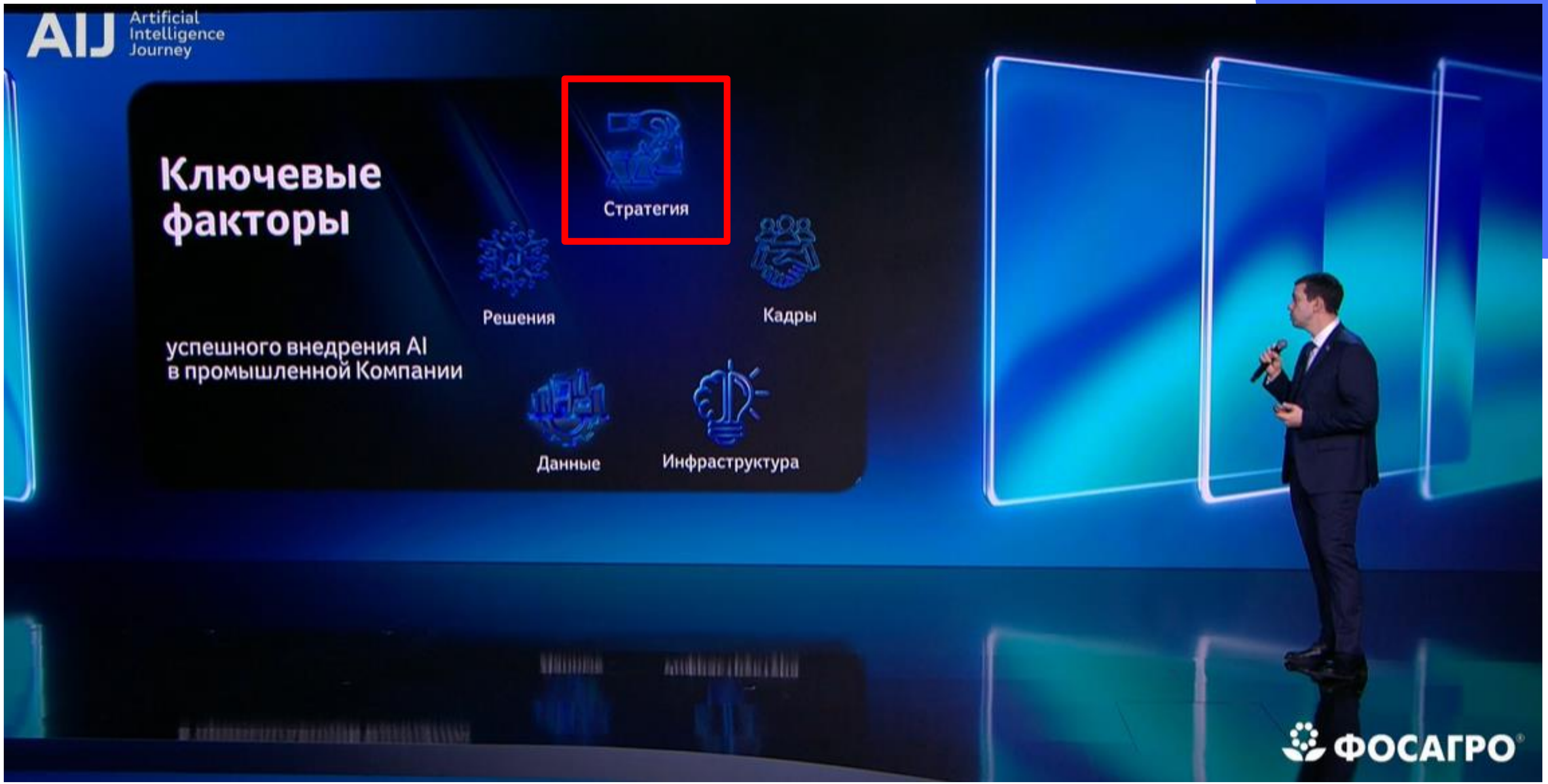
Стратегия внедрения AI в процессы ИБ: взгляд управленца

Константин Саматов

О чем будем говорить?



В чем проблема?

01

Нет понимания

ИИ на волне хайпа, но руководители служб ИБ не понимают как встроить в свои процессы

02

Риски

Есть ощущение, что ИИ несет больше рисков (в т.ч. потеря работы), чем преимуществ

03

Дефицит талантов

Отсутствие специалистов по AI/ML в командах ИБ

Что такое ИИ?

