**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:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **№** | **Наименование технологии** | **Наличие в проекте, возможное использование, возможные уязвимости и способы защиты** |
| 1 | BigData | Применима для нашей схемы, т.к. у нас используется большой массив данных о клиентах, продуктах и пр. Риски мошенничества, потери данных, нарушения конфиденциальности. Периодические мониторинги и аудиты. |
| 2 | NN, AI, machinelearning | Думаю для данной схемы применимо использование нейросетей для проведения пентестинга, используя социальную инженерию, анализ вредоносного кода, поиск уязвимостей. В качестве защиты можно использовать кластеризацию входящих потоков данных. |
| 3 | Web- and mobile application | Мастхэв для нашей системы, т.к. в ИС используются мобильные устройства и компьютеры. Возможны атаки XSS, Broken Authentication, Sensitive Data Exposure и др. В качестве защиты используют криптографию и шифрование данных, экранирование данных, многофакторную аутентификацию. |
| 4 | IoT | На схеме не представлено. Но как вариант может быть какие-то терминалы по заказам, кассовые терминалы, камеры и др. Угроза получения доступа к управлению этими устройствами, перехват данных. В качестве защиты необходимо реализовать стандартизованные правила обеспечения ИБ в соответствии с best practiceю |
| 5 | Cloud services | Облачные системы используются в нашей ИС. Основные угрозы: целевые и сетевые атаки, кража учетных данных, взлом API интерфейсов. Для защиты использовать пентестинг и создание сервисов с учетом стандартизации и best practice. |
| 6 | Виртуализация и контейнирезация | В нашей ИС используется контейнеризация через Docker. Существуют угрозы атак на гипервизоры среды виртуализации и виртуальные диски. Для защиты следует обеспечивать безопасность виртуальных сетей, гипервизоров, изолированных данных. |