

Как мы убеждались ранее, данная схема состоит из 4 зон. Есть внешняя сеть с пользователями мобильных устройств и подрядчиком. Подобные подключения должны быть максимально ограничены настройками сетевого оборудования, WAF, IPS и прочими сервисами.

В соответствии с законодательством РФ (149, 152 ФЗ) и международными стандартами ISO 27k необходимо наложить соответствующие требования к ИС (установить файерволлы, антивирусы, системы DLP и пр.)

Все события должны собираться в единой системе SIEM для последующей обработки информации для прогнозирования угроз. В дополнение система поможет выявить кибератаки и нарушения политик безопасности.

В инсайде не забываем развернуть сервер резервного копирования, тем более у нас там есть боевые БД.

Периодические мониторинги, пентесты и нагрузочные тестирования защищенности придадут нам уверенности, спокойствия и здоровый сон. 😊