

Регламент управления ИТ-сервисом VPN

1. Описание предоставляемого сервиса

1.1. Наименование сервиса

ИТ-сервис: «Защищённый удалённый доступ (VPN)»

Назначение: обеспечение безопасного и стабильного соединения сотрудников клиента с корпоративной сетью предприятия посредством VPN-технологий.

Цель: предоставить пользователям возможность удалённого доступа к внутренним ресурсам организации с требуемым уровнем безопасности, доступности и производительности.

1.2. Типы запросов по сервису

Обработка запросов по VPN-сервису осуществляется через систему Service Desk и портал самообслуживания. Запросы делятся на следующие категории:

Категория	Пример запроса	Характер обработки
Инцидент (Incident)	Недоступен VPN, невозможно подключиться, низкая скорость соединения, частые обрывы	Реакция по приоритету, устранение сбоя, восстановление работоспособности
Запрос на обслуживание (Service Request)	Подключение нового пользователя, изменение прав доступа, настройка туннеля, установка клиента VPN	Выполняется по стандартной процедуре без изменения конфигурации сервиса
Запрос на изменение (Change Request)	Замена VPN-шлюза, обновление прошивки, изменение схемы маршрутизации	Оформляется через процесс Change Management, с согласованием и тестированием
Запрос на информацию (Information Request)	Предоставить отчёт о доступности сервиса, статистику инцидентов, рекомендации по подключению	Выполняется в течение 1 рабочего дня
Безопасность (Security Incident)	Подозрение на компрометацию учётных данных, несанкционированное	Эскалируется службе безопасности, проводится расследование

	подключение	
--	-------------	--

1.3. Источники и роли, подающие запросы

Роль / Источник	Описание	Права и ограничения
Обычный пользователь	Сотрудник организации, использующий VPN для доступа к ресурсам	Может регистрировать инциденты и запросы на обслуживание через портал
ИТ-администратор клиента	Представитель клиента, ответственный за взаимодействие с поставщиком	Может направлять запросы на изменение, получать отчётность
Служба информационной безопасности (ИБ)	Контролирует соблюдение политик безопасности и аудит подключений	Получает уведомления о нарушениях и инцидентах безопасности
Служба поддержки (Service Desk)	Обрабатывает обращения, классифицирует и маршрутизирует их	Инициирует процессы Incident/Request/Change Management
Инженер поддержки (Support Engineer)	Выполняет диагностику, устранение неисправностей и изменения	Исполняет запросы в установленные сроки SLA

1.4. Результаты выполнения запросов

Результатом обработки запроса является: восстановление доступа к VPN-сервису; успешное подключение нового пользователя; изменение параметров конфигурации по запросу клиента; предоставление отчёта или справочной информации; уведомление клиента о выполнении и закрытии заявки в системе. Каждая заявка сопровождается отчётом о выполнении, содержащим: номер запроса, описание проблемы или задачи, выполненные действия, фактическое время реакции и восстановления, отметку о подтверждении клиентом.

1.5. Критерии качества обслуживания

В соответствии с соглашением SLA для VPN-сервиса, определяются следующие показатели качества (SLO):

Показатель	Целевое значение	Метод контроля
------------	------------------	----------------

Доступность сервиса (Uptime)	$\geq 99.95\%$ в месяц	Автоматический мониторинг шлюзов
Задержка (Latency)	≤ 50 мс	Средняя круговая задержка (ping)
Потеря пакетов (Packet Loss)	$\leq 0.5\%$	Сбор метрик с сетевого оборудования
Время реакции на инцидент (Response Time)	15 мин (высокий приоритет), 2 ч (средний), 8 ч (низкий)	С момента регистрации заявки
Время восстановления сервиса (Resolution Time)	≤ 4 ч (высокий приоритет), ≤ 24 ч (средний), ≤ 72 ч (низкий)	До полного восстановления VPN
Информирование клиента	В течение 15 мин после регистрации критического инцидента	Уведомление по email/телефону

1.6. Правила обработки запросов

Регистрация — все запросы фиксируются в системе Service Desk или через портал самообслуживания.

Классификация — определяется тип (инцидент, запрос, изменение) и приоритет.

Назначение исполнителя — система маршрутизирует заявку на инженера или менеджера по процессу.

Исполнение — производится устранение проблемы или выполнение задачи.

Отчётность — исполнитель фиксирует результаты, заполняет отчёт о выполнении.

Закрытие — клиент получает уведомление и подтверждает выполнение.

Анализ (при необходимости) — в случае повторяющихся сбоев проводится анализ первопричин (Problem Management).

