователей и службы поддержки о появлении уже известных ошибок, которые могут быть связаны с регистрируемым или обрабатываемым инцидентом, на основе информации о его категории, конфигурационной единице или услуге.

Эскалация

Функциональная – на основе определяемых в ручном режиме или преднастроенных условий (целевой показатель уровня услуги и операционного уровня, приоритет бизнеса и степень поддержки);

Иерархическая – на основе преднастроенных (в SLA) и заданных вручную условий, в том числе оповещение подрядчика, ответственного сотрудника, бизнес-заказчика.

Диагностика и исследование

Встроенная система управления конфигурациями CMDB, позволяющая идентифицировать, анализировать и диагностировать инциденты;

Установление и поддержка связи между инцидентом и записью конфигурационной единицы;

Установление и поддержка связи инцидента с одной или несколькими записями о проблемах;

Возможность создания проблемы на основе анализа схожих, ранее зарегистрированных/решенных инцидентов.

Возможность создания запроса на обслуживание из записи инцидента, а также установления связи между ним и запросом на обслуживание;

Возможность открытия запроса на изменение (RFC) из записи инцидента, а также установления причинно-следственных связей между событиями и запросами на изменение.

Разрешение инцидента и восстановление

Назначение ответственных за устранение инцидента исполнителей (группа, отдел или сотрудник);

Хранение информации о статусе инцидента;

Все авторизованные пользователи имеют доступ к данным об инциденте, при этом накладываются ограничения на операции с ключевыми атрибутами (приоритет, статус, место в очереди), которые доступны только сотрудникам техподдержки или иным ответственным лицам;

Введение резолюции с возможностью разграничения к просмотру для ИТ специалистов/пользователей;

Сохранение в истории инцидента полных данных о действиях, произведенных в процессе разрешения и восстановления услуги, и осуществлявших их сотрудниках;

Автоматические массовые операции с записями инцидентов (классификация, создание и объединение записей);

Автоматический контроль и мониторинг времени реакции и разрешения проблемы в соответствии с уровнем услуги и/или приоритетом.

Закрытие инцидента

Фиксация данных о разрешении/закрытии инцидента, включая время и дату;

Оценка удовлетворенности пользователей результатами работ по устранению проблемы.

3.1.1.3. Необходимые функции

1. Использование заранее предустановленных действий объектов, выполняющих по определенным правилам различные операции.
2. Раздельные потоки обработки обычных инцидентов, значительных (Major) и инфраструктурных инцидентов;
3. Построение иерархических структур инцидентов (мастер-инцидент и зависимые инциденты);
4. Возможность поменять тип заявки с «Инцидент» на «Запрос на обслуживание», на «Запрос на изменение», на «Проблему»;
5. Закрытие / повторное открытие инцидента.
6. Назначение одного инцидента на нескольких специалистов ИТ.
7. Возможность создания дополнительных подзапросов - рабочих заданий с назначением на разных сотрудников и возможностью назначить срок исполнения по каждой задаче

8. Назначение/переназначение ответственных.
9. Работа с таймерами SLA (счетчик времени, остановка, запуск, ожидание поставки и т. д.).
10. Установка инцидента в качестве критичного инцидента (Major Incident);
11. Планирование будущих действий. Ввод действий, которые будут осуществляться в определенное время будущего. Напоминания о запланированных задачах.
12. Возможность вывода полного списка действий по инциденту для печати или отправки отчета по электронной почте.
13. Возможность резервирования номера инцидента до его сохранения.
14. Возможность создания связи между событиями, объединение в группы. Любые действия можно в дальнейшем при необходимости применять сразу ко всей группе.
15. Регистрация критических инцидентов и управление ими.
16. Возможность, как часть объединенного управления ИТ сервисами, создания связи с проблемами, RFC, KE, известными ошибками.
17. Подтверждение принятия ИТ события группой специалистов в виде индикации в общем списке инцидентов.
18. Индикация необходимости первоначальной связи с пользователем в общем списке инцидентов.
19. Статистика по обработке инцидентов в режиме реального времени.
20. Использование для решения инцидентов в рамках первой линии поддержки поиска по «похожим инцидентам». Поиск ведется по KE, затронутому пользователю, категории и т. д.
21. Возможность настройки процессов, применимых к инцидентам, для их дальнейшей полной автоматизации.
22. На основе инцидента можно создать сущности: проблему или изменение (процесса, задачи и т. д.).
23. Функция, позволяющая вставлять в качестве значений текст, таблицы, видео и изображения из буфера, в том числе скриншоты экрана.
24. Автоматическое отклонение или подтверждение решения со стороны участника системы с помощью портала самообслуживания или по электронной почте;
25. Коммуникации между сотрудниками различных линий поддержки, а также пользователями.
26. Настройка уведомлений по электронной почте и в личном кабинете по различным параметрам: создание заявок, изменение статуса, назначение заявок и установление сроков исполнения и т.д.
27. Возможность гибкой фильтрации списка всех инцидентов по различным параметрам: статусу, срочности, назначенному сотруднику и т.д.
28. Цветовое подсвечивание заявок по различным параметрам (сроки исполнения, приоритеты, влияние на группы пользователей и т.д.)
29. Мониторинг всего процесса разрешения инцидента по мере прохождения всех стадий.
30. Создание формы инцидента с возможностью определить, какие поля являются обязательными для заполнения.
31. Подсчет трудозатрат решения инцидента, отдельной задачи, сотрудника.

32. При назначении инцидентов руководителем группы должна быть предусмотрена возможность просмотреть текущую загрузку сотрудника по открытым заявкам.
33. Возможность автоматического назначения инцидента на сотрудника в зависимости от типа заявки.
34. Приоритет формируется на основании срочности, предоставляемой пользователем (может быть пересмотрена сотрудником поддержки) и влияния, предоставляемого сотрудником.
35. Система должна отслеживать инциденты с превышением времени разрешения, несоответствия уровня обслуживания, по указанным метрикам, и предоставлять возможность просмотра данных.
36. Контроль времени исполнения заявок.

3.1.1.4. Взаимодействие с другими модулями

Интеграция с инструментами управления заявками на обслуживание;

Интеграция с инструментами управления проблемами;

Интеграция с инструментами управления Базой знаний;

Возможность создать запрос на изменение (RFC) из модуля управления инцидентами;

Интеграция с инструментами управления релизами и развертыванием;

Интеграция с системой управления конфигурациями (CMDB) и управления ИТ активами (IT Asset Management).

