Министерство образования Красноярского края
Краевое государственное бюджетное профессиональное образовательное учреждение
«Красноярский колледж радиоэлектроники и информационных технологий»

Отчет по Проекту

Выполнил студент группы 9САД2.20
Соколов Данила

О компании

- **Организация** - "ИнтеллектТех"
- **Название** - "ИнтеллектТех"
- **Основная бизнес-функция:**
- "ИнтеллектТех" связана с разработкой и предоставлением инновационных информационных технологий и программных решений для удовлетворения потребностей клиентов. Это включает в себя разработку кастомизированного программного обеспечения, создание высокотехнологичных информационных систем, консультирование и поддержка клиентов в внедрении современных технологий. Возможно, "ИнтеллектТех" также специализируется на разработке систем искусственного интеллекта, аналитических решений и других инновационных продуктов, направленных на оптимизацию бизнес-процессов и повышение эффективности операций клиентов.
- Компания "ИнтеллектТех"имеет имеет 5 филиалов которые состоят из 2 этажей .

Схема первого и второго этажа первого филиала

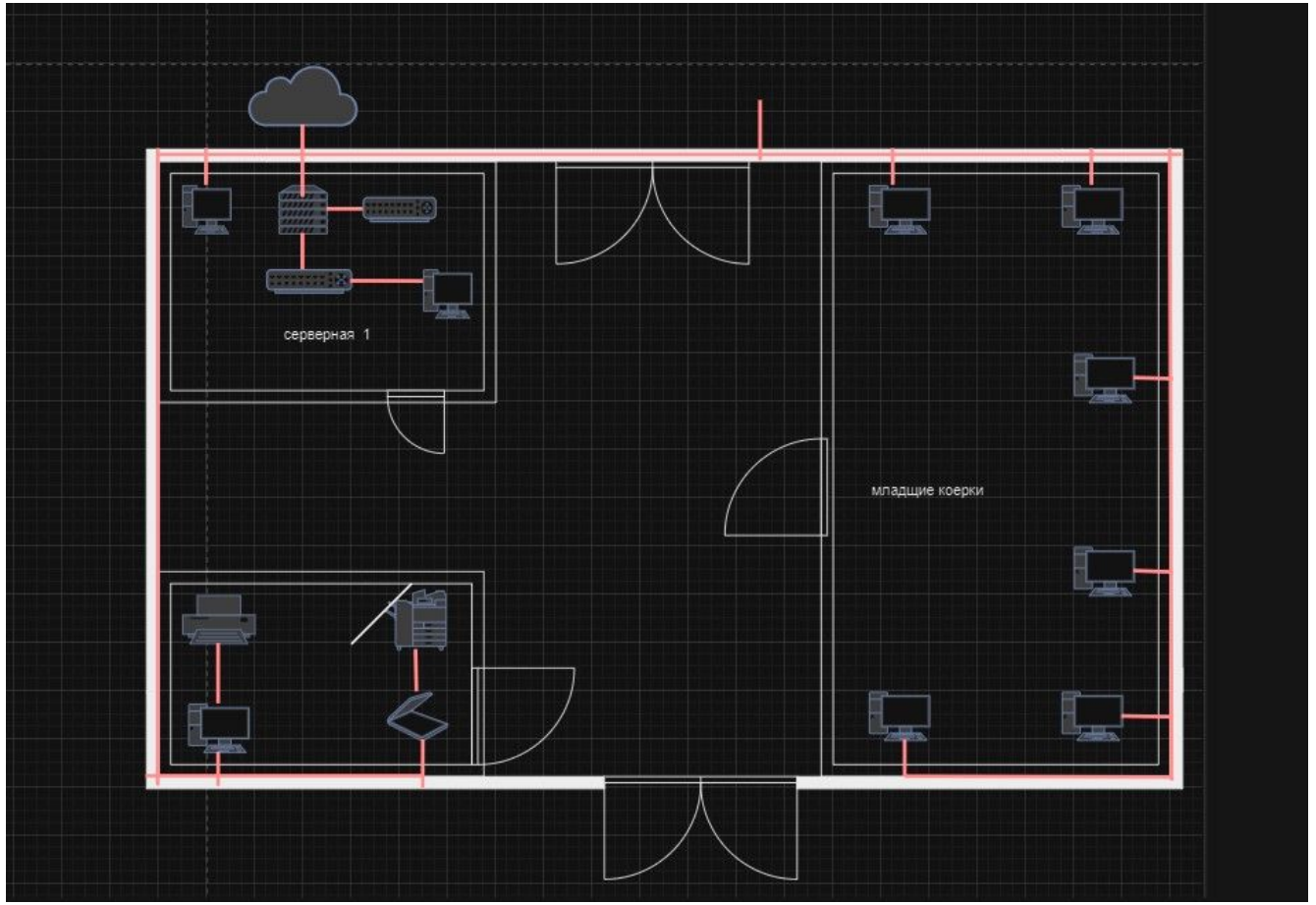


Схема первого и второго этажа первого филиала

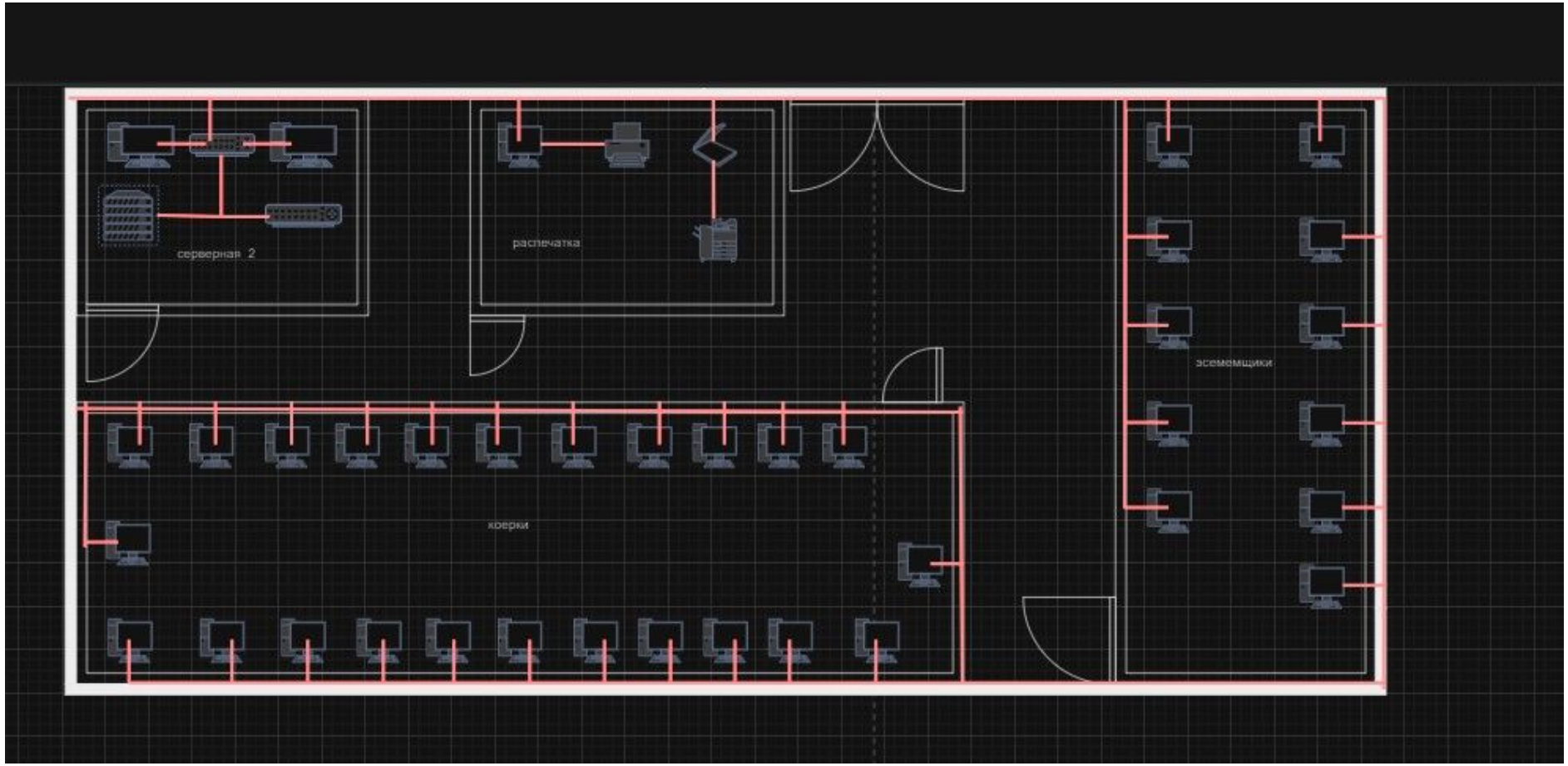


Схема первого и второго этажа второго филиала

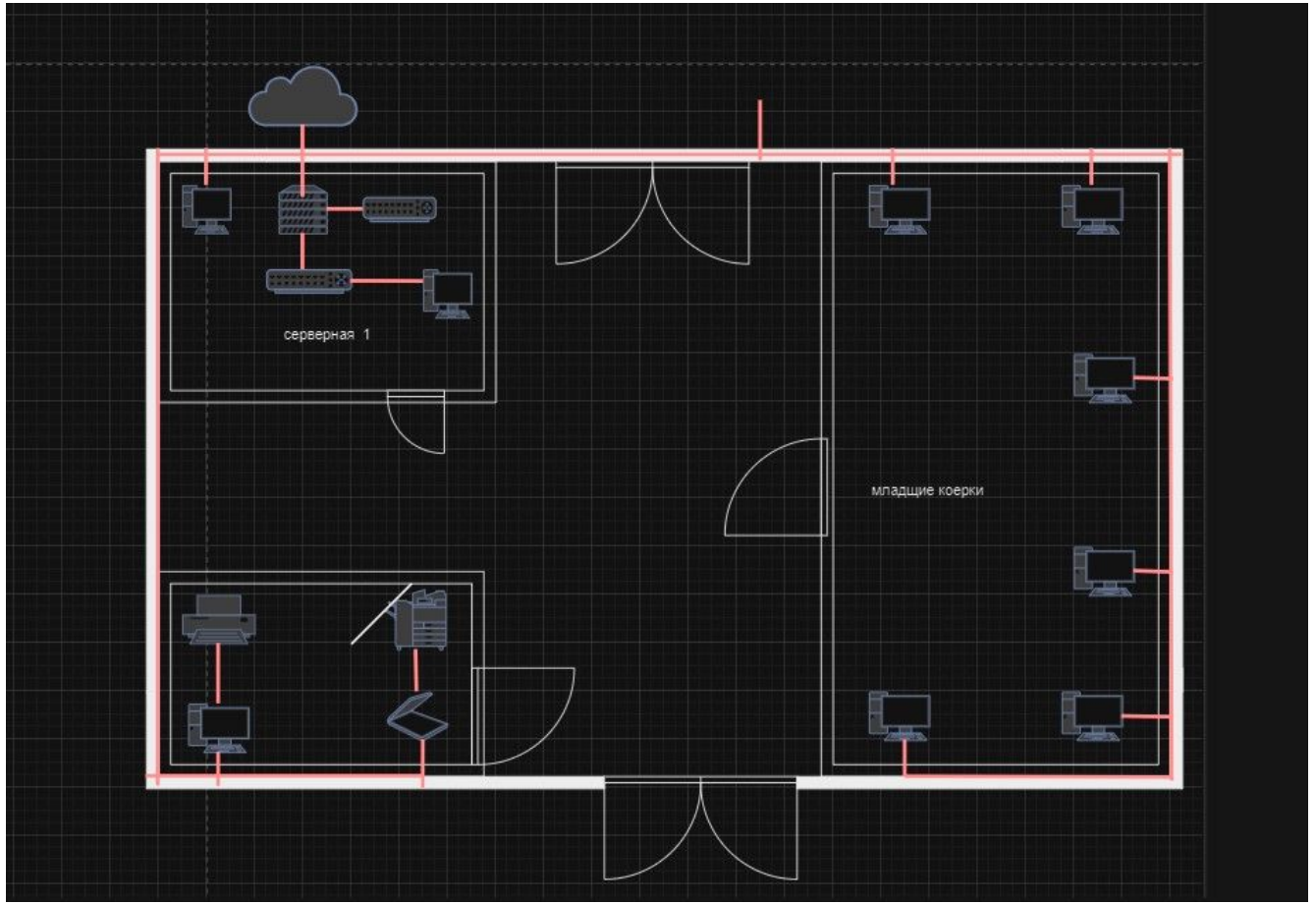


Схема первого и второго этажа второго филиала

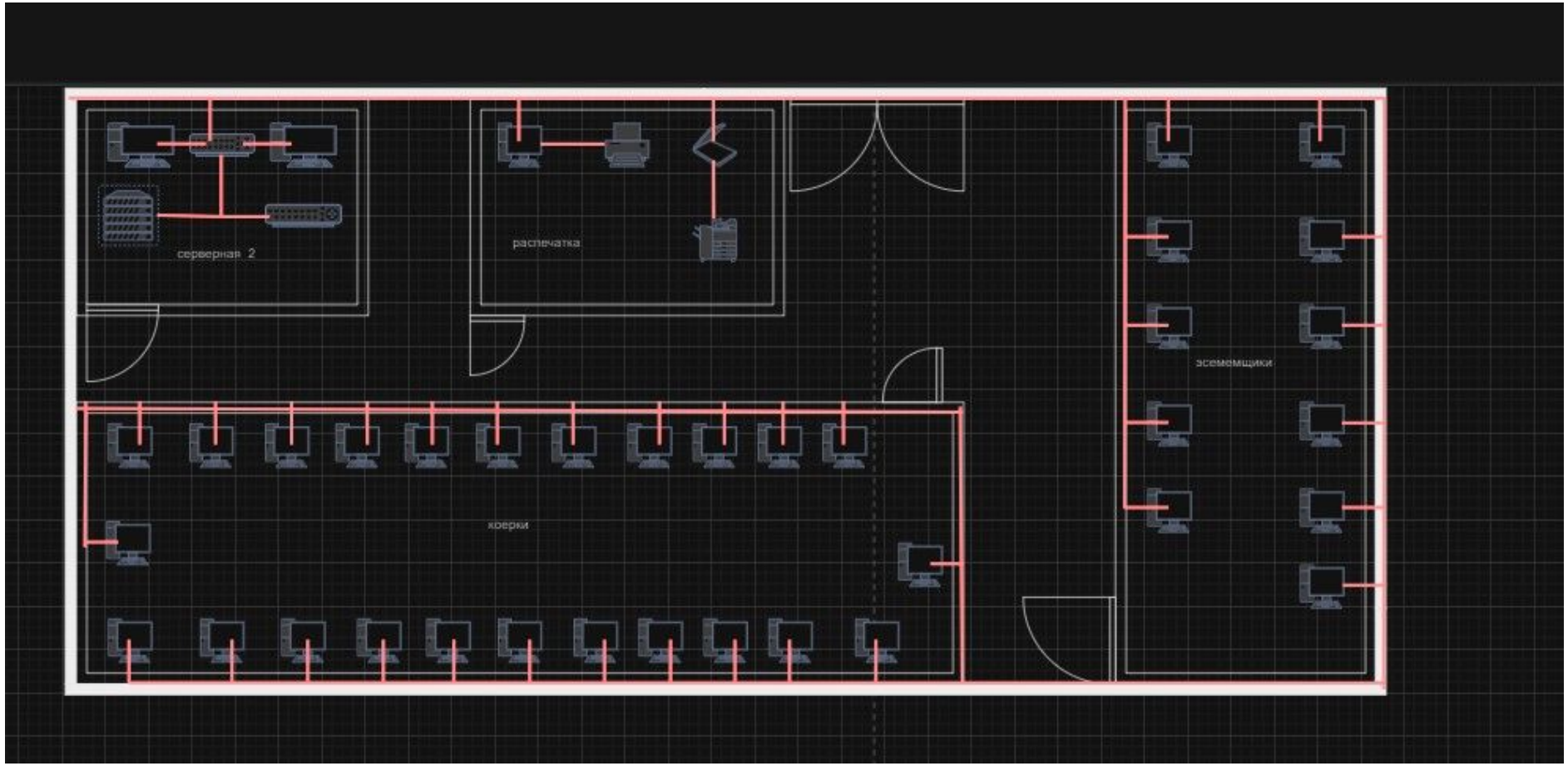


Схема первого и второго этажа третьего филиала