Все запросы должны быть выполнены в пределах установленных SLA, а в случае нарушения параметров клиенту предоставляется сервисный кредит (компенсация).

2. Описание окружения предоставляемого сервиса

2.1. Общая характеристика окружения

ИТ-сервис «Защищённый удалённый доступ (VPN)» является частью корпоративной инфраструктуры предприятия и обеспечивает безопасное подключение сотрудников к внутренним ресурсам компании с удалённых рабочих мест.

Сервис функционирует в составе экосистемы взаимосвязанных ИТ-сервисов,

поддерживающих бизнес-процессы организации, и зависит от корректной работы сетевой, серверной и аутентификационной инфраструктуры.

2.2. Наличие других ИТ-сервисов на предприятии

VPN-сервис не является автономным и интегрирован с рядом других ИТ-сервисов предприятия, обеспечивающих его функционирование и безопасность:

Категория сервиса	Наименование	Назначение / Взаимосвязь
Сетевая инфраструктура	Корпоративная сеть, маршрутизаторы, межсетевые экраны	Обеспечивают маршрутизацию трафика и защиту каналов связи
Служба каталогов (Directory Service)	Active Directory (AD)	Управляет учётными записями пользователей и групп, обеспечивает централизованную аутентификацию VPN
Служба мониторинга	Zabbix / Grafana / Nagios	Отслеживает состояние VPN-шлюзов, нагрузку, пропускную способность и время отклика
Служба Service Desk	Портал заявок / HelpDesk	Принимает, классифицирует и обрабатывает обращения пользователей по инцидентам и запросам
Система безопасности (SOC)	SIEM, антивирус, IDS/IPS	Анализирует сетевые события, выявляет попытки несанкционированного доступа
Почтовый сервис	Корпоративная почта	Используется для уведомлений и рассылки отчётов по SLA
Облачные сервисы	Google Cloud, Huawei Cloud, Alibaba Cloud (в сравнении)	Возможные внешние площадки размещения VPN-шлюзов, обеспечивающие отказоустойчивость и масштабирование

2.3. Характеристика потребителей сервиса

Пользователи VPN-сервиса подразделяются на несколько категорий в зависимости от выполняемых функций и требований к качеству обслуживания.

Категория пользователей	Пример	Основные требования к сервису	Уровень квалификации
Офисные сотрудники	Бухгалтерия, HR, отдел закупок	Доступ к внутренним системам и файлам, стабильное соединение	Средний
Удалённые специалисты	Разработчики, аналитики,	Высокая пропускная способность, минимальные	Высокий

	инженеры	задержки, круглосуточная доступность	
Менеджеры и руководство	Руководители отделов, директора	Гарантиированная доступность и безопасность соединения	Средний
ИТ-персонал клиента	Администраторы сети и систем	Полный доступ к панели управления, мониторинг, возможность эскалации	Высокий
Временные подрядчики / партнёры	Внешние консультанты	Ограниченные права доступа, временные учётные записи	Различный

Общая численность пользователей сервиса – около **150 активных подключений**, из которых около **60% работают удалённо**.

2.4. Характеристика ИТ-инфраструктуры

Инфраструктура, обеспечивающая функционирование VPN-сервиса, включает в себя аппаратные и программные компоненты, средства защиты и мониторинга.

Компонент	Назначение	Технические характеристики / особенности
VPN-шлюзы (основной и резервный)	Обеспечивают туннелирование и шифрование трафика	Поддержка IPSec, SSL; резервирование по схеме Active/Standby
Сервер аутентификации (RADIUS / AD)	Проверка подлинности пользователей	Интеграция с корпоративным каталогом
Сервер управления и отчёtnости	Хранение логов подключений, статистики, SLA-отчётов	Автоматическая генерация ежемесячных отчётов
Каналы связи	Соединение между офисом, облачными площадками и пользователями	Доступ через интернет с резервированием каналов
Портал самообслуживания	Ввод заявок, получение инструкций, отслеживание статуса	Веб-доступ 24/7, интеграция с Service Desk
Система мониторинга	Контроль состояния шлюзов и подключений	Сбор метрик: доступность, задержка, потери пакетов

2.5. Зависимости сервиса от других компонентов

VPN-сервис зависит от работы следующих элементов инфраструктуры и сервисов:

1. **Сетевой инфраструктуры** – при нарушении маршрутизации или отказе сетевых устройств доступ к VPN невозможен.
2. **Сервиса каталогов (AD)** – сбои аутентификации приводят к отказу в доступе пользователей.
3. **Интернет-канала** – нестабильность канала вызывает снижение доступности сервиса.
4. **Мониторинга и логирования** – их корректная работа необходима для SLA-контроля и анализа инцидентов.
5. **Службы Service Desk** – без неё невозможна регистрация, классификация и отслеживание заявок.
6. **Систем безопасности (SOC, SIEM)** – обеспечивает своевременное выявление угроз и защиту трафика VPN.