3.1.2. УПРАВЛЕНИЕ ЗАПРОСАМИ НА ОБСЛУЖИВАНИЕ

3.1.2.1. Задачи модуля

- a. Сформировать централизованный портал, сфокусированный на предоставлении услуг и ориентированный на потребителя этих сервисов.
- b. Ускорить выполнение запросов на обслуживание.
- c. Оптимизировать затраты на выполнение запросов.
- d. Контролировать и планировать загрузку сотрудников по выполнению запросов на обслуживание.
- e. Обеспечить коммуникации между сотрудниками разных подразделений для сокращения времени работы над выполнением запроса.
- f. Контролировать и документировать ход работ с запросами.
- g. Обеспечить прозрачность выполнения работ над запросом путем возможности мониторинга всего процесса.

3.1.2.2. Жизненный цикл заявок на обслуживание

Система должна иметь инструмент для реализации всего жизненного цикла заявок на обслуживание (*Приложение 2*).

Регистрация заявок на обслуживание

- a. Записи могут создаваться пользователями ИТ-услуг с помощью портала самообслуживания.
- b. Записи могут создаваться сотрудниками ИТ от имени пользователя.
- c. Источники исходящего запроса через Telegram bot, Чат бот
- d. Регистрация заявок по телефону, IVR (см. пункт Интеграция) – «голос в текст» (speech to text);
- e. Автоматическая регистрация обращений, поступающих на электронный адрес службы поддержки;
- f. С помощью настраиваемых web-форм;
- g. Регистрация обращений из корпоративных порталов, сайтов и внешних бизнес-систем посредством интеграции.

Категоризация и приоритезация

Определение категории заявок на основе настраиваемого справочника с иерархической структурой;

Приоритезация заявок в соответствии с установленными приоритетами в ручном режиме либо преднастроенными условиями;

Автоматический расчет приоритета на основе информации о SLA, типе конфигурационной единицы и т.д.;

Возможность корректирования приоритета в процессе обработки заявки с фиксацией изменений для последующего аудита и отражения в отчетах;

Возможность изменения типа заявки с инцидента на другой тип заявки (запрос на обслуживание, проблема, запрос на изменение).

Утверждение заявки на обслуживание

Перенаправление заявки на утверждение автоматически согласно преднастроенным правилам или вручную ответственным сотрудником.

Делегирование полномочий

Перенаправление заявки на утверждение сотруднику, замещающему руководителя, в случае отсутствия руководителя на работе.

Выполнение заявки на обслуживание

Назначение ответственных за выполнением заявки (группа, отдел или сотрудник);

Встроенная система управления конфигурациями CMDB, позволяющая связывать запросы на обслуживание и КЕ.

Возможность создания запроса на обслуживание из записи инцидента, а также установления связи между ним и запросом на обслуживание;

Хранение информации о статусе;

Введение резолюции с возможностью разграничения к просмотру для ИТ специалистов/пользователей;

Сохранение в истории заявки полных данных о действиях, произведенных в процессе выполнения заявки, и осуществлявших их сотрудниках;

Массовые операции с записями (классификация, создание и объединение записей);

Автоматический контроль и мониторинг времени реакции и выполнения в соответствии с уровнем услуги и/или приоритетом.

Закрытие заявки на обслуживание

Фиксация данных о разрешении/закрытии заявки, включая время и дату;

Оценка удовлетворенности пользователей результатами работ по заявке.

3.1.2.3. Необходимые функции

1. Создание записей запросов на обслуживание и хранение детальной информации о запросе;
2. Возможность поменять тип заявки с «Запрос на обслуживание» на «Инцидент», на «Запрос на изменение», на «Проблему»;
3. Возможность для пользователей видеть описание доступных им услуг при создании запроса на обслуживание на портале самообслуживания;
4. Возможность для пользователей видеть/использовать доступные базы знаний при регистрации запроса на обслуживание на портале самообслуживания;
5. Верификация прав доступа пользователя к запрашиваемой услуге;
6. Фиксация даты и времени создания записи запроса на обслуживание и его изменения;
7. Категоризация запросов;
8. Инструмент для проведения согласования и утверждения перед выполнением запроса;
9. Фиксация сведений о срочности, степени влияния и приоритетности в записи запроса, возможность поменять эти атрибуты в ходе выполнения заявки.
10. Функциональная эскалация ответственности за выполнение или согласование запроса на основе преднастроенных или выбранных вручную условий;
11. Иерархическая эскалация ответственности за выполнение или согласование запроса менеджеру или указанной в SLA роли на основе преднастроенных или выбранных вручную условий;
12. Предоставление пользователю детализированной информации о статусе выполнения запроса;
13. Возможность сопоставлять новые запросы на обслуживание с уже существующими;

14. Автоматическая маршрутизация запросов исполнителям: сотрудникам, группам, внешним организациям;
15. Использование шаблонов для наиболее типичных запросов на обслуживание;
16. Возможность создавать правила и процессы для определенных запросов или групп запросов, автоматизирующие их обработку и оповещение заинтересованных сторон;
17. Хранение сведений о категории закрытия запроса;
18. Средства для проведения анализа запросов на обслуживание для выявления тенденций;
19. Средства для проведения опросов об удовлетворенности пользователей;
20. Возможность возобновить обработку ранее закрытого запроса;
21. Автоматическое отклонение или подтверждение решения со стороны участника системы с помощью портала самообслуживания или по электронной почте;
22. Коммуникации между сотрудниками различных линий поддержки, а также пользователями.
23. Настройка уведомлений по электронной почте и в личном кабинете по различным параметрам: создание заявок, изменение статуса, назначение заявок и установление сроков исполнения и т.д.
24. Возможность гибкой фильтрации списка всех заявок по различным параметрам: статусу, срочности, назначенному сотруднику и т.д.
25. Цветовое подсвечивание заявок по различным параметрам (сроки исполнения, приоритеты, влияние на группы пользователей и т.д.)
26. Мониторинг всего процесса по мере прохождения всех стадий.
27. Создание форм заявок на выполнение с возможностью определить, какие поля являются обязательными для заполнения.
28. Подсчет трудозатрат решения заявок, отдельной задачи, сотрудника.
29. При назначении заявки руководителем группы должна быть предусмотрена возможность просмотреть текущую загрузку сотрудника по открытым заявкам.
30. Возможность автоматического назначения заявки на сотрудника в зависимости от типа заявки.
31. Система должна отслеживать заявки с превышением времени разрешения, несоответствия уровня обслуживания, по указанным метрикам, и предоставлять возможность просмотра данных.
32. Контроль времени исполнения заявок.

3.1.2.4. Взаимодействие с другими модулями

Интеграция с инструментами управления инцидентами;

Возможность создать запрос на изменение (RFC) из модуля управления запросами на обслуживание;

Интеграция с инструментами управления релизами и развертыванием;

Интеграция с системой управления конфигурациями;

Интеграция с модулем каталога услуг для поддержки создания пользователем запроса на обслуживание прямо из каталога услуг, а также для создания и поддержки связей между записями о запросах на обслуживание и каталогом услуг;

3.1.3. УПРАВЛЕНИЕ ПРОБЛЕМАМИ

3.1.3.1. Задачи модуля

- a. Своевременное и эффективное определение причин возникших проблем, в том числе на уровне инфраструктуры.
- b. Превентивно выявлять потенциально возможные проблемы и риски, связанные с их появлением.
- c. Оценивать масштаб влияния проблемы на бизнес.
- d. Контролировать и документировать работу с проблемами.
- e. Управлять изменениями, направленными на решение проблем.

