Работа 1. Разработка проекта Service Level Agreement

Вариант 2

Тема: Организация удалённого доступа к информационным ресурсам по защищённому каналу с помощью технологий VPN

1. Введение

Современные организации активно используют технологии VPN (Virtual Private Network) для обеспечения защищённого доступа сотрудников к корпоративным ресурсам. VPN позволяет создавать зашифрованные соединения через общедоступные сети, обеспечивая конфиденциальность и целостность данных.

Для оценки и управления качеством предоставления услуги удалённого доступа применяется Соглашение об уровне сервиса (SLA) — документ, фиксирующий параметры доступности, производительности и безопасности сервиса.

Цель работы: разработать типовой проект SLA для услуги организации удалённого доступа по технологии VPN.

Задачи:

- Изучить теоретические основы SLA;
- Проанализировать не менее трёх примеров SLA, относящихся к VPN или аналогичным сетевым услугам;
- Провести сравнительный анализ примеров;
- Разработать собственный вариант SLA.

2. Выбор ИТ-сервиса

Организация удалённого доступа к корпоративным ресурсам по защищённому каналу с использованием технологий VPN (например, OpenVPN, IPSec, WireGuard)

Описание услуги:

Сервис обеспечивает удалённое подключение сотрудников к внутренним информационным системам предприятия через защищённое зашифрованное соединение. Подключение возможно с корпоративных или личных устройств, прошедших процедуру аутентификации.

Основные требования к качеству:

- высокая доступность сервиса
- минимальные задержки при установлении соединения
- устойчивость к сбоям и попыткам несанкционированного доступа
- конфиденциальность и целостность передаваемых данных

3. Анализ примеров SLA

Для анализа были выбраны три примера SLA:

№	**Источник**	**Тип услуги**	**Основные параметры SLA**
1	Microsoft Azure VPN Gateway SLA	Облачная VPN-служба	99,95% доступности 24/7 поддержка мониторинг и отчётность компенсации при нарушении
2	AWS Site-to-Site VPN SLA	Корпоративная VPN	99,9% доступности восстановление соединения ≤ 30 мин

			отчёты по инцидентам эскалация в 3 уровня
3	Cisco Meraki VPN SLA	Корпоративная VPN-платформа	99,95% доступности круглосуточная поддержка MTTR ≤ 60 мин аудит безопасности ежеквартально

4. Сравнительный анализ

Общие характеристики:

- Все SLA определяют целевые показатели доступности (Availability) на уровне не ниже 99,9%.
- Присутствуют обязательные параметры: время реакции (Response Time), время восстановления (MTTR), периодичность отчётности.
- Установлены обязанности сторон, включая отчётность поставщика и уведомление клиента о сбоях.
- Предусмотрены механизмы компенсации при несоблюдении SLA.

Отличительные особенности:

- Azure и Cisco включают регулярный аудит безопасности, AWS — нет.
- У AWS чётче регламентирована эскалация инцидентов.
- Cisco вводит метрики качества обслуживания (QoS) и мониторинг сетевой пропускной способности.

Вывод:

Наиболее сбалансированным является подход Cisco, где SLA охватывает как технические показатели, так и безопасность. Однако оптимальной является

комбинация подходов AWS (чёткая эскалация) и Azure (компенсации и прозрачность отчётности).

5. Проект типового SLA для VPN-сервиса

5.1. Общие сведения

Название услуги: VPN-доступ к корпоративным ресурсам
Поставщик: ИТ-отдел организации
Потребитель: сотрудники компании

5.2. Область действия

Данный SLA регулирует качество предоставления услуги VPN-доступа и устанавливает обязательные параметры обслуживания, методы контроля и ответственность сторон.