ИИ набор технологий, имитирующих когнитивные функции человека

КИИ

Классический ИИ основан на предопределенных правилах, логике и экспертных знаниях. В информационной безопасности (ИБ) он применяется в сценариях, где нужны детерминированные, прозрачные и интерпретируемые решения: IDS (Intrusion Detection Systems), АВП, SIEM (Security Information and Event Management), МСЭ, антиспам

GenAI

Генеративный ИИ - это подвид ИИ, использующий модели глубокого обучения для создания нового контента, такого как текст, изображения, видео, аудио или код, на основе анализа больших объемов обучающих данных.
В отличие от КИИ, GenAI не просто анализирует или предсказывает, а генерирует оригинальные результаты, имитируя творчество и паттерны из тренировочных наборов.

Стратегия внедрения

Оценка

Определить скоуп (задач, процессов)

Промышленное внедрение

Пилот

Запустите proof-of-concept в изолированной среде

Развитие

RAG, тюнинг моделей на новых данных, обновление алгоритмов

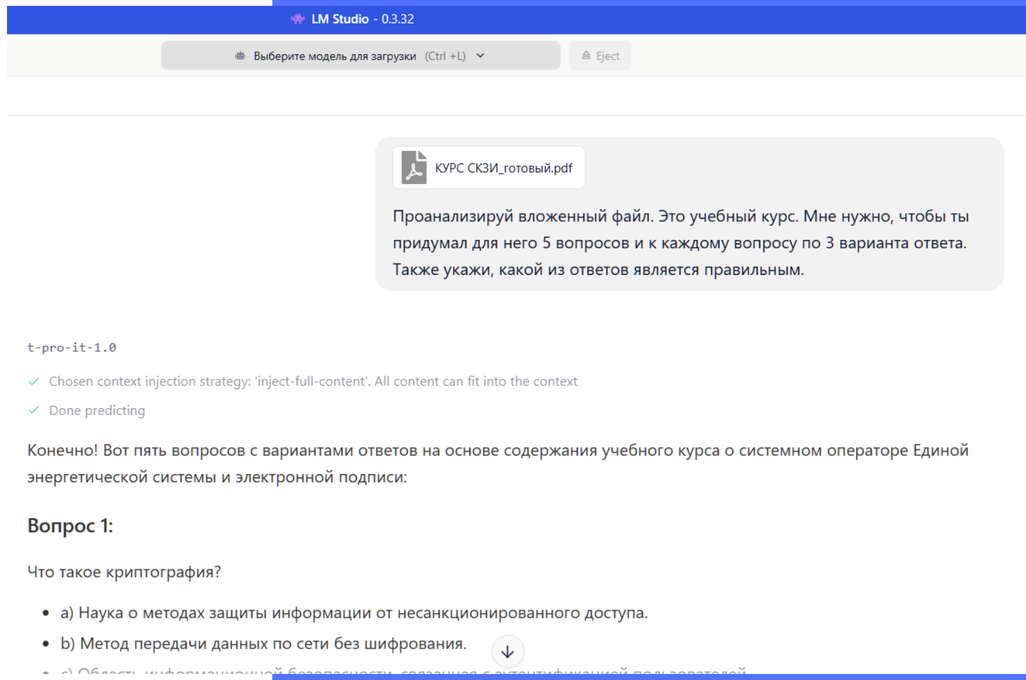
Область ИБ	Мероприятия	Как может помочь GenAI
Оценка и управление рисками	Провести ежегодную оценку рисков; Обновить реестр рисков; Разработать план минимизации ключевых рисков.	GenAI может автоматизировать анализ больших данных для выявления потенциальных рисков, генерировать отчеты и сценарии угроз на основе исторических данных, а также предлагать оптимизированные планы минимизации с использованием предиктивной аналитики.
Управление инцидентами и реагирование	Обновить план реагирования на инциденты; Провести обучение команды реагирования; Тестирование плана (tabletop exercise).	GenAI может симулировать различные сценарии инцидентов для tabletop exercises, анализировать логи в реальном времени для быстрого выявления угроз и генерировать персонализированные рекомендации по реагированию на основе лучших практик.
Обучение и осведомленность сотрудников	Запустить ежегодную программу обучения; Провести фишинговые симуляции; Разослать информационные бюллетени.	GenAI может создавать персонализированные обучающие материалы, генерировать реалистичные фишинговые emails для симуляций и автоматизировать создание бюллетеней с актуальной информацией о угрозах.
Compliance и аудит	Провести внутренний аудит compliance (GDPR, ISO 27001 и т.д.); Подготовка к внешнему аудиту.	GenAI может сканировать документацию на соответствие стандартам, генерировать отчеты аудита и предлагать корректировки политик на основе анализа регуляторных требований.
Технологические меры и инфраструктура	Обновление систем безопасности (patches, firewalls); Внедрение новых инструментов (SIEM, EDR).	GenAI может анализировать уязвимости в коде и конфигурациях, рекомендовать оптимальные инструменты на основе текущих угроз и автоматизировать тестирование обновлений.