2.6. Вывод

Окружение сервиса VPN характеризуется высокой взаимозависимостью с другими ИТ-сервисами предприятия.

Для обеспечения устойчивой работы и соответствия SLA требуется:

- поддержание отказоустойчивости инфраструктуры (резервирование шлюзов и каналов);
- взаимодействие между командами сетевой, серверной и сервисной поддержки;
- регулярный аудит производительности и безопасности;
- координация изменений через процессы ITIL (Change, Problem, Capacity, Security Management).

3. ITIL-процессы, реализуемые для управления ИТ-сервисом VPN

3.1. Общие положения

Для эффективного управления ИТ-сервисом «Защищённый удалённый доступ (VPN)» необходимо внедрение набора процессов, соответствующих лучшим практикам библиотеки **ITIL (Information Technology Infrastructure Library)**.

Данные процессы обеспечивают прозрачность, предсказуемость и управляемость жизненного цикла сервиса — от обработки инцидентов до стратегического планирования его развития.

3.2. Цели внедрения ITIL-процессов

- Повышение доступности и надёжности VPN-сервиса;
- Сокращение времени реакции и восстановления при инцидентах;
- Обеспечение стабильного качества обслуживания (SLA);
- Контроль рисков при изменениях;
- Формирование устойчивой системы планирования и улучшения сервиса;

- Поддержка информационной безопасности и соответствие политикам ИБ.

3.3. Выбранные процессы ITIL и обоснование их внедрения

№	Процесс ITIL	Назначение и обоснование внедрения	Уровень
1	Incident Management	Обеспечивает оперативное восстановление нормальной работы VPN при сбоях и минимизацию времени простоя. Критичен для SLA с показателем доступности $\geq 99.95\%$.	Операционный
2	Request Fulfillment	Отвечает за обработку стандартных пользовательских запросов: подключение, изменение прав, сброс пароля, выдачу отчётов. Позволяет разграничить обслуживание от инцидентов.	Операционный
3	Change Management	Регулирует процесс внесения изменений в инфраструктуру VPN (обновление шлюзов, изменение маршрутизации, настройка безопасности). Минимизирует риски простоев и несогласованных изменений.	Тактический
4	Problem Management	Анализирует повторяющиеся инциденты, выявляет первопричины и предлагает корректирующие меры. Повышает стабильность и снижает нагрузку на поддержку.	Тактический
5	Service Level Management (SLM)	Контролирует выполнение SLA, формирует отчётность для клиента, обеспечивает постоянную коммуникацию между бизнесом и ИТ.	Тактический / стратегический
6	Availability Management	Отвечает за обеспечение требуемого уровня доступности сервиса. Анализирует метрики времени простоя, определяет узкие места инфраструктуры.	Тактический
7	Capacity Management	Оценивает пропускную способность каналов, производительность шлюзов и прогнозирует рост нагрузки при увеличении числа пользователей.	Тактический
8	Information Security Management (ISM)	Гарантирует соблюдение политик безопасности: контроль доступа, защита данных, предотвращение несанкционированных подключений. Критичен для VPN-услуги.	Тактический / стратегический
9	Continual Service	Формирует культуру постоянного улучшения сервиса. Анализирует метрики, отчёты и	Стратегический

	Improvement (CSI)	обратную связь пользователей для внедрения улучшений.	
--	--------------------------	---	--

3.4. Взаимосвязи между процессами (прямые зависимости)

Исходный процесс	Взаимосвязанные процессы	Описание зависимости
Incident Management	Problem Management, Change Management	Инциденты могут выявлять необходимость анализа причин или корректирующих изменений
Request Fulfillment	Service Level Management	Выполнение стандартных запросов влияет на показатели SLA (сроки реакции и закрытия)
Problem Management	Availability, Capacity, CSI	Анализ причин сбоев помогает улучшать доступность и производительность
Change Management	Information Security, SLM	Все изменения должны быть безопасны и согласованы в рамках SLA
Availability Management	Capacity, Change	Поддержание доступности требует контроля ресурсов и планирования изменений
Information Security Management	Incident, Change	Инциденты безопасности инициируют изменения политик доступа
CSI	Все остальные процессы	Обеспечивает анализ, контроль и улучшение эффективности всех процессов