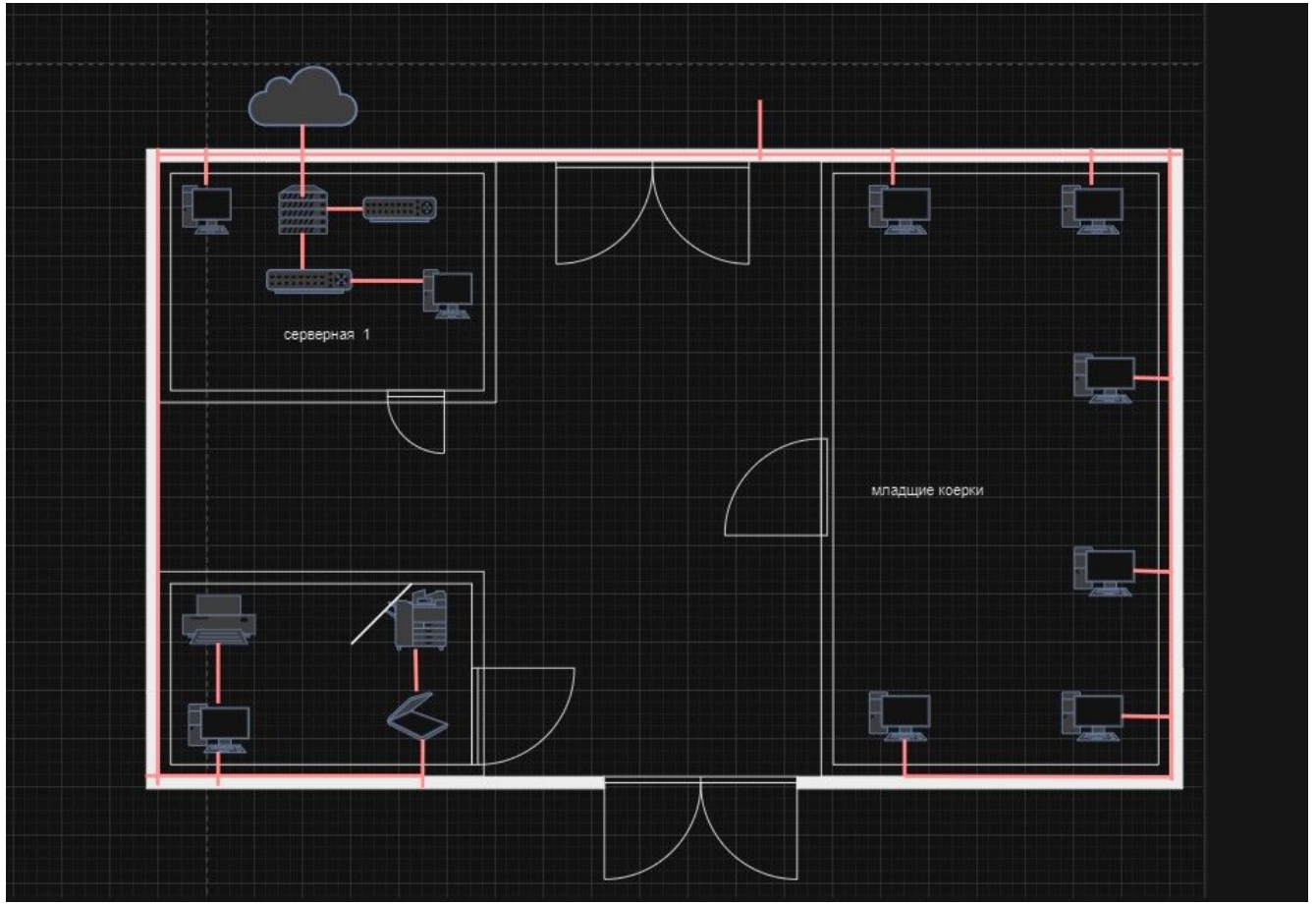


Схема первого и второго этажа третьего филиала

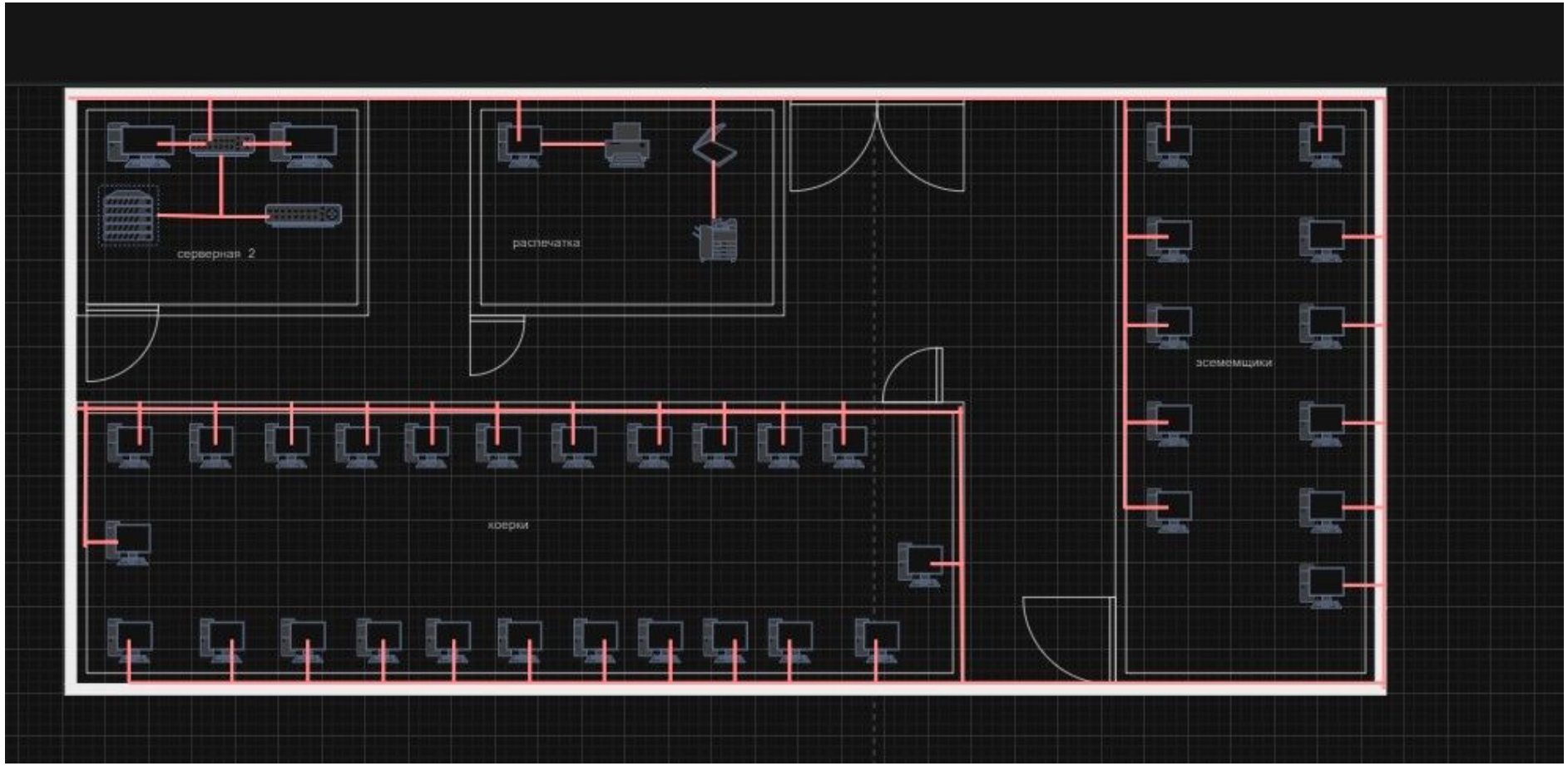


Схема первого и второго этажа четвертого филиала

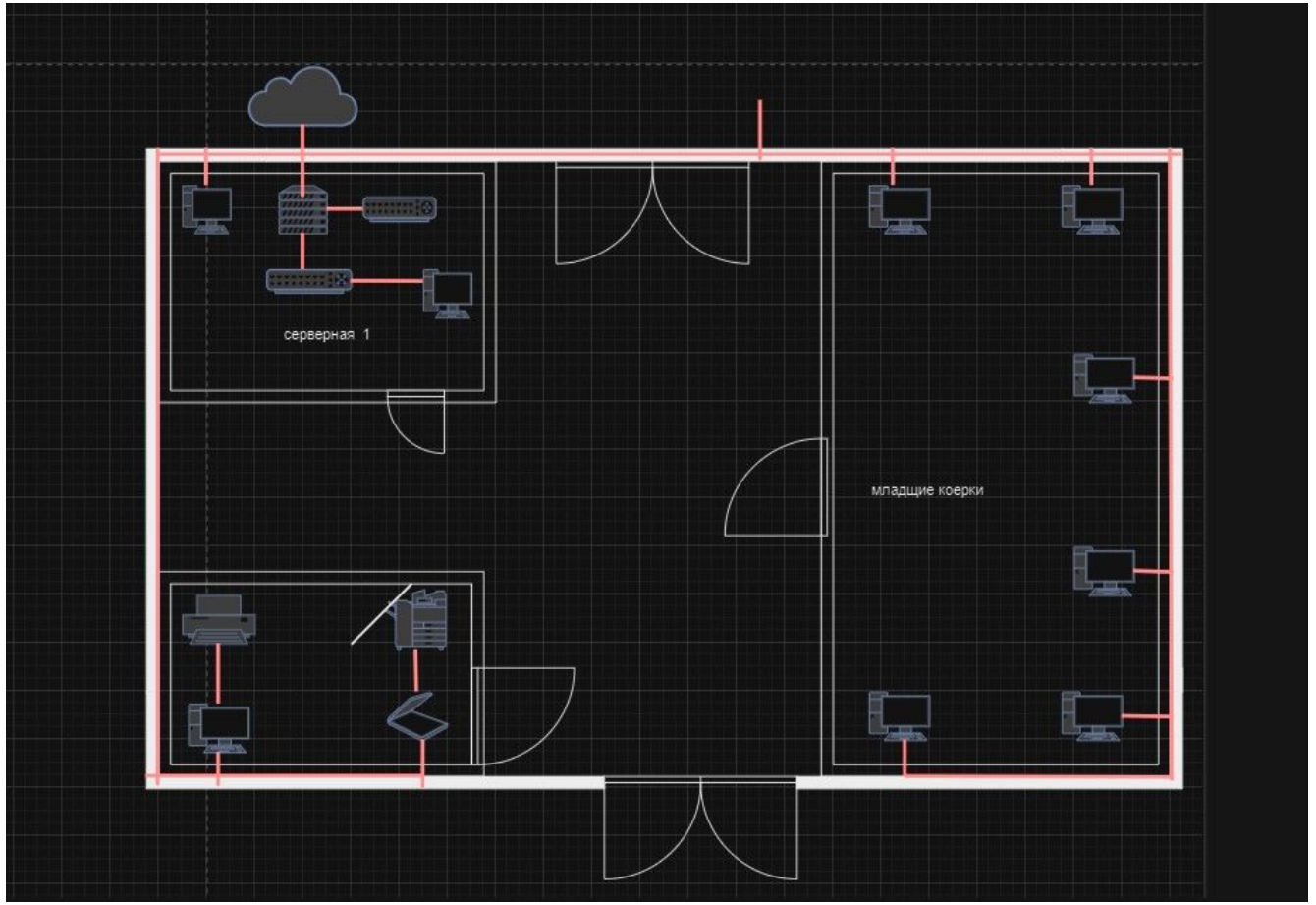
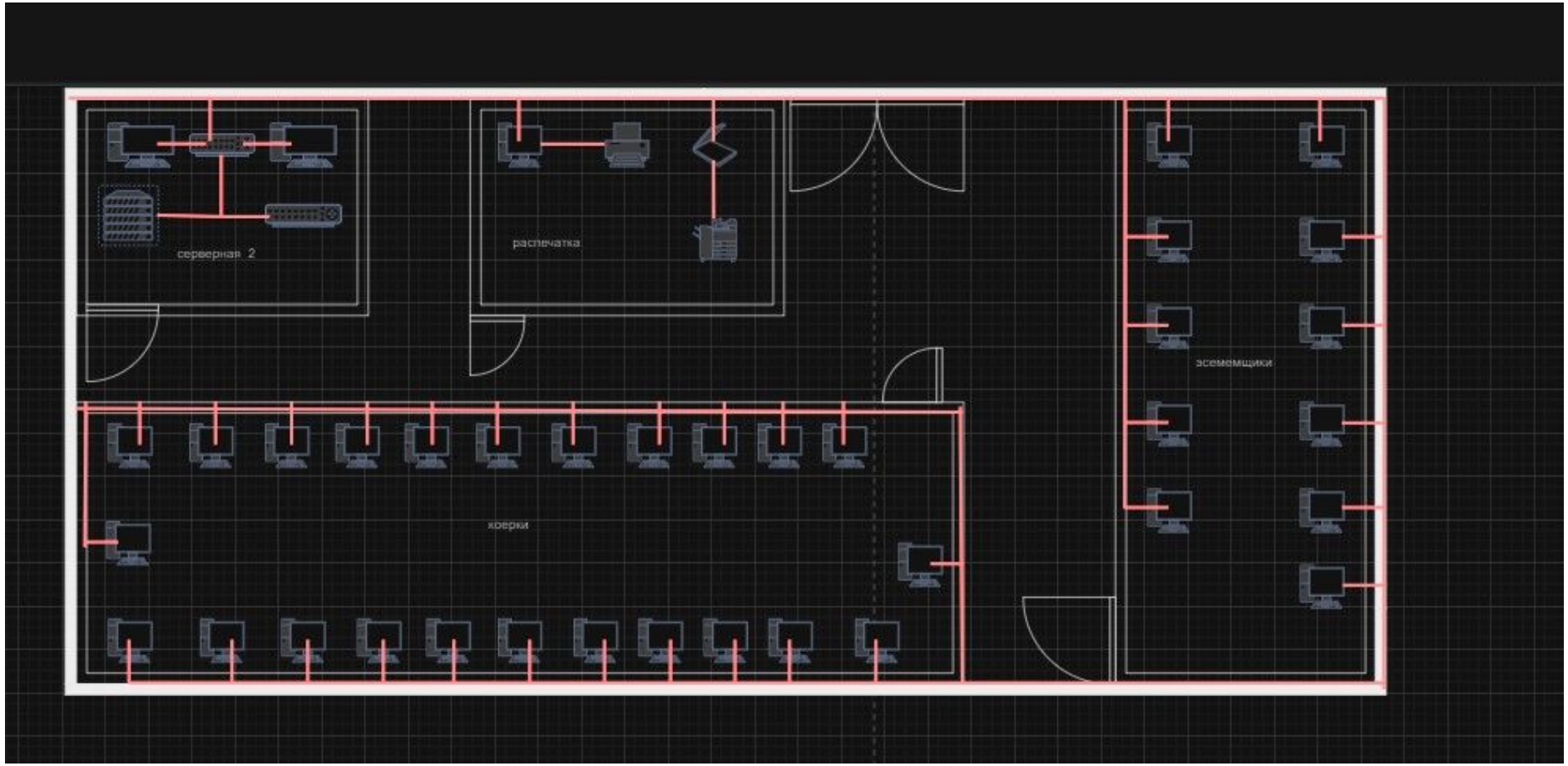


Схема первого
и второго этажа четвертого филиала



Ключевые характеристики компании "ИнтеллектТех"

- 1. Инновационные технологии: Фокус на разработке и внедрении передовых информационных технологий и продуктов.
- 2. Экспертность и профессионализм: Команда высококвалифицированных специалистов, способных предоставлять качественные услуги и продукты.
- 3. Гибкие решения: Способность предлагать клиентам гибкие и индивидуальные технологические решения, адаптированные под их потребности.
- 4. Ориентация на клиента: Сильное внимание к потребностям клиентов и стремление к удовлетворению их ожиданий.
- 5. Безопасность данных: Забота о защите конфиденциальности и безопасности информации клиентов.
- 6. Исследования и разработки: Возможно, компания активно инвестирует в научные исследования и разработку новых технологий.