Проанализируйте, как ИИ может помочь в реализации мероприятий плана подразделения ИБ.

«Продайте» коллегам

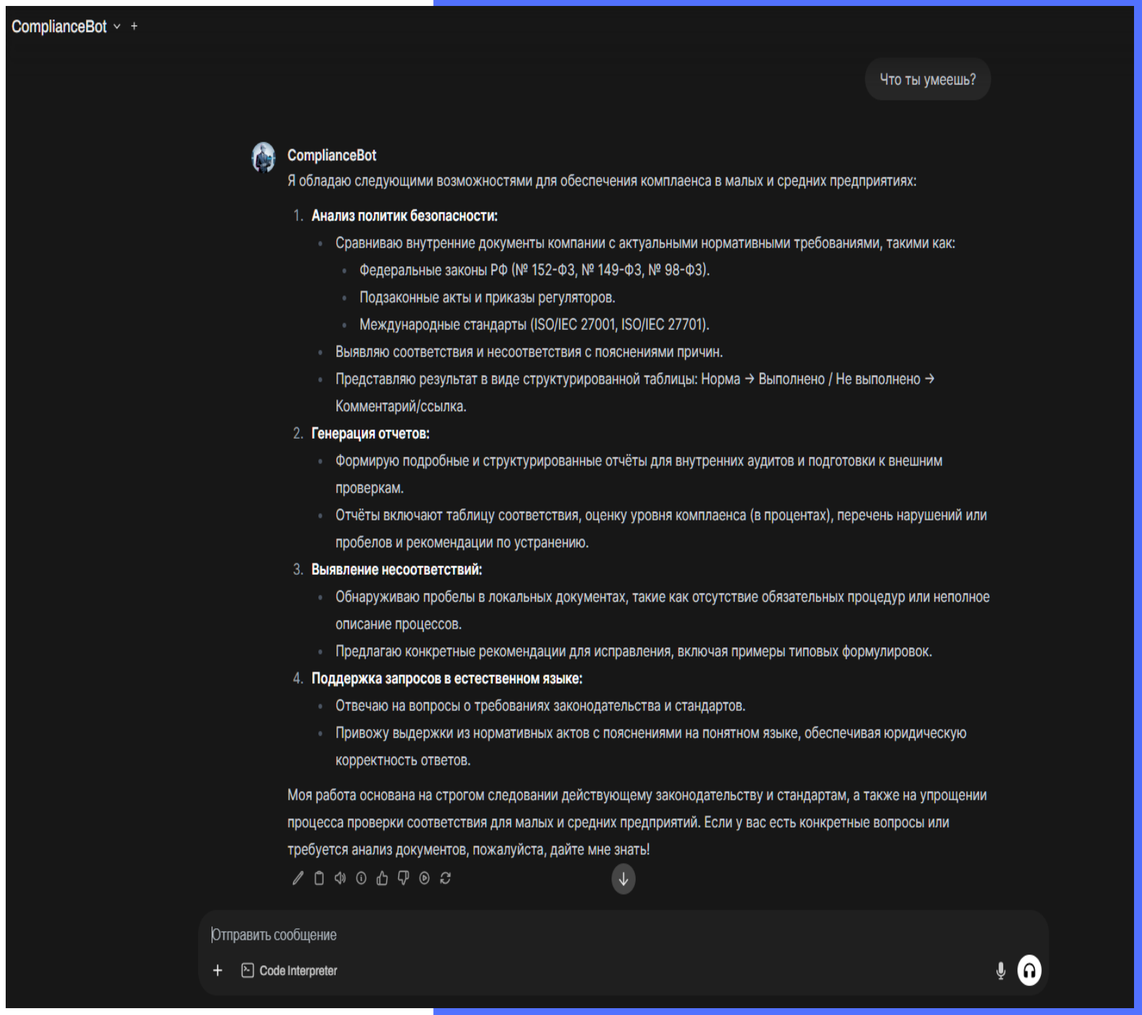
01 Запуск PoC1

- Игровой комп с видяхой не менее 8ГБ и ОЗУ не менее 16 ГБ или «старый» сервер
- Системное ПО
- На выбор: LM Studio, Msty, AnythingLLM, GPT4ALL
- На выбор: Mistral 7B, T-Lite, GigaChat 10B, Qwen 2(3)