3.1.3.2. Необходимые функции

- 1. Создание проблем на основе инцидентов;
- 2. Ведение записей проблем отдельно от записей инцидентов;
- 3. Автоматическое назначение уникального ID при создании записи о проблеме;
- 4. Фиксация даты и времени создания записи о проблеме и ее обновления;
- 5. Фиксация источника сведений о проблеме (события, человека или группы);
- 6. Создание записи о проблеме в ручном режиме;
- 7. Категоризация проблем на основе данных структурированного справочника;
- 8. Приоритезация проблем в соответствии с преднастроенными либо указанными в ручном режиме условиями;
- 9. Автоматический расчет начального приоритета проблемы на основе информации о типе КЕ, затронутой бизнес-услуге, степени выхода услуги из строя, уязвимости с точки зрения безопасности, затрат на решение;
- 10. Возможность изменения приоритета проблемы на основе информации о ее влиянии и/или срочности;
- 11. Возможность настроить автоматическое назначение ответственного (сотрудник, группа, отдел) за решение проблемы в зависимости от категории.
- 12. Хранение информации о статусе проблемы (в процессе диагностики, эскалирована, в процессе разрешения, закрыта);
- 13. Фиксация в записи о проблеме симптомов сбоя, включая параметры события и/или сообщившего о нем пользователя;
- 14. Фиксация сведений о проведенных работах по диагностике проблемы;
- 15. Фиксация сведений о разрешении проблемы, включая дату и время;
- 16. Проведение эскалации и оповещения о находящихся в работе проблемах при достижении порогового значения, например, если корневая причина не установлена в отведенный период времени;
- 17. Возможность создавать записи об известных ошибках, которые становятся доступны для участников смежных процессов;

18. Доступ к архивным данным, информации о проблемах и известных ошибках для использования в рамках диагностики инцидентов и проблем;
19. Категоризация причин закрытия проблемы;
20. Поддержка создания и использования шаблонов для разрешения проблем;
21. Поддержка управления и документирования оценки проблем.
22. Создание изменений на основе проблем.
23. Распределение работ в рамках проблем, декомпозиция проблемы на подзадачи с возможностью назначить разных ответственных и сроки исполнения.

3.1.3.3. Взаимодействие с другими модулями

Установление и поддержка связей между записью о проблеме/известной ошибке и записями инцидентов;

Средства проактивного выявления проблем на основе анализа тенденций инцидентов;

Фиксация обходного решения, найденного в процессе разрешения проблемы, и публикация этой информации в смежные процессы;

Создание записи запроса на изменение на основе записи о проблеме/известной ошибке;

Создание и поддержка связей между записями о проблемах/известных ошибках и записями об изменениях;

Создание связей между записями о проблемах/известных ошибках и записями о конфигурационных единицах;

Интеграция с системой управления конфигурациями, позволяющая идентифицировать, исследовать, диагностировать и устранять проблемы;

Интеграция с базой знаний для поддержки методов исследования, диагностики и анализа корневых причин, а также для создания/обновления обходных решений, временных «заплаток» и решений;

3.1.4. УПРАВЛЕНИЕ ЗНАНИЯМИ

3.1.4.1. Задачи модуля

- a. Организовать создание и сопровождение базы знаний.
- b. Использовать материалы базы знаний в различных процессах управления.
- c. Получать отзывы пользователей о качестве материалов, представленных в базе знаний.
- d. Минимизировать участие сотрудников службы поддержки и предоставлять проактивные механизмы помощи пользователям на различных этапах обработки запросов.

3.1.4.2. Необходимые функции

1. Настраиваемые уровни доступа к материалам базы знаний (БЗ) для пользователей и сотрудников ИТ подразделений;
2. Возможность автоматической проверки при вводе новых данных на соответствие установленным требованиям;
3. Генерация уникального ID для каждой записи/статьи в базе знаний;
4. Возможность размещать в записях БЗ вложенные файлы произвольных форматов (сообщения, электронные документы, таблицы, мультимедиа контент и т.д.);
5. Единый структурированный метод ввода с использованием форм создания новых записей;
6. Создание и поддержание связи между записями БЗ;
7. Автоматическая фиксация в записи базы данных информации об авторе, владельце данных, дате создания и т.д.;
8. Средства выявления избыточной или дублирующей информации в одной или нескольких записях;
9. Средства выявления тенденций в использовании БЗ;
10. Автоматическое оповещение заинтересованных сторон о новых статьях базы знаний/решениях, подходящих для них;
11. Мониторинг частоты обращения к статье БЗ;
12. Поиск данных в записях базы знаний по различным условиям (теме, владельцу, дате, ключевым словам и т.д.);
13. Поиск контента, который хранится в разных форматах;
14. Представление сведений о степени актуальности или важности информации при поиске;
15. Архивирование и удаление устаревшей или нежелательной информации из БЗ;
16. Возможность установления связи с внешними источниками данных, а также импорта данных из внешних источников;
17. Средства создания и поддержки FAQ для клиентов и пользователей;
18. Возможность фиксировать отрезки времени, когда важность записи БЗ повышается для определенного сотрудника или рабочей группы;
19. Средства классификации данных в БЗ;
20. Согласование материалов базы знаний на предмет их включения в общие знания или знания для пользователей;
21. Обсуждение материалов из базы знаний, в том числе пользователями.
22. Возможность отправить статью на утверждение перед публикацией.

3.1.4.3. Взаимодействие с другими модулями

Возможность для персонала, отвечающего за управление инцидентами, создавать записи БЗ;

Возможность для персонала, отвечающего за управление проблемами, создавать записи БЗ;

Быстрое создание записи базы знаний из записи изменения (RFC) и установление связи между записями;

Интеграция с базой данных о конфигурациях (CMDB) для поддержки связей между записями базы знаний и записями о конфигурационных единицах;