15 угроз для сетей и их устранения

- 1. Вредоносное программное обеспечение (malware): Установите антивирусное программное обеспечение и удостоверьтесь, что оно регулярно обновляется. Обучайте пользователей, как избегать скачивания и открытия подозрительных файлов.
- 2. Фишинг и социальная инженерия: Обучайте пользователей распознавать подозрительные электронные письма и ссылки. Используйте электронную почту с фильтром спама.
- 3. DDoS-атаки: Используйте защитные механизмы, такие как межсетевые экраны, системы обнаружения вторжений (IDS) и системы обнаружения аномалий (IPS), чтобы обнаруживать и отражать атаки.
- 4. Слабые пароли: Инструктируйте пользователя создавать сложные пароли, используя комбинацию букв, цифр и специальных символов. Введите политику регулярного обновления паролей.
- 5. Несанкционированный доступ: Регулируйте доступ к сетевым ресурсам, разграничивайте права доступа и ограничивайте использование гостевых сетей.
- 6. Неактуальное программное обеспечение: Регулярно обновляйте операционные системы, приложения и устройства сетевой инфраструктуры, чтобы устранить известные уязвимости.
- 7. Межсетевые шлюзы и фильтрация трафика: Внедряйте межсетевые экраны и применяйте фильтры трафика для блокировки подозрительных или нежелательных пакетов.
- 8. Несанкционированный доступ к беспроводным сетям: Обеспечьте безопасность Wi-Fi сети с помощью шифрования (например, WPA2) и используйте авторизацию с применением сильных паролей.

15 угроз для сетей и их устранения

- 9. Управление устройствами в сети: Ограничьте физический доступ к сетевым устройствам, используйте механизмы аутентификации и шифрования для защиты управляющего трафика.
- 10. Неавторизованное использование ресурсов: Используйте механизмы аутентификации, авторизации и учета доступа, чтобы предотвратить несанкционированное использование ресурсов сети.
- 11. Внутренние угрозы: Реализуйте контроль доступа и мониторинг действий пользователей, чтобы выявлять и предотвращать внутренние угрозы.
- 12. Отсутствие резервного копирования данных: Регулярно создавайте резервные копии данных и проверяйте их целостность. Храните резервные копии в отдельном и защищенном хранилище.
- 13. Отказ в обслуживании (DoS): Используйте средства защиты от DDoS-атак. Оптимизируйте сетевую инфраструктуру, чтобы снизить вероятность DoS-атаки.
- 14. Недостаточный мониторинг сетевой активности: Реализуйте системы мониторинга, которые могут обнаруживать аномальную активность сети и предупреждать о ней.
- 15. Передача данных через незащищенные каналы: Используйте шифрование (например, протокол SSL/TLS) для защиты передачи конфиденциальных данных через сеть.

План после аварийного восстановления

- 1. Оценка ущерба: Определите масштаб проблемы, проанализируйте повреждения и определите приоритеты восстановления.
- 2. Уведомление: Свяжитесь с соответствующими заинтересованными сторонами, такими как сотрудники, поставщики услуг и клиенты, чтобы сообщить о проблеме и предоставить информацию о плане восстановления.
- 3. Анализ причины: Определите, что стало причиной сбоя или аварии. Это может потребовать анализа журналов событий, диагностики оборудования или экспертной оценки.
- 4. Изоляция и устранение проблемы: Изолируйте поврежденную секцию сети, проверьте и восстановите подключения и оборудование, исправьте программные ошибки или замените неисправное оборудование.
- 5. Восстановление услуг: Восстановите функциональность сети и восстановите связность между узлами. Это может включать запуск резервных систем, восстановление системных настроек или восстановление данных.
- 6. Тестирование и проверка: Проверьте работу сети, протестируйте функциональность и убедитесь, что все восстановлено и работает должным образом.
- 7. Обучение и документация: Обучите сотрудников по новым процедурам и изменениям в сети в результате восстановления. Обновите документацию и инструкции по восстановлению.
- 8. Пост-аварийный анализ: Проанализируйте непредвиденные события и их последствия, чтобы выявить уязвимости и предпринять меры для предотвращения или снижения рисков в будущем.