**Практика**

Предлагаю теперь взглянуть на нашу схему с точки зрения технической стороны менеджмента информационной безопасности.

Необходимо решить следующие задачи:

1. Защита внешнего периметра.
2. Защита внутренних сетевых сервисов и информационных обменов.
3. Защита серверов и рабочих станций.
4. Защита информационной инфраструктуры удаленных офисов.
5. Защита системных ресурсов и локальных приложений на серверах и рабочих станциях.
6. Защита выделенных сегментов и интеграционных туннелей.
7. Защита чувствительной информации всех компонентов IT-ландшафта.

Исходя из вашей методички и тех знаний, которые вы получили на сегодняшнем уроке, я предлагаю вам сделать 10 минутный тест и направить его мне почтовым сообщением.

Формат теста:

|  |  |  |
| --- | --- | --- |
|  | **ФИО студента: Глинника Дмитрия Вячеславовича** | |
| **№** | **Направления менеджмента** | **Возможные инструменты реализации\рекомендации по применению** |
| 1 | Защита внешнего периметра | Межсетевые экраны/NGFW/WAF (FortiGate, Sophos, Paloalto) Антиспам. APT |
| 2 | Защита внутренних сетевых сервисов и информационных обменов | Сегментация сети. Пентесты. Сканеры безопасности. APT, SIEM |
| 3 | Защита серверов и рабочих станций | Антивирусы, брандмауэры. Сканеры безопасности операционных систем. DLP. |
| 4 | Защита информационной инфраструктуры удаленных офисов | Защищенные каналы связи, файрволлы.  Антивирусы на конечных узлах. WAF |
| 5 | Защита системных ресурсов и локальных приложений на серверах и рабочих станциях | Сканеры безопасности приложений. Антивирус. |
| 6 | Защита выделенных сегментов и интеграционных туннелей | WAF, более глубокая настройка сетевого оборудования для контроля трафика. Мониторинг. Сканеры уязвимостей. |
| 7 | Защита чувствительной информации всех компонентов IT-ландшафта | DLP, IDM, разграничения прав доступа |