3.1.5. УПРАВЛЕНИЕ СЕРВИСНЫМИ АКТИВАМИ И КОНФИГУРАЦИЯМИ

3.1.5.1. Задачи модуля

- a. Вести учет ИТ-активов и конфигурационных единиц, понимать их связи и влияние друг на друга и на услуги.
- b. Распределять ролевую ответственность за сопровождение КЕ, автоматизируя часть процедур связанных процессов.
- c. Отслеживать окончание гарантийных сроков и обязательств по лицензионным соглашениям или контрактам на использование аппаратного обеспечения, программного обеспечения и аппаратно-программного обеспечения.
- d. Сверка с данными финансовой системы (по фактической и остаточной стоимостям) ИТ активов.
- e. Проводить аудит имеющейся ИТ-инфраструктуры (ПО, серверов, сетевых устройств).
- f. Поддерживать в актуальном состоянии базу данных управления конфигурациями.
- g. Документировать все активности, связанные с конфигурационными единицами.
- h. Поддерживать процессы управления проблемами и изменениями благодаря анализу воздействий и тенденций ИТ-активов.
- i. Усиление ИТ-безопасности, благодаря полному контролю над конфигурационными единицами.
- j. Повышение качества финансового планирования, благодаря четкому определению всех активов и их взаимосвязей.
- k. Повышение качества управления лицензиями на использование программного обеспечения

3.1.5.2. Необходимые функции

- 1. Хранение актуальной и точной информация обо всех конфигурационных единицах ИТ-инфраструктуры.
- 2. Хранение информации о КЕ в зависимости от типа (уникальный ID, тип, наименование, описание, версия, расположение, дата поставки, детали лицензирования, владельца, статус);
- 3. Определять взаимосвязи между запросами на изменения, лицензиями на ПО, описаниями ПО, адресами нахождения авторизованного системного ПО.
- 4. Управление имеющимися активами на протяжении всего жизненного цикла каждого ИТ-актива – от момента размещения заявки на него до списания.

5. Добавление различных статусов активов и дополнительных полей формы.
6. Возможность автоматизировать привязку активов к программным лицензиям, контрактам на аренду, обслуживание и поддержку.
7. Отслеживание общей стоимости владения, обратных платежей и износа.
8. Поддержка КЕ. Связь КЕ с определенными контрактами на поддержку, SLA с внешними организациями, поставщиками оборудования.
9. Перемещение КЕ. Ввод и просмотр всех событий, связанных с физическим перемещением, а также любыми другими изменениями конфигурации КЕ в течение ее жизненного цикла.
10. Обзоратель взаимосвязей КЕ– графическое отображение взаимосвязей КЕ. Дает возможность сопоставления анализируемой информации о возможных воздействиях и рисках КЕ, позволяет просматривать КЕ, существующие зависимости КЕ-КЕ, КЕ-сервис.
11. Управление активами. Может быть использовано при объединении отдельных КЕ в группы, просмотра существующих взаимосвязей КЕ, контроля использования единых пользовательских лицензий, печати отчетов о связях отдельных КЕ.
12. Аудит конфигураций. Обеспечивает возможность использования идентификаторов штрих-кодов для идентификации КЕ. Загрузка файлов штрих-кодов и автоматическое создание списка КЕ. Выявление и устранение расхождений.
13. Системы КЕ. Объединяют группы КЕ, например работающие физически совместно или же выполняющие одинаковые функции.
14. Быстрый и гибкий поиск КЕ по необходимым параметрам.
15. Хранение информации о КЕ в зависимости от типа (уникальный ID, тип, наименование, описание, версия, расположение, дата поставки, детали лицензирования, владельца, статус);
16. Добавление статусов активов и дополнительных полей формы.
17. Автоматическая проверка вводимых данных на уникальность и другие условия;
18. Установление связи с другими КЕ при добавлении записи о новой КЕ;
19. Поддержка контроля над программным обеспечением на всех стадиях его жизненного цикла: от проектирования до эксплуатации;
20. Управление и использование baseline (базовые состояния инфраструктуры или КЕ), которые могут быть использованы для возврата к ним;
21. Ведение истории КЕ, включая даты инсталляции, записи об изменениях и местоположениях;
22. Визуализация связей между КЕ в виде карты;
23. Автоматическое определение КЕ, которые могут быть затронуты в случае инцидента, проблемы, известной ошибки или изменения;
24. Автоматическое обновление номера версии КЕ в случае изменения номера версии КЕ, являющейся ее компонентом;
25. Возможность привязки конфигурационной единицы к записям пользователей, использующих КЕ;
26. Контроль количества остатков КЕ для использования;

3.1.5.3. Взаимодействие с другими модулями

Создание и поддержка связей между записями КЕ и записями инцидентов, проблем, запросов на обслуживание, задач/нарядов, проблем и запросов на изменение.

3.1.6. УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ

3.1.6.1. Задачи

- a. Реализовать стандартизированные процессы внедрения изменений, охватывающие весь жизненный цикл запроса на внесение изменения – от планирования, внедрения и до контрольной проверки.
- b. Оценка влияния изменений на бизнес-процессы за счет анализа степени риска и технических последствий изменений.
- c. Увеличение процента эффективности за счет усиления контроля над изменениями.
- d. Сокращение времени, необходимого для осуществления изменений.
- e. Четкий контроль и подробные отчеты о ходе выполнения изменений.
- f. Контролировать все стадии процесса изменения и настройки и тем самым снижать риски, связанные с внедрением изменений.
- g. Оптимизировать процедуру присвоения приоритетности запросам на изменения и за счет этого обеспечить поддержку наиболее важных бизнес-услуг.
- h. Снизить объем звонков в службу поддержки благодаря сведению к минимуму сбоев, связанных с внесением изменений.
- i. Планировать предстоящие изменения, согласовывая с заинтересованными сторонами, контролировать ответственность за внедрение изменений.
- j. Вести учет затрат на подготовку и внедрение изменений.
- k. Анализировать результаты изменений.

3.1.6.2. Необходимые функции

1. Присвоение уникального ID каждой записи запроса на изменение (RFC);
2. Возможность создания изменений на основе проблем и инцидентов;
3. Фиксация даты и времени создания записи запроса на изменение и ее последующего изменения;
4. Мониторинг и отслеживание изменений на протяжении всего их жизненного цикла (от предварительной оценки до закрытия);
5. Разделение изменений на типы и возможность настройки процесса для обработки изменений каждого типа;
6. Категоризация изменений по степени их влияния и приоритету;
7. Документирование хода и результатов процедуры согласования изменений;
8. Возможность отклонения запроса на изменение специальной ролью;
9. Возможность настройки полномочий членов Комитета по изменениям (CAB) в зависимости от их роли;
10. Индикация факта одобрения на проведение изменения;
11. Инструменты для проведения предварительной оценки изменения;

