Контрольный лист аудита ит-инфраструктуры

1. Инвентаризация компонентов IT-инфраструктуры:

1.1. Сервера ☐

1.1.1. ОС_____ назначение: _____

1.1.2. ОС_____ назначение:_____

1.1.3. ОС_____ назначение:_____

1.2. Анализ достаточности ресурсов серверного оборудования выполняемым задачам:

переизбыток ресурсов ☐

недостаточность ресурсов ☐

соответствует выполняемым задачам ☐

1.3. Количество рабочих станций _____шт. Из них:

1.3.1. Win xp _____ шт.

1.3.2, Win 7_____ шт.

1.3.3. Win 8_____ шт.

1.3.3. *unix _____ шт.

1.4. Активное сетевое оборудование ☐

Коммутаторы ☐:	Маршрутизаторы ☐:
Модель: _____	Модель: _____
Модель: _____	Модель: _____

1.5. Периферийное оборудование:

_____

_____

_____

1.5.1 Наличие сетевых принтеров/мфу ☐

2. Анализ Безопасности ИТ-инфраструктуры и ее элементов

2.1. Аудит информационной безопасности

2.1.1. вероятность преднамеренных угроз □

• анализ систем защиты от внешнего проникновения:

_____

_____

_____

•анализ возможных путей утечки информации внутри организации

_____

_____

_____

• несанкционированный доступ к информации □

• есть ли разграничение прав доступа к коммерческой информации / серверам □

• разграничение правд доступа в программных комплексах (1С) □

2.1.2. вероятность непреднамеренных (случайных) угроз □

потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации

• сбои и отказы оборудования □

• зависания компьютеров / серверов □

•нестабильная работа программ/ основного используемого софта □

2.1.3. Анализ системы хранения и резервирования данных:

•осуществляется ли резервное копирование □ Если да, то:

• как часто _____

• есть ли расписание _____

• дублирование информации: сосредоточенное / рассредоточенное (нужное подчеркнуть)

• шифрование важной коммерческой информации □

•анализ принципов межсетевого взаимодействия:

_____

_____

_____

•анализ существующих политик IP-адресации, IP-маршрутизации:

_____

_____

_____

2.2 Технические и программные средства

• наличие установленных антивирусов □

•из них работающих и обновленных _____

• файерволы / сетевые экраны □ _____

• установленные источнки бесперебойного питания □

• устойчивость технических средств к всевозможным отказам и сбоям □

• анализ организации системы бесперебойного электропитания

_____

_____

_____

2.3. Обслуживающий персонал и пользователи

• возникают ли ошибки пользователей и/или обслуживающего персонала □
• аутентификация пользователей □
• Ошибочные операции или действия пользователей, допускающие отказы аппаратных и программных средств □
Если да, то какого плана: _____

3. Заключение

•проверка сетевой безопасности серверов и рабочих станций с целью исключения возможного несанкционированных проникновений через сеть Интернет и/или по другим каналам связи показала *возможность / невозможность* (нужное подчеркнуть) угроз с внешнего мира.

•диагностика системы электроснабжения, кабельных сетей и пассивных компонентов IT-инфраструктуры предприятия показала вероятность *отказа /не отказа* выхода оборудования из строя.

•полезная эффективность IT-инфраструктуры организации (соответствие технических и программных средств предприятия реальным целям, задачам и потребностям бизнеса)
•информационная безопасность IT-инфраструктуры предприятия (включая устойчивость технических средств к всевозможным отказам и сбоям, а также обеспечение сохранности важной информации: пресечение ее утечки и/или уничтожения и защита от несанкционированного доступа)

Для блокирования (парирования) случайных угроз безопасности информации в компьютерных системах должен быть решен комплекс задач:

•дублирование информации
•повышение надежности системы
•создание отказоустойчивых систем
•минимизация ущерба от аварий и стихийных бедствий
•блокировка ошибочных операций
•оптимизация взаимодействия человека и компьютерной системы