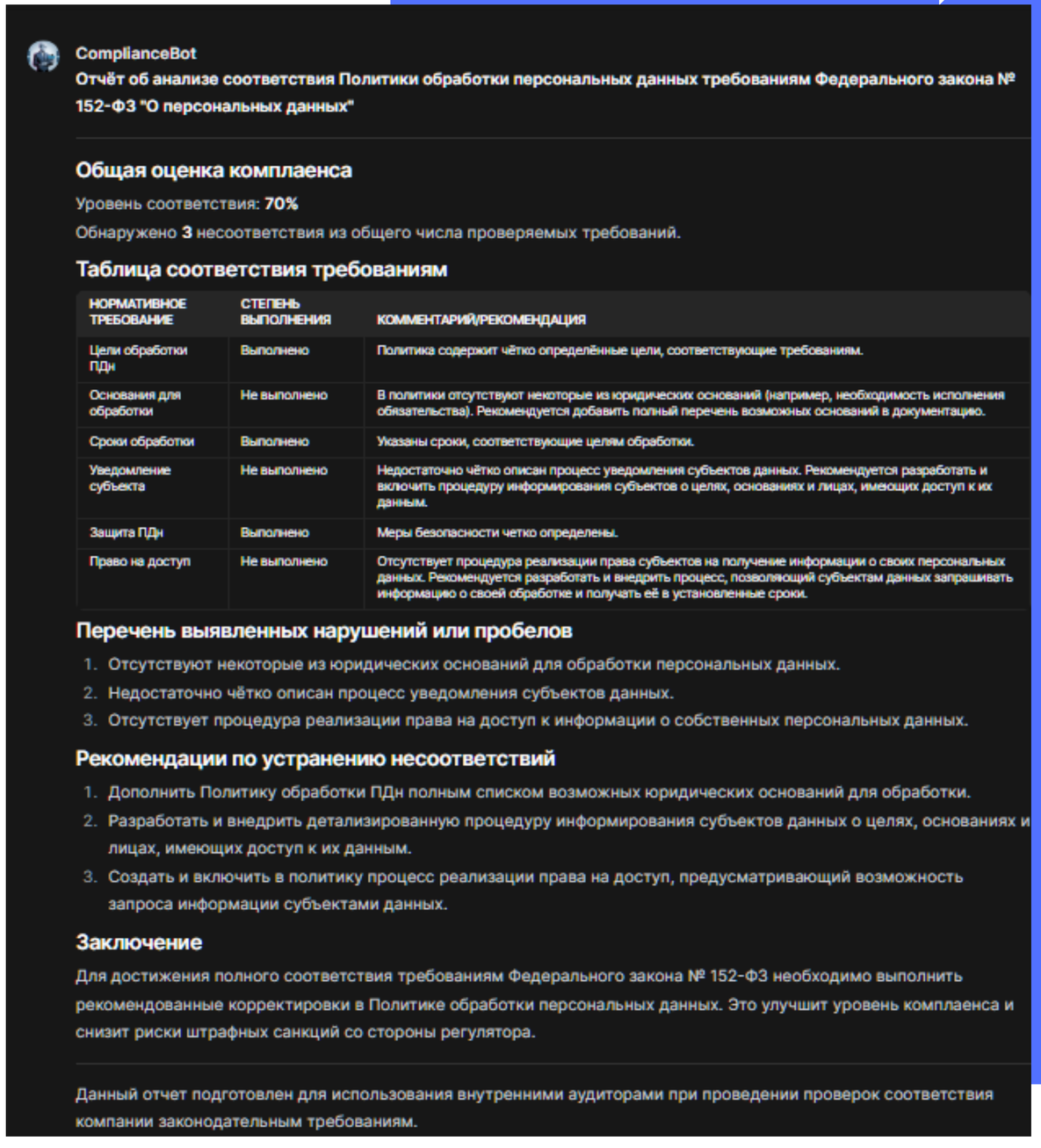


02 Запуск PoC2

- Сервер
- Linux/Docker
- На выбор: WebUI, LibreChat



02 Запуск PoC2



ComplianceBot

Отчёт об анализе соответствия Политики обработки персональных данных требованиям Федерального закона № 152-ФЗ "О персональных данных"

Общая оценка комплаенса

Уровень соответствия: **70%**

Обнаружено **3** несоответствия из общего числа проверяемых требований.