12. Формирование графика изменений с соответствующим контролем доступа, отражающего все утвержденные изменения и уведомления для пользователей и персонала ИТ-подразделений;
13. Формирование графика ожидаемого простоя услуг;
14. Контроль наличия протестированного плана отката или восстановления при утверждении изменения;
15. Напоминания о готовности к проверке завершенных изменений;
16. Фиксация информации об уже проведенных проверках изменений;
17. Фиксация даты закрытия изменений. Возможность указать категорию закрытия;
18. Поддержка создания и использования шаблонов изменений;
19. Поддержка процесса внедрения стандартных изменений;
20. Отображение стандартных изменений в графике изменений;
21. Инструменты для анализа, проработки и планирования предложений об изменениях;
22. Поддержка связи между изменением и его технико-экономическим обоснованием, а также документацией по рискам и требованиям;
23. Возможность указывать влияние изменения (с помощью ссылок на CMDB, SLA или другую информацию);
24. Документирование масштаба изменения услуги;
25. Ручное и автоматическое распределение ответственности на сотрудника или команду;
26. Возможность поделить изменение на этапы;
27. Расчет запланированного и реально потраченного времени;
28. Согласование изменений посредством электронной почты или через портал самообслуживания;
29. Использование сложных согласований для важных изменений.
30. Возможность связать RFC с одним или несколькими инцидентами и проблемами, взаимосвязанными с данным изменением.
31. К RFC могут быть привязаны один или несколько КЕ, на которые будет воздействовать данное изменение.
32. Управление комплексными изменениями. К RFC привязывается процесс, который состоит из последовательности уровней, и они разбиваются на задания. Дополнительно каждый уровень может иметь подпроцессы.
33. Наличие средства для автоматизации процессов выполнения изменений. На разные этапы процесса выполнения изменения могут автоматически назначаться различные сотрудники или группы специалистов.
34. Наличие календаря изменений, который обеспечивает графическим изображением все планируемые и текущие изменения, делает доступным отслеживание возможных конфликтов в результате пересечений стадий внедрения изменений.
35. Возможность создания так называемых «окон обслуживания» – периода времени для какой-либо выбранной системы КЕ, в течение которого возможно проводить изменения для данной системы КЕ. Соответствующий период должен отображаться в календаре изменений. При попытке создания изменения с данной системой КЕ в период времени, не совпадающий с периодом обслуживания, возникает конфликт.

36. Возможность приостановки хода изменений для выбранных систем в заранее введенные сроки (плановые аудиты и т. д.) - «Заморозка изменений».
37. Уведомление об изменениях и их графике службы поддержки пользователей и групп пользователей при помощи электронной почты, веб-портала и т.д;

3.1.6.3. Взаимодействие с другими модулями

Установление и поддержка связей между записями об изменениях и записями инцидентов;

Установление связи между записями о проблемах/известных ошибках и записями об изменениях;

Создание и поддержка связей между записями об изменениях и записями конфигурационных единиц (КЕ);

Инструменты для предварительной оценки и авторизации изменений на основе данных из системы управления конфигурациями (CMDB);

Возможность согласования и планирования работ по релизам и развертыванию с помощью инструментов управления изменениями.

3.1.7. УПРАВЛЕНИЕ КАТАЛОГОМ СЕРВИСОВ (УСЛУГ)

3.1.7.1. Необходимые функции

1. Централизованный контроль всех услуг.
2. Размещение описаний услуг в электронном виде; инструмент для дизайна и реконфигурации услуг;
3. Управление структурой размещаемых данных о сервисах (категории, группы, виды);
4. Назначение уровней предоставления услуги;
5. Хранение информации о текущей стадии жизненного цикла сервиса;
6. Инструментарий для визуализации каталога услуг с учетом зависимостей и связей между ними;
7. Создание настраиваемых шаблонов описания услуг;
8. Разделение сервисного и технического каталогов;
9. Поддержка жизненного цикла услуг, начиная с создания сервиса и до его списания;
10. Назначение в автоматическом режиме заданий ответственным лицам для выполнения запросов на подключение сервисов и их согласование;
11. Организация поиска, облегчающего пользователям формирование заказа;
12. Средства документирования правил доступа к каталогу;
13. Функционал проектирования каталога услуг;
14. Формирование каталога бизнес-услуг;
15. Возможность опубликовать услуги на портале самообслуживания с возможностью ограничения доступов пользователям, группам или подразделениям компании.

3.1.8. УПРАВЛЕНИЕ УРОВНЕМ УСЛУГ

3.1.8.1. Задачи

- a. Создать единый источник информации о всех соглашениях с потребителями услуг и внешними поставщиками.
- b. Управлять уровнем предоставления услуг в рамках соглашений.
- c. Контролировать качество предоставления услуг.
- d. Измерять уровень удовлетворенности пользователей.
- e. Отслеживать сроки действия контрактов по предоставлению услуг с потребителями и внешними подрядчиками.

3.1.8.2. Необходимые функции

- 1. Ведение перечня активных услуг;
- 2. Фиксация согласованных сроков предоставления услуг;
- 3. Учет времени по любым задачам в системе - инциденты, задачи инцидентов, задачи изменений;
- 4. Фиксация целевых показателей уровня услуг;
- 5. Создание записей для каждого требования к уровню услуги;
- 6. Создание записей соглашений об уровне услуги (SLA) и возможность установления связей с требованиями к уровню услуги;
- 7. Детализация содержания SLA, включая дату соглашения, охват, контактную информацию и целевые показатели;
- 8. Детализация соглашений операционного уровня (OLA);
- 9. Детализация договоров с внешними поставщиками;
- 10. Редактирование записей SLA, OLA и хранение истории всех изменений;
- 11. Поддержка мониторинга соглашений операционного уровня и метрик производительности;
- 12. Индикация проведения оценки услуг с заказчиками и подрядчиками;
- 13. Представление списка заключенных и незаключенных SLA, OLA и внешних договоров для любой услуги;
- 14. Мониторинг успешности выполнения соглашений об уровне услуг;
- 15. Мониторинг пороговых значений доступности и производительности услуг по сравнению с определенными в соглашениях об уровне услуг;
- 16. Автоматизированный сбор данных об удовлетворенности пользователей;
- 17. Поддержка создания плана качества обслуживания;
- 18. Возможность организации поддержки и ответственности за услугу;
- 19. Уведомления о нарушениях параметров качества предоставления услуги, настраиваемая эскалация.
- 20. Возможность настроить автоматический процесс для определенного типа услуг.
- 21. Хранение информации о внешних и внутренних поставщиках услуг;
- 22. Хранение информации о заказчиках, включая контактную информацию и местонахождение.

3.1.8.3. Взаимодействие с другими модулями

Поддержка управления портфелем услуг за счет контроля и формирования отчетности по атрибутам услуг и уровням обслуживания, опубликованным в каталоге услуг;

Доступ к информации о соглашениях об уровне услуг, технологических перерывах, периодах запрета на изменения и требованиях к доступности для участников процесса управления изменениями;

Поддержка связей конкретного уровня услуги с персональными записями или записями конфигурационных единиц;

Возможность инициировать действия, связанные с поддержкой услуг при достижении установленных пороговых значений, на основе данных из процесса управления событиями и средств мониторинга;

3.1.9. УПРАВЛЕНИЕ СОБЫТИЯМИ

3.1.9.1. Задачи

- a. Своевременно узнавать о событиях, способных привести к возникновению инцидентов.
- b. Оперативно инициировать активности, направленные на предотвращение инцидентов.
- c. Собирать данные о событиях в разрезе элементов инфраструктуры.
- d. Оценивать влияние событий на качество предоставления услуг.
- e. Использовать гибкие механизмы категоризации событий.

