

Работа 2. Разработка регламента управления ИТ-сервисом

ИТ-сервис: Организация удалённого доступа к информационным ресурсам по защищённому каналу с помощью технологий VPN

1. Описание предоставляемого сервиса

1.1. Назначение сервиса

ИТ-сервис обеспечивает защищенный удаленный доступ сотрудников компании к корпоративным информационным системам (файловым хранилищам, CRM, почтовым серверам, системам документооборота) посредством VPN-соединения. Главная цель – обеспечить безопасную, стабильную и управляемую работу пользователей вне офиса.

1.2. Типы запросов

№	Тип запроса	Пример	Категория ITIL
1	Подключение к VPN	Новый сотрудник запрашивает доступ	Request Fulfilment
2	Восстановление подключения	Потеря связи или ошибка аутентификации	Incident Management
3	Изменение конфигурации	Добавление нового сервера, политика шифрования	Change Enablement
4	Повторяющийся сбой	Неустойчивые соединения, сбои шифрования	Problem Management
5	Консультация	Инструкция по установке клиента, настройке	Service Desk Support

1.3. Источники запросов (роли)

- Пользователи (сотрудники, подрядчики) – обращаются через Service Desk.
- Service Desk – принимает, классифицирует и назначает запросы.
- Системные администраторы VPN – обрабатывают технические инциденты.
- Инженеры ИБ – контролируют безопасность, ключи и сертификаты.

1.4. Результаты выполнения запросов

- VPN- доступ предоставлен, изменен или восстановлен
- Инцидент устранен
- Предоставлена консультация пользователю
- Выполнено изменение конфигурации с сохранением доступности

1.5. Критерии качества

- Доступность сервиса $\geq 99,9\%$
- Среднее время реакции ≤ 15 минут
- Среднее время устранения неисправности ≤ 1 час
- Уровень удовлетворенности пользователей $\geq 90\%$

1.6. Правила обработки запросов

1. Все обращения фиксируются в Service Desk
2. Классификация выполняется автоматически или оператором
3. Приоритет определяется по влиянию и срочности
4. Исполнитель назначается согласно SLA
5. После устранения проблемы проводится подтверждение пользователем

2. Окружение предоставляемого сервиса

2.1. Другие ИТ-сервисы предприятия

- Корпоративная почта (Exchange/Outlook)
- Файловое хранилище (SMB)
- Система документооборота
- CRM-система
- Веб-портал сотрудников
- Система управления пользователями (Active Directory)

VPN обеспечивает защищённый доступ ко всем перечисленным системам.

2.2. Характеристика потребителей

Группа пользователей	Требования	Квалификация
Офисные сотрудники	Стабильное подключение, высокая скорость	Средняя
Руководители	Быстрый доступ, мобильное подключение	Средняя

Разработчики	Доступ к репозиториям и серверам	Высокая
Подрядчики	Ограниченные права, контроль безопасности	Средняя-высокая

2.3. Характеристика инфраструктуры

- VPN-серверы: основной и резервный
- Протоколы: OpenVPN, IPSec
- Шифрование: AES-256
- Аутентификация: через Active Directory
- Мониторинг: Zabbix + Syslog
- Резервирование: аппаратное и сетевое
- Service Desk: система регистрации инцидентов (Jira)

2.4. Зависимости

VPN зависит от:

- сетевого оборудования (маршрутизаторы, коммутаторы)
- DNS и DHCP
- системы AD
- SIEM для анализа логов безопасности

3. Процессы ITIL, реализуемые для управления VPN-сервисом

Процесс ITIL	Назначение	Обоснование
Incident Management	Восстановление работы VPN после сбоев	Минимизация простоев
Problem Management	Анализ повторяющихся инцидентов	Устранение корневых причин
Change Enablement	Управление изменениями конфигурации	Безопасное внедрение обновлений
Service Request Management	Выполнение стандартных запросов пользователей	Оперативное обслуживание
Information Security Management	Контроль доступа и шифрования	Ключевая особенность VPN
Availability Management	Поддержание целевых показателей доступности	Соблюдение SLA 99,9%
Continual Improvement (CSI)	Повышение качества обслуживания	Оценка метрик, совершенствование процессов

4. Роли и задачи

Роль	Операционные задачи	Стратегические задачи
Service Desk специалист	Регистрация и классификация обращений	Оптимизация маршрутизации запросов
Системный администратор VPN	Устранение инцидентов, настройка	Анализ и оптимизация конфигураций
Инженер ИБ	Контроль сертификатов и логов	Разработка политики безопасности
Менеджер ИТ-сервисов	Контроль SLA, подготовка отчётов	Планирование развития сервиса
Change Manager	Согласование изменений	Разработка стратегии обновлений
Problem Manager	RCA-анализ и документирование	Профилактика сбоев

5. Регламенты выполнения задач

5.1. Инцидент (Incident Management)

Цель: Восстановление VPN-доступа.

Вход: зарегистрированный инцидент.

Шаги:

1. Регистрация обращения в Service Desk.
2. Проверка статуса серверов в Zabbix.
3. Определение причины (оборудование, аутентификация, маршрут).
4. Устранение проблемы.
5. Проверка восстановления.
6. Закрытие инцидента, уведомление пользователя.

Выход: восстановленная работоспособность.

Критерий приёма: подтверждение пользователем.

5.2. Запрос на подключение ((Request Fulfilment)

Цель: Создание новой учётной записи VPN.

Шаги:

1. Пользователь подаёт заявку.
2. Проверка прав доступа.
3. Создание учётной записи.
4. Отправка инструкции пользователю.
5. Проверка успешного подключения.

Критерий: успешная авторизация.

5.3. Внесение изменений (Change Enablement)

Цель: Безопасное обновление конфигурации.

Шаги:

1. Инициатор создаёт RFC-заявку.
2. Change Manager анализирует риски.
3. Одобрение CAB.
4. Тестирование и внедрение.

5. Проверка корректности.

Критерий: отсутствие сбоев после внедрения.

5.4. Анализ проблем (Problem Management)

Цель: Устранение повторяющихся сбоев.

Шаги:

1. Сбор данных об инцидентах.
2. Анализ причин (RCA).
3. Разработка корректирующих действий.
4. Документирование решений.

Критерий: снижение количества схожих инцидентов.

5.5. Контроль безопасности (Information Security Management)

Цель: Поддержание защищённости VPN.

Шаги:

1. Проверка сроков сертификатов.
2. Ротация ключей шифрования.
3. Анализ логов SIEM.
4. Отчёт службе ИБ.

Критерий: отсутствие нарушений безопасности.