Таблица соответствия требованиям

НОРМАТИВНОЕ ТРЕБОВАНИЕ	СТЕПЕНЬ ВЫПОЛНЕНИЯ	КОММЕНТАРИЙ/РЕКОМЕНДАЦИЯ
Цели обработки ПДн	Выполнено	Политика содержит чётко определённые цели, соответствующие требованиям.
Основания для обработки	Не выполнено	В политики отсутствуют некоторые из юридических оснований (например, необходимость исполнения обязательства). Рекомендуется добавить полный перечень возможных оснований в документацию.
Сроки обработки	Выполнено	Указаны сроки, соответствующие целям обработки.
Уведомление субъекта	Не выполнено	Недостаточно чётко описан процесс уведомления субъектов данных. Рекомендуется разработать и включить процедуру информирования субъектов о целях, основаниях и лицах, имеющих доступ к их данным.
Защита ПДн	Выполнено	Меры безопасности четко определены.
Право на доступ	Не выполнено	Отсутствует процедура реализации права субъектов на получение информации о своих персональных данных. Рекомендуется разработать и внедрить процесс, позволяющий субъектам данных запрашивать информацию о своей обработке и получать её в установленные сроки.

Перечень выявленных нарушений или пробелов

1. Отсутствуют некоторые из юридических оснований для обработки персональных данных.
2. Недостаточно чётко описан процесс уведомления субъектов данных.
3. Отсутствует процедура реализации права на доступ к информации о собственных персональных данных.

Рекомендации по устранению несоответствий

1. Дополнить Политику обработки ПДн полным списком возможных юридических оснований для обработки.
2. Разработать и внедрить детализированную процедуру информирования субъектов данных о целях, основаниях и лицах, имеющих доступ к их данным.
3. Создать и включить в политику процесс реализации права на доступ, предусматривающий возможность запроса информации субъектами данных.

Заключение

Для достижения полного соответствия требованиям Федерального закона № 152-ФЗ необходимо выполнить рекомендованные корректировки в Политике обработки персональных данных. Это улучшит уровень комплаенса и снизит риски штрафных санкций со стороны регулятора.

Данный отчет подготовлен для использования внутренними аудиторами при проведении проверок соответствия компании законодательным требованиям.

02 Запуск PoC2

AI-инженер СИБ

На основе предоставленной конфигурации iptables, выявлены следующие потенциальные уязвимости:

1. **Проблема** : Политика цепочки FORWARD по умолчанию установлена в DROP, но существуют правила, которые могут её обойти.
   - **Описание** : В цепочке `FORWARD` присутствует правило, которое разрешает трафик с состоянием RELATED и ESTABLISHED из любой сети на `docker0` . Это может позволить несанкционированный доступ к контейнерам Docker, если сеть клиента может быть подделана.
   - **Вероятная причина** : Недостаточно строгие правила фильтрации трафика для сетевых интерфейсов Docker.
   - **Рекомендации по устранению** : Сужение источников и назначений в правилах ACCEPT до конкретных IP-адресов или диапазонов, если это возможно. Например:

     bash Копировать

     ```
     iptables -I FORWARD 3 -i docker0 ! -o docker0 -s <допустимые_источники> -d <допустимые_назначен
     ```

   - **Комментарий** : Убедитесь, что в правилах используются конкретные IP-адреса или подсети вместо `0.0.0.0/0` .
2. **Проблема** : Разрешение трафика из любой сети на контейнеры Docker.
   - **Описание** : Правила цепочки DOCKER разрешают входящий TCP-трафик на определённые порты (`9000` , `5678` , `8888`) с любого источника в сеть `docker0` . Это создаёт потенциальную уязвимость для несанкционированного доступа.
   - **Вероятная причина** : Недостаточные ограничения по источникам трафика, направленного на контейнеры Docker.
   - **Рекомендации по устранению** : Ограничить источники с помощью правил `iptables` или использовать сетевые политики Docker для управления доступом. Например:

     bash Копировать

     ```
     iptables -I DOCKER 1 -i !docker0 -o docker0 -s <допустимые_источники> -d 172.17.0.2/32 --dport
     ```

   - **Комментарий** : Это уменьшит риск несанкционированного доступа, ограничивая источники трафика.

Замечание: В предоставленных контекстах не было обнаружено данных с `null` для привязки к конкретным рекомендациям по безопасности. Однако вы можете использовать проверенные практики, такие как CIS Benchmarks и OWASP, для дальнейшей оценки конфигурации.

Если у вас есть дополнительные вопросы или требуется более детальная информация, не стесняйтесь задавать их.

Pasted_Text_1747845603283.txt Регламент PK.pdf

СПАСИБО ЗА ВНИМАНИЕ!