3.1.9.2. Необходимые функции

1. Хранение детализированной информации о событии (ID устройства, тип сбоя, связанные компоненты, дата и время события и пр.);
2. Эскалация оповещений;
3. Конфигурируемые правила и настройки для оповещения отдельных лиц или групп;
4. Фильтрация оповещений о событиях в зависимости от типа события (информирование, предупреждение или сбой);
5. Использование правил и процессов (workflow), обеспечивающих выполнение автоматизированных действий с событиями в зависимости от их типа;
6. Индикация завершенных действий и событий, готовых к закрытию;
7. Приоритезация событий на базе настроенных критериев и правил назначения приоритета;
8. Возможность отслеживать тенденции (рост количества событий в интервале времени и др.);
9. Возможность консолидированного представления всех событий по услуге или системе;

10. Возможность сопоставлять информацию о событиях, полученную из нескольких систем мониторинга;
11. Возможность консолидировать события по разным типам аппаратных средств, платформ, систем мониторинга и др.;
12. Автоматическое выявление и консолидация дублирующих друг друга событий.
13. Проактивные оповещения о наступлении определенных событий с целью предупреждения возникновения инцидентов, в том числе ответственным за элементы инфраструктуры.

3.1.9.3. Взаимодействие с другими модулями

Прямой интерфейс передачи данных из оповещений (alerts) и уведомлений (notifications) в процесс управления инцидентами для регистрации инцидентов;

Автоматическое выполнение действий (отправка сообщения, регистрация инцидента и др.) в качестве реакции на определенные ситуации;

Возможность сопоставления связанных событий, позволяющего выявлять проблемы в проактивном режиме;

Автоматическое создание связей между событиями и записями о конфигурационных единицах в CMDB;

Возможность обработки событий и оповещений с использованием данных о бизнес-процессах, требованиях к уровню услуг, наличии аналогичных и множественных событий с конфигурационной единицей или услугой;

3.1.10. УПРАВЛЕНИЕ ЗАДАЧАМИ И НАРЯДАМИ

3.1.10.1. Задачи

Управление единичных работ сотрудников различных подразделений для применения в рамках управления инцидентами, управления изменениями и ряда других процессов.

3.1.10.2. Необходимые функции

1. Возможность создавать задачи и наряды в рамках процессов и за их границами;
2. Планирование персональных или общекомандных активностей сотрудникам, подразделениям и руководителям;
3. Контроль исполнительской дисциплины;
4. Распределение задач между исполнителями и контроль уровня их загрузки;
5. Учет фактических трудозатрат;
6. Преднастройка шаблонов задач / нарядов на работы;
7. Возможность автоматического распределения ответственности за задачи / наряды между сотрудниками;
8. Автоматическое или ручное создание задач / нарядов из инцидентов, запросов на обслуживание, запросов на изменение, проблем с фиксацией информации об иницилирующем объекте;

9. Автоматическое изменение параметров связанных объектов (запросы, инциденты, другие задачи / наряды и т.д.) при выполнении / невыполнении задач / нарядов.

3.1.11. УПРАВЛЕНИЕ ФИНАНСАМИ

3.1.11.1. Задачи

- a. Учет и контроль финансовой составляющей предоставления и поддержки услуг (фактическая совокупная стоимость владения ИТ услуг и ИТ активов).
- b. Бюджетирование и оценка стоимости новых разрабатываемых услуг (планируемая совокупная стоимость владения ИТ услуг и ИТ активов)
- c. Формирование ИТ-бюджета на основе детализации статей затрат по различным направлениям и накопленной базы стоимости составляющих этих статей.
- d. Интеграция с финансовой системой КГК для сверки плановой, фактической и остаточной стоимостей ИТ услуг и ИТ активов.

3.1.11.2. Необходимые функции

1. Учет стоимости выполняемых по инцидентам и запросам на обслуживание задач / нарядов;
2. Контроль бухгалтерской составляющей используемых активов и ее использование для расчетов итоговых стоимостей услуг;
3. Учет стоимости КЕ;
4. Учет расходов, связанных с предоставлением услуги;

3.2. Нефункциональные требования к программному обеспечению

3.2.1. Расположение данных

Решение может быть On-Premise или Private Cloud и должно быть развернуто в Центрах Обработки данных, арендуемых или приобретенных КГК.

3.2.2. Требования к производительности

Система должна быть способной обрабатывать функции и запросы от пользователей, подключенных и работающих в системе одновременно (100 пользователей). При этом должен работать принцип FI/LO (First In/Last Out).

Время отклика серверного приложения на средний запрос клиентского приложения не должно превышать 500 мс. Транзакционная обработка при сохранении данных должна быть независимой от процесса блокировки таблиц данных по приоритетам. Одновременное редактирование одних и тех же данных разными пользователями не должно допускаться.

Клиентское приложение должно передавать данные к серверу по каждой микрооперации во избежание обработки больших данных. Тайм аут обработки запроса не должен превышать 30 секунд.

3.2.3. Требования к интеграции с существующими системами

Интеграция с телефонной системой Cisco Unified Communications Manager (System version: 12.5.1.11900-146).

Интеграция с ERP и системой электронного документооборота (в т.ч. автоматическое создание заявок из СЭД в ITSM) будет реализована на следующем этапе внедрения.

3.2.4. Требования к отчетности системы

Должны быть доступны основные отчеты, отслеживающие такие параметры как:

- a. Среднее время разрешения по сотруднику или подразделению
- b. Количество заявок с превышением времени разрешения
- c. Общее количество закрытых заявок за определенный период времени
- d. Количество заявок с разбивкой по дням\бизнес-услугам\уровням поддержки и
- e. Формирование инвентаризационных отчетов ИТ активов для проведения аудита
- f. Отчет, показывающий неавторизованные добавления ИТ-активов к инфраструктуре
- g. Преднастроенные отчеты по ключевым показателям эффективности SLA
- h. Создание информационных панелей (dashboards), показывающих данные по метрикам услуг и процессов в режиме реального времени

Должна быть опция для загрузки отчетов в Excel, PDF без ограничения по количеству строк.

Возможность создавать кастомизированные отчеты по любым параметрам и атрибутам.

Возможность отправлять отчеты по электронной почте в заданное время.

3.2.5. Требования к технологическому стеку

3.2.5.1. Использование веб браузеров, «тонких» клиентов, мобильные приложения на iOS, Android

Отдаётся предпочтение архитектурным решениям с «тонким клиентом», веб браузерам, мобильным приложениям на iOS, Android.

