Практика

Предлагаю теперь взглянуть на нашу 2 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: Лешков И.А.	
№	**Наименование мер защиты**	**Цели, прикладное размещение (вектор эксплуатации) и необходимость использования**
1	Применение СКЗИ	Данные средства применяются для защиты ПДн, чувствительной информации, а также для шифрования данных предаваемых по различным каналам связи. Необходимость очень велика, так как в открытом виде вышеупомянутая инфа находиться никак не может в современных реалиях.
2	Подключение SOC центра	Данные центры – это достаточно мощный инструмент для комплексного мониторинга и контроля, а также реагирования на события, связанные с ИБ. В современном мире просто необходимы для обеспечения непрерывности бизнеса, так как чётко отлаженный и функционирующий SOC, позволит эффективно и своевременно реагировать на события ИБ, а также управлять активами, уязвимостями и, в целом, рисками, связанными с ИБ.
3	Обеспечение процесса пентестинга	Это очень важный инструмент для анализа защищенности всей бизнес-системы. Имитация возможных атак извне абсолютно разными способами и, с применением различный векторов и техник (агрессивное/пассивное сканирование, прослушивание сетевого траффика, закрепление в системе через внедрение эксплоитов или вредоносов, и.т.д.). Позволяет понять насколько хорошо защищена it-система, обнаружить дыры и закрыть их.
4	Использование анализаторов кода	Данные инструменты, позволяют идентифицировать и предотвратить эксплойты и ошибки (баги) в исходном коде. Очень хороши с точки зрения анализа кода и исправления критических ошибок, которые могу привести к формированию входов привлекательных для злоумышленника.

5	Необходимость подключения Anti-fraud	Очень важный инструмент для обеспечения безопасности финансовых операций в сети. Позволяет минимизировать риски, связанных с транзакциями ы выявит мошеннические действия в них. Необходимость абсолютно логично вытекает из того, подавляющее большинство операций по движению средств осуществляется в онлайне.