5.3. Целевые уровни качества

Параметр	**Целевое значение**	**Метод измерения**
Доступность сервиса (Availability)	≥ 99,9% в месяц	Мониторинг серверов
Время реакции службы поддержки	≤ 15 минут	Логи обращений
Время восстановления (MTTR)	≤ 1 час	Система отчётности инцидентов
Максимальное время установления соединения	≤ 10 секунд	Мониторинг соединений
Пропускная способность	≥ 100 Мбит/с (в среднем)	Тестирование пропускного канала
Уровень безопасности шифрования	AES-256	Конфигурация VPN-сервера

Время обновления сертификатов	≤ 24 часа с момента запроса	Отчёт службы безопасности

5.4. Ответственность сторон

Поставщик обязуется:

- обеспечивать функционирование VPN-сервиса в заявленных параметрах
- своевременно проводить профилактические работы (с уведомлением за 24 часа)
- осуществлять постоянный мониторинг доступности и безопасности

Потребитель обязуется:

- использовать только утверждённые клиенты VPN
- не передавать данные для подключения третьим лицам
- сообщать о сбоях или инцидентах безопасности

5.5. Мониторинг и отчётность

- Автоматический сбор метрик производится круглосуточно.
- Отчёты о доступности формируются ежемесячно и направляются в ИТ-департамент.
- Все инциденты фиксируются в системе учёта заявок.

5.6. Санкции и эскалация

- При снижении доступности ниже 99,9% — скидка 5% за каждый день отклонения.
- При повторных нарушениях в течение трёх месяцев SLA подлежит пересмотру.

- Эскалация выполняется по уровням: инженер → руководитель отдела → директор по ИТ.

5.7. Порядок изменения SLA

Изменения возможны по взаимному согласию сторон, с предварительным уведомлением не менее чем за 10 рабочих дней.

5.8. Срок действия и пересмотр

Соглашение действует 12 месяцев, пересматривается ежегодно в рамках бюджетного цикла или при изменении технологической инфраструктуры.

6. Заключение

В ходе работы были изучены принципы построения SLA и проведён анализ трёх документов, регулирующих качество VPN-сервисов.

Результатом стала разработка типового проекта SLA, отражающего ключевые показатели качества, методы мониторинга и ответственность сторон.

Разработанный SLA может использоваться как основа для внутренней регламентации работы ИТ-отдела при предоставлении услуги удалённого доступа.

Приложение

Соглашение об уровне предоставления услуг

1. Стороны соглашения

Поставщик услуги: _____, в лице _____, действующего на основании _____, именуемый в дальнейшем **«Поставщик»**, с одной стороны, и Заказчик услуги: _____, в лице _____, действующего на основании _____, именуемый в дальнейшем **«Заказчик»**, с другой стороны, совместно именуемые **«Стороны»**, заключили настоящее Соглашение об уровне предоставления услуг (SLA) со следующими условиями, указанными в данном договоре.

2. Предмет соглашения

Поставщик обязуется предоставлять Заказчику услугу защищённого VPN-доступа к корпоративным ресурсам, а Заказчик обязуется использовать услугу в соответствии с настоящим Соглашением.

SLA определяет:

- перечень предоставляемых услуг
- требования к качеству их оказания
- порядок контроля выполнения и взаимодействия сторон
- меры ответственности при нарушении установленных параметров

3. Функциональные характеристики услуги

3.1. Обеспечение защищённого подключения сотрудников к корпоративной сети посредством VPN.
3.2. Использование протоколов OpenVPN и IPSec, а также шифрования AES-256 для защиты передаваемых данных.
3.3. Поддержка одновременного подключения до 10 000 пользователей с масштабируемостью до 25 000.
3.4. Поддержка удалённого администрирования и централизованного контроля подключений.
3.5. Интеграция с системой аутентификации Active Directory.
3.6. Мониторинг состояния соединений и регистрация событий безопасности.
3.7. Масштабируемая пропускная способность до 10 Гбит/с.

