**ТЕХНИЧЕСКОЕ ЗАДАНИЕ ДЛЯ МОДУЛЯ А**

Необходимо провести установку и настройку отечественного инфраструктурного программного обеспечения для нескольких филиалов предприятия N. В состав инфраструктуры входят программные и программно-аппаратные комплексы следующих отечественных вендоров: Группа Астра, ИнфоТеКС, РЕД Софт, Базальт СПО, КиберПротект, Элтекс.

Руководство компании N предоставляет Вам максимальный допуск для выполнения работ по настройке и защите корпоративной ИТ-инфраструктуры.



Руководством компании N было принято решение воспользоваться отечественным средством виртуализации в рамках основной виртуализации – ISP VMmanager. Вся инфраструктуры компании должна функционировать на вышеуказанной виртуализации, за исключением отдельных филиалов.

Доступ к виртуализации: manager:xxXX.1234 ;
manager@ib-sec.org:xxXX.1234

Филиал Центральный – основное средство виртуализации.

Филиал Уральский – средство виртуализации РЕД Виртуализация.

Филиал Дальневосточный – средство виртуализации Альт Виртуализация.

**ПРОГРАММНО- И ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ ФИЛИАЛОВ**

**Центральный филиал должен включать в себя следующие средства защиты:**

* Защищенный сетевой координатор – С1
* Защищенный сетевой фаервол – FW1
* Защищенный сетевой маршрутизатор – R1
* Средства мониторинга IDS (TIAS, NS, MC, HS)
* Средства защиты EP/SP (Endpoint/Safepoint)

**Основной филиал использует аппаратное и программное обеспечение компании ПАО Группа Астра:**

* Программный комплекс централизованного управления компьютерам – ALD Pro
* Защищенные рабочие места на базе отечественной ОС – Astra Linux Special Edition 1.8

**Уральский филиал должен включать в себя следующие средства защиты:**

* Защищенный сетевой координатор – С2
* Защищенный сетевой фаервол – FW2
* Защищенный сетевой маршрутизатор – R2

**Уральский филиал использует аппаратное и программное обеспечение компании ООО РЕД СОФТ:**

* Программный комплекс централизованного управления компьютерам – РЕД АДМ
* Защищенные рабочие места на базе отечественной ОС – РЕД ОС 8

**Дальневосточный филиал должен включать в себя следующие средства защиты:**

* Защищенный сетевой координатор – С3
* Защищенный сетевой фаервол – FW3
* Защищенный сетевой маршрутизатор – R3

**Дальневосточный филиал использует аппаратное и программное обеспечение компании ООО БАЗАЛЬТ СПО:**

* Защищенные рабочие места на базе отечественной ОС – Альт Рабочая станция К

**СЕТЕВАЯ ИНФОРМАЦИЯ И РЕГЛАМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Требования к сетевой инфраструктуре каждого филиала:

|  |  |  |
| --- | --- | --- |
| Подсеть | Шлюз | Доп. информация |
| /24 | \*.\*.\*.1/24 | Автоматическая настройка для раздачи и получения сетевых адресов. Разграничение сетей по VLAN рекомендована, но необязательна.Доступность сетевых устройств между филиалов должна проверяться с помощью отправки ICMP-пакетов (ограничения для прохождения данных пакетов должны быть сняты) |

Требования к безопасности выражается установкой сложных паролей (xxXX.1234) для всех устройств филиалов, а также установкой средств резервного копирования компании ООО Киберпротект на пользовательские устройства.

Для устройств с возможностью ограничения трафика (FW) должны быть установлены политики, запрещающие использование следующих сайтов: vk.com, youtube.com, ok.ru, google.ru.

Для каждого возможного устройства должен быть разрешен доступ до веб-интерфейса для упрощения взаимодействия.

Между филиалами должно быть установлено VPN-соединение с помощью средств защиты компании АО ИнфоТеКС.

**АВТОМАТИЗАЦИЯ ДЕЙСТВИЙ**

При использовании комплексов централизованного управления компьютерами необходимо: реализовать возможность распределения настроек на доменные устройства. За доменные устройства принять защищенные рабочие места конкретного филиала.

**ИНФОРМАЦИЯ ПО ВИРТУАЛИЗАЦИИ**

|  |  |
| --- | --- |
| РЕД Виртуализация | Режим standalone |
| Альт Виртуализация | PVE, nginx |