Практика

Предлагаю теперь взглянуть на нашу схему с точки зрения наличия IT-инноваций и выявить их.

Необходимо решить задачу идентификации возможных уязвимостей и предложить способы защиты.

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 технологии**	**Наличие в проекте, возможное использование, возможные уязвимости и способы защиты**
1	BigData	Касаемо схемы 7, наличие вполне резонно (крупная торговая площадка). Использовать для хранения, консолидации и обработки больших объемов данных, поступающих от клиентов. Риски нарушения конфиденциальности, потери данных, мошенничества, итд. Защита путём криптозащиты, гранулированного контроля доступа, мониторинга безопасности в режиме реального времени, итд.
2	NN, AI, machinelearning	Касаемо схемы 7, наличие не обнаружил, но, думаю вполне может быть, например, для распознавания легитимных клиентов. Риски нарушения целостности, доступности, итд. Как защиту, можно использовать кластеризацию входящего потока, создание устойчивой поведенческой модели, использование искусственного интеллекта, итд.
3	Web and mobile application	Касаемо схемы 7, логичное присутствие, так как данные обрабатываются, как с ПК, так и с мобильных устройств. Уязвимости из OWASP TOP TEN (XSS, Injection, XXE, broken authentication, etc…). Защита заключается в грамотной конфигурации компонентов приложения, серверов и баз данных, исключения поддержки внешних сущностей, обеспечения многофакторки, итд.
4	IoT	Касаемо схемы 7, наличие не указано, однако интернет вещей – это, наверное, неотъемлемая часть жизни и бытия человечества, и, несмотря на то, что в нашем проекте – виртуальный магазин и в основном облачные решения, но наличие операторов, администраторов, которые где-то располагаются, где могут быть различные смарт-устройства (камеры, умные колонки, итд.), то важно защитить данные узлы. Самая важная угроза – это перехват управления и угон чувствительной информации. Поэтому важно спроецировать IoT — архитектуру на плоский IT-ландшафт и реализовать стандартизованные правила обеспечения ИБ, в соответствии с best practice.

5	Cloud services	Касаемо схемы 7, то тут присутствуют облачные решения. Основные уязвимости связанны с утечкой и компрометацией данных, кражей учетных данных, целевыми и сетевыми атаками, итд. Как меры защиты здесь можно проводить пентестинг, обеспечение централизованного управления, создание облачных сервисов с учетом стандартизации и best practice, итд.
6	Виртуализация и контейнирезация	Касаемо схемы 7, здесь есть Docker, который содержит в себе сервер приложений RichCall. Существуют угрозы платформ виртуализации, уязвимости ядра, которые позволяют получить доступ ко всем контейнерам, управляемые ботсети, итд. Защита строится путём автоматизированной проверки уязвимостей контейнеров, обеспечения контроля доступа, использованием API, итд.