3.5. Процессы стратегического развития окружения сервиса

Для обеспечения долгосрочной стабильности и развития VPN-сервиса рекомендуется внедрить следующие **стратегические ITIL-процессы**:

1. **IT Service Continuity Management (ITSCM)** — управление непрерывностью ИТ-услуг.
 - Создание резервных VPN-шлюзов и каналов.
 - План восстановления после аварий (Disaster Recovery Plan).
 - Тестирование сценариев отказа.
2. **Financial Management for IT Services** — управление затратами и бюджетированием.
 - Учёт стоимости инфраструктуры и лицензий.

- Расчёт окупаемости и стоимости владения VPN-сервисом.
- Формирование бюджета на модернизацию оборудования.

3. **Supplier Management** — управление поставщиками.

- Контроль качества услуг сторонних провайдеров (интернет-каналы, облачные площадки).
- Оценка SLA поставщиков и соответствие их показателей внутренним стандартам.

4. **Knowledge Management** — управление знаниями.

- Создание базы знаний по инцидентам и стандартным операциям.
- Повышение эффективности поддержки и сокращение времени решения типовых проблем.

4. Роли в рамках выделенных процессов и задачи для каждой роли

4.1. Общие положения

В целях эффективного управления ИТ-сервисом «Защищённый удалённый доступ (VPN)» устанавливается распределение ролей и ответственности в соответствии с принципами ITIL. Каждая роль обеспечивает выполнение определённого набора задач в рамках соответствующих процессов.

4.2. Роли и их задачи

Роль	Основные задачи	Уровень ответственности
Service Manager (Менеджер сервиса)	<ul style="list-style-type: none"> • Контроль выполнения SLA и SLO • Анализ метрик доступности, качества и инцидентов • Организация взаимодействия между поставщиком и клиентом • Подготовка ежемесячных отчётов и предложений по улучшению сервиса 	Стратегический
Incident Manager (Менеджер по инцидентам)	<ul style="list-style-type: none"> • Контроль своевременной регистрации и обработки инцидентов • Определение приоритетов и эскалация 	Операционный / Тактический

	<ul style="list-style-type: none"> • Ведение журнала инцидентов и отчётности по SLA 	
Change Manager (Менеджер изменений)	<ul style="list-style-type: none"> • Координация запросов на изменения (RFC) • Оценка влияния изменений на сервис • Планирование и утверждение изменений • Контроль послерелизного тестирования 	Тактический
Problem Manager (Менеджер по проблемам)	<ul style="list-style-type: none"> • Идентификация корневых причин инцидентов • Разработка корректирующих и предупреждающих мер • Подготовка отчётов по проблемам и рекомендаций 	Тактический / Стратегический
Support Engineer (Инженер поддержки)	<ul style="list-style-type: none"> • Исполнение запросов и устранение инцидентов • Мониторинг состояния VPN-шлюзов • Поддержание базы знаний и документации 	Операционный
Security Officer (Специалист по ИБ)	<ul style="list-style-type: none"> • Контроль аутентификации и политик доступа • Анализ инцидентов безопасности • Реализация мер защиты и расследование нарушений 	Тактический / Стратегический
Service Desk Operator (Оператор службы поддержки)	<ul style="list-style-type: none"> • Регистрация заявок • Первичная диагностика и классификация обращений • Информирование пользователей о ходе обработки 	

5. Регламенты выполнения задач

Ниже приведены основные регламенты для ключевых процессов ITIL, реализуемых в рамках управления VPN-сервисом.

5.1. Регламент процесса Incident Management

Цель: оперативное восстановление нормальной работы VPN-сервиса при возникновении сбоев.

Ответственные роли: Service Desk Operator, Support Engineer, Incident Manager.

Входные данные:

- зарегистрированная заявка в Service Desk;
- описание проблемы и приоритет;
- контактные данные пользователя.

Последовательность действий:

1. Регистрация инцидента в системе Service Desk.
2. Классификация и определение приоритета (высокий, средний, низкий).
3. Назначение инженера поддержки.
4. Диагностика причины сбоя (проверка шлюза, туннеля, журналов).
5. Принятие мер по устранению: перезапуск сервиса, обновление маршрутов, сброс сессий.
6. Восстановление работоспособности и тестирование подключения.
7. Информирование клиента о решении.
8. Закрытие заявки и обновление базы знаний.