4. Показатели качества услуги

4.1. Доступность услуги — не менее 99,9 % в расчёте на календарный месяц.
4.2. Надёжность — фактическая доступность не ниже 99,8 % от плановой.
4.3. Время обслуживания:
  4.3.1. работа службы поддержки — круглосуточно (24/7);
  4.3.2. время реакции на обращение — не более 15 минут;
  4.3.3. время устранения неисправностей (MTTR) — не более 1 часа.
4.4. Производительность — средняя пропускная способность от 100 Мбит/с до 10 Гбит/с, при средней загрузке не выше 80 %.
4.5. Безопасность и конфиденциальность — использование сертифицированных алгоритмов шифрования AES-256; отсутствие доступа к содержимому передаваемых данных.

4.6. Время восстановления сертификатов — не более 24 часов.

5. Обязанности Поставщика

5.1. Обеспечивать круглосуточное функционирование VPN-сервиса в пределах установленных показателей SLA.
5.2. Обеспечивать резервирование каналов связи и серверов VPN.
5.3. Поддерживать службу технической поддержки и реагировать на обращения в установленные сроки.
5.4. Вести постоянный мониторинг доступности и качества услуги.
5.5. Ежемесячно предоставлять Заказчику отчёт о доступности, производительности и инцидентах.
5.6. При выявлении инцидентов безопасности предпринимать корректирующие меры и уведомлять Заказчика.

6. Обязанности Заказчика

6.1. Использовать услугу в пределах согласованных нагрузок.
6.2. Сообщать Поставщику о планируемом росте числа пользователей и объёма трафика.
6.3. Обеспечивать защиту конечных устройств и персональных данных сотрудников.
6.4. Не передавать учётные данные третьим лицам и соблюдать внутренние политики безопасности.
6.5. Сообщать о выявленных неполадках через систему Service Desk.

7. Ответственность и санкции

При нарушении SLA Поставщиком:

- снижение доступности ниже 99,9 % компенсируется снижением тарифа или зачётом в следующем периоде.
- превышение времени устранения инцидента более чем на 1 час влечёт штраф в размере ___ % от месячной стоимости услуги.

При нарушении SLA Заказчиком:

- при превышении согласованной нагрузки без уведомления тариф увеличивается с применением коэффициента ___.
- при нарушении правил эксплуатации Поставщик вправе ограничить доступ к услуге до устранения нарушений.

8. Мониторинг и отчётность

8.1. Поставщик осуществляет мониторинг доступности, производительности и инцидентов с использованием средств Zabbix и Service Desk.
8.2. Отчёты формируются ежемесячно и предоставляются Заказчику в письменной или электронной форме.
8.3. По запросу Заказчика возможно предоставление внепланового отчёта.

9. Пересмотр SLA

9.1. Настоящее Соглашение подлежит обязательному пересмотру не реже одного раза в год.
9.2. Внеплановый пересмотр возможен при изменении инфраструктуры, политики безопасности или при росте числа пользователей.
9.3. Все изменения фиксируются в виде дополнительного соглашения, вступающего в силу после подписания обеими сторонами.

10. Взаимодействие сторон

10.1. Ежеквартальные отчётные встречи представителей Сторон для анализа показателей SLA и планирования улучшений.

10.2. Каналы связи: электронная почта, служба поддержки, телефон горячей линии.

10.3. Вопросы и предложения рассматриваются в течение 5 рабочих дней с момента получения.

11. Срок действия соглашения

Настоящее Соглашение вступает в силу с даты подписания и действует в течение _____, с возможностью продления по соглашению сторон.

12. Реквизиты и подписи сторон

Поставщик:	**Заказчик:**
_____	_____
_____	_____
_____	_____
_____	_____
название организации	название организации
_____	_____
_____	_____
_____	_____
адрес	адрес
_____	_____
_____	_____
телефон/email	телефон/email
_____	_____
_____	_____
_____	_____
_____	_____
ИНН, ОГРН	ИНН, ОГРН
_____	_____
должность ответственного лица	должность ответственного лица
_____	_____
подпись/расшифровка	подпись/расшифровка