Для использования приложения с «тонким клиентом» на рабочей станции пользователя должно быть установлено только стандартное ПО, не требующее последующего сопровождения.

Установка изменений осуществляется только на серверной части информационной системы, не требуя множественных изменений на рабочих станциях, мобильных приложениях.

Устойчивость приложения к неоднородности конфигураций рабочих станций, мобильных приложений.

Минимальные требования к мощности рабочих станций, мобильных приложений.

3.2.5.2. 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.

Микросервисная архитектура в сочетании с SOA (Service Oriented Architecture) наиболее полно обеспечивает слабосвязанность информационной среды.

3.2.5.3. Основные компоненты технологического стека приложений

- Язык программирования
- Среда разработки
- Технология подключения к базе данных
- Методика и инструменты тестирования приложений
- Система управления базой данных (СУБД)
- Операционные системы
- Фреймворки
- HTTP сервер
- Система контроля версий

3.2.5.4. Среда разработки

Рекомендуются следующие среды разработки приложений:

- (Java) IntelliJ IDEA ,
- Vim
- Android Studio
- (Python) PyCharm CE, Jupiter Lab
- VS Code
- Visual Studio
- XCode

Для разработки приложений на языках Java можно использовать среду разработки IntelliJ IDEA. Эта универсальная интегрированная среда разработки приложений, которая предоставляет все средства, необходимые для создания профессиональных десктоп приложений, корпоративных, мобильных и веб-приложений на платформе Java. В зависимости от задач и выбранного языка можно использовать другие инструменты как VS или Vim.

3.2.5.5. Технология подключения к базе данных

Для подключения к системе базе данных из Java приложения можно применить технологию и спецификацию Hibernate / JPA, как одну из самых признанных методов работы с БД. Данная спецификация работает для обеих версий Java EE и Java SE. Она описывает систему управления сохранением java объектов в таблицы реляционных баз данных в удобном виде.

Данная спецификация не ограничивает методы подключения к БД из Java, есть и другие технологии/драйвера для различных баз данных. Поэтому в зависимости от задач и БД могут использоваться и другие методы.

3.2.5.6. Тестирование приложений

Каждое приложение должно проходить тщательное тестирование после разработки по процессу SDLC. Методы и инструменты тестирования ПО достаточно много. Более общепризнанными из них для веб приложений являются следующие:

- Selenium,
- JSFUnit,
- JUnit,

- TestNG

3.2.5.7. Требования к протоколам обмена данными при интеграции информационных систем

Платформа должна поддерживать информационный обмен данными посредством API (например, использование микросервисов на Java SpringBoot).

Интеграционная технология должна поддерживать один из следующих протоколов передачи данных: JSON (RPC), gRPC, XML (RPC), HTTPS, batch import, SQL

В качестве технологии и стандартов обмена данными должна быть поддержка технологий RESTful API и SOAP.

3.2.5.8. Фреймворки

В зависимости от задач к разработке могут применяться ниже перечисленные фреймворки. Кроме перечисленных могут применяться и другие фреймворки в зависимости от задачи, которые предназначены для веб и мобильных решений.

- Spring Framework
- PrimeFaces
- Blade
- Dropwizard
- Google Web Toolkit (GWT)
- JavaServer Faces (JSF)
- JHipster
- Spark Framework
- MyBatis
- Play Framework
- (JavaScript) React.js, Vue.js, Node.js

3.2.5.9. Система контроля версий

Каждое разработанное ПО должно иметь репозиторий и контроль версий. Каждое приложение должно быть заблокировано от изменения перед началом разработки и должно быть разблокировано после внедрения приложения в прод среду согласно SDLC процессу.

Рекомендуемые системы контроля версий:

- GITHUB
- GitLab

3.2.5.10. ETL процессы

ETL (Extract, Transfer and Load) - относится к процессу извлечения, преобразования и загрузки. Это своего рода этап интеграции данных, когда данные, поступающие из разных источников, извлекаются и отправляются в хранилища данных. Данные, извлеченные из различных ресурсов, сначала преобразуются, чтобы преобразовать их в определенный формат в соответствии с требованиями бизнеса.

Для построения ETL процесса могут применяться различные методы и инструменты в зависимости от задач к отчетам и данным. Для интеграции и построения ETL на уровне микросервисов должны применяться следующие технологии и стандарты:

- Брокер сообщений Apache Kafka
- Контейнеризация: технология Containerized от решения Kubernetes, технология с открытым кодом - Red Hat OpenShift
- Поддержка DataOps и DevOps, что обеспечивает взаимодействия внутри команд и отделов по развертыванию изменений
- Технология и протоколы передачи – HTML, XML, JSON, SOAP, REST, API

А также может быть применен подход ELT – сначала извлечение данных, затем загрузка и затем преобразование. Данный подход лучше подходит для обработки машинных данных.

3.2.5.11. SDLC процесс

Все разработки и изменения в ПО, независимо от того, что изменение касается клиентской или серверной части, должны проходить весь жизненный цикл разработки – SDLC (System Development Life Cycle).

Описание этапов процесса жизненного цикла стандартного SDLC процесса:

1. Требование и архитектура. Прежде чем начинать проектировать дизайн необходимо согласовать и утвердить требования (функциональные и нефункциональные). На основе нефункционального требования требуется разработать архитектуру ПО (клиентская платформа, серверная платформа, протокол передачи данных и т.д.).
2. На фазе дизайна необходимо спроектировать и документировать все планируемые компоненты приложения: пользовательский интерфейс (UI), программный интерфейс (требования к фронтенд и бэкенд разработке), структура и модель данных (СУБД)
3. Разработка – непосредственная разработка приложения. Прежде чем начать разработку необходимо заблокировать версию приложения в системе контроля версий (VC). В процессе разработки могут быть уточнения и изменения в документы предыдущих фаз. Необходимо достичь минимум изменений и возвращения в предыдущие фазы.
4. В фазе модульного тестирования разработчик должен проводить тест помодульно всех затронутых частей ПО. Можно применять автоматизированные инструменты.
5. На этапе автотестирования автотестирующи должны протестировать весь затронутый модуль на функциональность и производительность.
6. На этапе приемочного тестирования требуется развертывать ПО в Пре Прод среду и проводить тестирование пользователями согласно требованиям к задаче.
7. На фазе развертывания в прод версию, все оттестированные версии разработки должны переходить в Прод среду. При этом важно соблюдать, чтобы версии приемочного тестирования и развертывания в прод среду совпадали на 100%. Для интеграционных разработок развертывание может быть автоматизировано через DevOps и CI/CD pipeline технологию. После

развертывания в прод среду все изменения должны сохраниться в системе контроля версий и разблокироваться для будущих изменений.