Выходные данные:

- отчёт об инциденте (дата, причина, действия, время восстановления);
- обновлённые данные мониторинга и статистики SLA.

Критерий приёма: подтверждение клиента о восстановлении доступа.

5.2. Регламент процесса Request Fulfillment

Цель: выполнение стандартных запросов пользователей без влияния на инфраструктуру VPN.

Ответственные роли: Service Desk Operator, Support Engineer.

Входные данные: заявка пользователя на подключение, изменение или отчёт.

Действия:

1. Регистрация запроса в системе Service Desk.
2. Проверка корректности данных и прав пользователя.
3. Выполнение запроса:
 - добавление в группу доступа;
 - сброс пароля;
 - предоставление отчёта или инструкции.
4. Уведомление клиента о выполнении.
5. Закрытие заявки и отчёт в системе.

Выход: выполненная операция, отчёт о выполнении.

Критерий приёма: клиент подтвердил корректность выполнения запроса.

5.3. Регламент процесса Change Management

Цель: минимизация рисков при внесении изменений в инфраструктуру VPN.

Ответственные роли: Change Manager, Service Manager, Support Engineer.

Входные данные: запрос на изменение (RFC), описание и обоснование.

Действия:

1. Регистрация RFC в журнале изменений.
2. Анализ рисков, влияния и зависимости (Change Impact Assessment).
3. Утверждение изменений Change Advisory Board (CAB).
4. Планирование окна обслуживания.
5. Реализация изменений и тестирование.
6. Подготовка отчёта и обновление документации.

Выход: внедрённое изменение, отчёт об успешном тестировании.

Критерий приёма: отсутствие инцидентов после внедрения.

5.4. Регламент процесса Problem Management

Цель: выявление и устранение первопричин повторяющихся инцидентов.

Ответственные роли: Problem Manager, Incident Manager, Support Engineer.

Входные данные: отчёты о повторных инцидентах, логи, данные мониторинга.

Действия:

1. Анализ инцидентов для выявления закономерностей.
2. Определение возможных первопричин.
3. Проведение расследования и документирование Root Cause Analysis (RCA).
4. Формирование корректирующих действий (например, изменение конфигурации).
5. Передача рекомендаций в Change Management.
6. Контроль внедрения решений и повторная оценка.

Выход: отчёт RCA, рекомендации по улучшению.

Критерий приёма: отсутствие повторных инцидентов в течение установленного периода.

5.5. Регламент процесса Information Security Management

Цель: обеспечение безопасности данных, передаваемых через VPN-каналы, и предотвращение несанкционированного доступа.

Ответственные роли: Security Officer, Service Manager.

Входные данные: политика безопасности, логи VPN, отчёты о попытках входа.

Действия:

1. Мониторинг событий безопасности (успешные/неудачные попытки входа).
2. Анализ подозрительных активностей.
3. Реагирование на инциденты безопасности.
4. Блокировка учётных записей при нарушениях.
5. Проведение расследования и уведомление руководства.
6. Обновление политик безопасности и инструкций.

Выход: отчёт по ИБ-инцидентам, предложения по усилению защиты.

Критерий приёма: отсутствие компрометации данных и подтверждённое устранение угрозы.

5.6. Регламент процесса Service Level Management (SLM)

Цель: обеспечение соблюдения SLA и постоянное улучшение качества обслуживания.

Ответственные роли: Service Manager, Incident Manager, Change Manager.

Вход: ежемесячные отчёты по доступности, времени реакции и восстановления.

Действия:

1. Сбор статистики SLA за отчётный период.
2. Анализ нарушений и причин.
3. Формирование отчёта клиенту.
4. Обсуждение корректирующих мер.
5. Внесение предложений в CSI для улучшения показателей.

Выход: отчёт SLA, протокол обсуждения, рекомендации по улучшению.

Критерий приёма: утверждение отчёта клиентом и согласование плана действий.

5.7. Регламент процесса Continual Service Improvement (CSI)

Цель: постоянное совершенствование сервиса на основе анализа данных и обратной связи.

Ответственные роли: Service Manager, Problem Manager, Security Officer.

Входные данные: отчёты SLA, RCA, результаты аудитов, отзывы пользователей.

Действия:

1. Анализ эффективности текущих процессов.
2. Сбор предложений по улучшению.
3. Оценка приоритетов и влияния изменений.
4. Разработка плана улучшений.
5. Реализация мер через Change Management.
6. Мониторинг результатов внедрения.

Выход: обновлённые процедуры, улучшенные показатели SLA.

Критерий приёма: достижение целевых показателей улучшений.