**Практика**

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

Необходимо решить задачу рационального использования рассмотренных на уроке инструментов.

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 Д.В.** | |
| **№** | **Наименование средства защиты** | **Цели, прикладное размещение и необходимость использования** |
| 1 | SIEM | Система сбора информации для прогнозирования угроз. Взаимодействует с почтовыми сервера, антивирусами, файловыми ресурсами и др. Помогает выявить кибератаки и нарушения политик безопасности на ранних стадиях и минимизировать ущерб от них. |
| 2 | SOAR | Дополнение к SIEM системам, SOAR-системы рассчитаны на автоматизацию и оркестровку работы нескольких различных систем информационной безопасности |
| 3 | IPS | Система предотвращения вторжений. Система исследует сетевой трафик, потоки для обнаружения и предотвращения эксплойтов. |
| 4 | IDS | Система обнаружения вторжений. IDS мониторит трафик в различных точках сети и дает понимание того, насколько хорошо обстоят дела с точки зрения защищенности. |
| 5 | Инструменты защиты от НСД | Технические средства, позволяющие предотвратить попытки несанкционированного доступа, такие как неавторизованный физический доступ, доступ к файлам, хранящимся на компьютере, уничтожение конфиденциальных данных. |