3.2.5.12. Пользовательский интерфейс

Система должна иметь пользовательский интерфейс на тонком клиенте / веб браузер, адаптивный дизайн веб интерфейса под смартфоны и планшеты. Требование к наличию мобильной версии приложения на iOS, Android будет определяться для каждой задачи индивидуально.

Клиентское приложение должно быть доступно через веб и мобильные приложения по протоколу HTTPS.

3.2.5.13. Язык интерфейса и данных

Приложение должно иметь опцию выбора языка, на котором необходимо отображать интерфейс для конечного пользователя. Английский и Русский языки обязательно должны присутствовать для выбора. Кроме этого, система должна поддерживать региональные установки Россия, Кыргызстан для обработки дат и чисел.

Пользовательский интерфейс должен отображать данные в юникоде, т.е. независимо от языка (кодировки – ANSI, Latin) данных.

3.2.5.14. Кеширование и сохранение данных

По технологии хранения и обработки данных клиентское приложение должно иметь возможность локального кеширования и обработки данных. При возникновении сбоя на стороне сервера или недоступности сервера, клиентское приложение должно иметь возможность локально завершить обработку данных текущей функции и хранить данные до полного возобновления работоспособности системы.

3.2.5.15. Дружелюбность и удобство пользовательского интерфейса

Пользовательский интерфейс должен быть дружелюбным и удобным для пользователей. Программа должна иметь подсказки и указатели на функциональные компоненты приложения. Приложения, предназначенные для обработки больших данных, должны иметь функции автоматической обработки данных, например такие как копирование, дублирование, импорт/экспорт из Excel файла, ввод и утверждение одинаковых данных на множество линий и т.д. При возникновении ошибки или сбоя, ПО должно выдавать соответствующее информационное сообщение/уведомление, понятное конечному пользователю.

На главной странице клиентского ПО должны быть доступны ссылки/команды перехода на последние или самые активные за последнее время приложения. Должен быть отображен список документов или транзакций в виде гиперссылки, требующих внимания пользователя, при нажатии которых пользователь должен попасть на необходимое приложение для обработки.

Должна быть функция авто сохранения при вводе несколько этапных и больших данных в процессе работы незавершенной функции. У пользователя должна быть возможность продолжить процесс с того места, которое было сохранено в последний раз.

3.2.5.16. Модуль справочников

При разработке приложения необходимо предусмотреть отдельный модуль или режимы для редактирования справочников системы. Модуль/режим редактирования справочников должен быть способным добавлять новые справочники при необходимости без вмешательства или привлечения дополнительной разработки на уровне кода.

3.2.6. Класс системы по времени восстановления и доступности за год

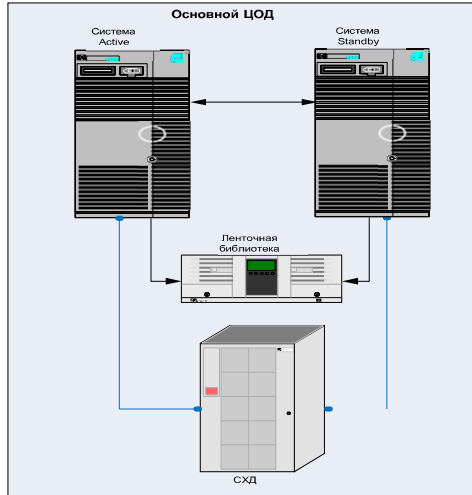
Код шаблона отказоустойчивости	Имя шаблона отказоустойчивости	Описание шаблона	Код класса Системы исполняющий функции шаблона	Регламентированный % доступности Системы за год (SLA)	Макс. допустимое время простоя Системы за год	*Восстановление в случае локального сбоя системы		*Восстановление в случае падения основного ЦОДа		Количество необходимых комплектов оборудования для обеспечения заявленной отказоустойчивости
						RT О	RP О	RT О	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

3.2.7. 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.

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

Код шаблона отказоустойчивости	Имя шаблона отказоустойчивости	Описание шаблона	Восстановление в случае локального сбоя Системы		Восстановление в случае падения 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.

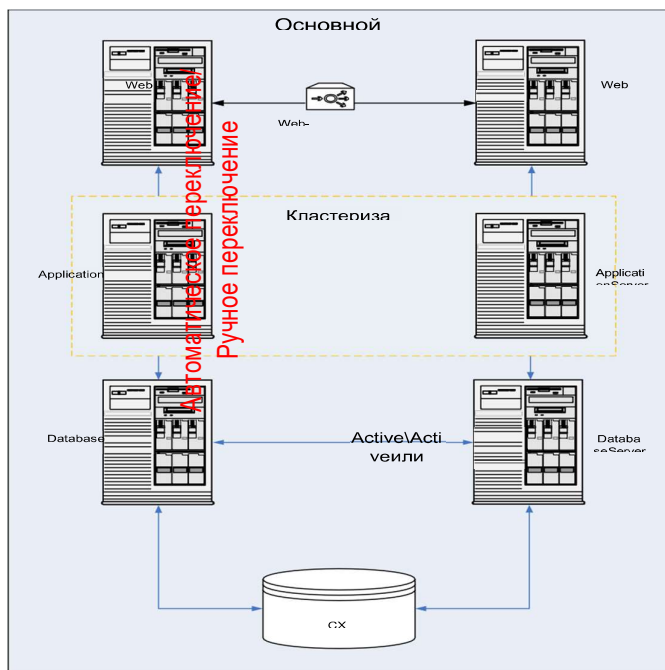
Схема восстановления Систем класса RC4 (Medium Speed

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 HA;
- 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



3.2.9. 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.

3.2.10. 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).
- Спецификация (Состав и описание программы. Сведения о логической структуре и функционировании программы. 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; сценарии интеграции приложений; схема развертывания системы в отказоустойчивой архитектуре, в разбивке сред – разработка, тест, препрод, прод).
- Сайзинг на аппаратное обеспечение системы, в разбивке сред (разработка, 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.

3.2.11. 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	Утверждение	Исполнение	Контроль	Отчетность
Руководитель		RU	R	R	R
Исполнитель			CRU		CRU
Администратор	CRU				
Офицер ИБ		CRU			

3.2.12. Требования к информационной безопасности

3.2.12.1. 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.

3.2.12.2. 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.

3.2.12.3. 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.

3.2.12.4. 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).

3.2.12.5. 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.

3.2.12.6. Антивирусная защита

Реализация антивирусной защиты или интеграция с существующими системами защиты.

3.2.12.7. Обнаружение вторжений

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

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

3.2.12.8. 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.

3.2.12.9. 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.

3.2.12.10. 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.

3.2.12.11. 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.

3.2.12.12. 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).

3.2.12.13. 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) скрывание 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 возникновения отказов (сбоев) в системе защиты информации информационной системы.

Защита мобильных технических средств, применяемых в информационной системе.