Техническое задание

на проведение аудита безопасности ИТ-инфраструктуры

1. Общая информация

Требуется провести аудит безопасности ИТ-инфраструктуры пяти тепличных комбинатов:

- ТКН — Тепличный комбинат Новосибирский;
- ТКТ — Тепличный комбинат Толмачевский;
- ТКЕ — Тепличный комбинат Емельяновский;
- ТКО — Тепличный комбинат Обской;
- ТКА — Тепличный комбинат Алтайский.

Комбинаты связаны между собой корпоративными каналами связи и используют общие информационные системы и сервисы.

В инфраструктуре используются Windows и Linux, системы виртуализации, 1С, СУБД, системы резервного копирования, сетевое оборудование и VPN.

Перечень сетей, внешних адресов, основных серверов и систем будет предоставлен перед началом работ.

Инвентаризация инфраструктуры в рамках аудита не требуется.

2. Цель аудита

Цель работ — выявить уязвимости, которые могут привести к получению несанкционированного доступа к корпоративным системам, серверам и данным.

В первую очередь требуется оценить:

- возможность проникновения во внутреннюю сеть с внешнего периметра;
- возможность повышения прав после получения доступа к рабочей станции или обычной пользовательской учётной записи;
- доступ к серверным сегментам;
- возможность перехода между сетями комбинатов;
- доступ к 1С и базам данных;
- доступ к системам резервного копирования;
- ошибки настройки серверного и сетевого оборудования, которые могут быть использованы при атаке.

Основной результат аудита должен показывать не только наличие отдельных уязвимостей, но и возможность их практического использования.

3. Внешний периметр

Проверить предоставленные Заказчиком внешние IP-адреса, доменные имена и опубликованные сервисы.