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: Лешков И.А.	
№	**Направления менеджмента**	**Возможные инструменты реализации\рекомендации по применению**
1	Защита внешнего периметра	Межсетевые экраны(FW) и граничные маршрутизаторы, VPN, а также IDS\IPS
2	Защита внутренних сетевых сервисов и информационных обменов	DLP, WAF, Антивирусное ПО, SIEM.
3	Защита серверов и рабочих станций	Антивирусное ПО, WAF, Сканеры уязвимостей.
4	Защита информационной инфраструктуры удаленных офисов	WAF с VPN сервисом на борту, реверс-прокси, Антивирусное ПО (веб-антивирус, почтовый антивирус)
5	Защита системных ресурсов и локальных приложений на серверах и рабочих станциях	WAF, Антивирусное ПО, Сканеры уязвимостей, APT
6	Защита выделенных сегментов и интеграционных туннелей	WAF, APT, Сканеры уязвимостей.
7	Защита чувствительной информации всех компонентов IT-ландшафта	DLP. Автоматический перехват и анализ информации, разграничение прав доступа, и.т.д.