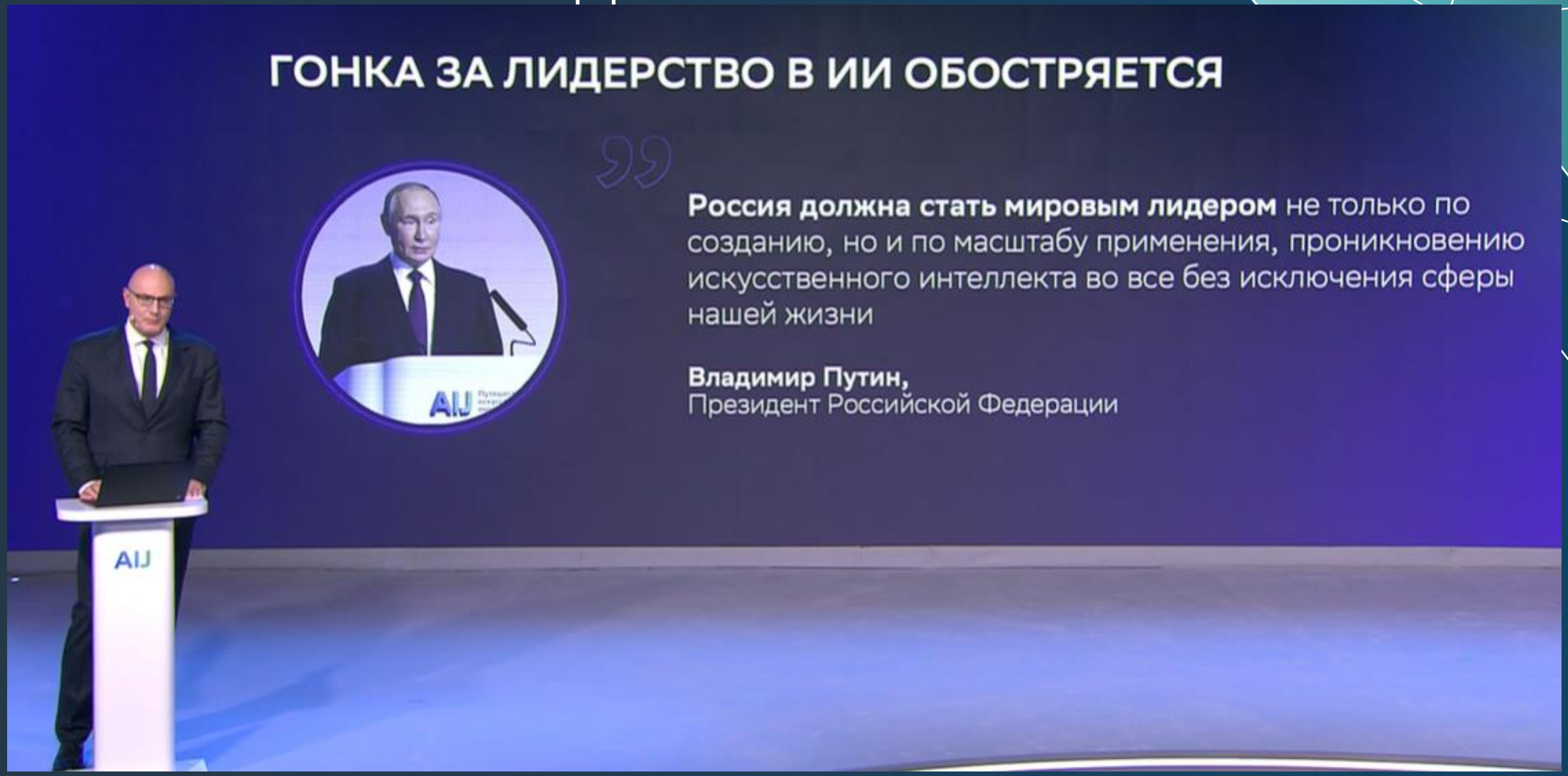
Применение инструментов AI в деятельности старшего офицера по ИБ (CISO)

Константин Саматов

Усиленные люди



Скрин с трансляции конференции AIJourney

Ключевые обязанности CISO

Разработка стратегии ИБ. Что помогает?

Большие языковые модели (LLM) — это тип нейросетей, которые обучены на огромных объемах текстовых данных для понимания и генерации естественного языка. Они способны предсказывать последовательность слов и генерировать текст, который выглядит как написанный человеком

Примеры сервисов:

- Зарубежные: ChatGPT от OpenAI, Claude от Anthropic, Mistral AI, Hauilo AI
- Отечественные: Yandex GPT от Яндекса, Giga Chat от Сбера

Разработка стратегии ИБ. Как помогает?

ChatGPT

Действуй как эксперт в области информационной безопасности. Я являюсь руководителем службы информационной безопасности в компании. Компания небольшая, около 500 рабочих мест. Ранее в этой компании небыло службы информационной безопасности, вопросами информационной безопасности занимались разные подразделения на несистематической основе. Разработай мне стратегию информационной безопасности. Сделай это в формате таблицы

Стратегия информационной безопасности компании (формат таблицы)

Этап	Описание	Срок реализации	Ответственные	Результат
1. Анализ текущего состояния				
Провести аудит инфраструктуры	Инвентаризация IT-систем, данных, процессов. Определение	1 месяц	Служба ИБ совместно с IT	Отчет об аудите, список активов, уязвимостей и критичных систем.

Разработка стратегии ИБ. Как помогает?

2. Разработка политики ИБ				
Разработка политики ИБ	Создание политики, описывающей цели, принципы, и ключевые правила ИБ в компании.	2 недели	Служба ИБ	Утвержденная политика ИБ.
Разработка регламентов	Создание регламентов управления доступом, реагирования на инциденты, резервного копирования.	1 месяц	Служба ИБ	Набор утвержденных регламентов.
3. Организационные меры				
Формирование структуры службы ИБ	Назначение сотрудников, распределение обязанностей, создание плана работы.	1 месяц	Руководство компании, Служба ИБ	Сформированная структура службы ИБ.

Разработка стратегии ИБ. Как помогает?

2. Разработка политики ИБ		**4. Технические меры**			
Разработка политики ИБ	Создание п описываю принципы, правила ИБ компании.	Внедрение базовой защиты	Установка антивирусов, межсетевых экранов, систем обнаружения вторжений (IDS/IPS).	3 месяца	IT-отдел, Служба ИБ	Реализована базовая защита.
Разработка регламентов	Создание р управлени реагирова инциденты копирова	Управление обновлениями	Внедрение автоматизированного процесса обновления ПО и ОС.	2 месяца	IT-отдел	Процесс обновления настроен.
3. Организационные меры		Многофакторная аутентификация	Внедрение MFA для критичных систем и доступа к корпоративной сети.	2 месяца	IT-отдел	Установлена многофакторная аутентификация.
Формирование структуры службы ИБ	Назначени сотрудник распредел обязанност плана рабо	**5. Обучение сотрудников**			
		Разработка программы обучения	Обучение основам ИБ, противодействию социальным	1 месяц	Служба ИБ, HR	Утвержденная программа обучения.

Разработка стратегии ИБ. Как помогает?

Действуй как эксперт в области информационной безопасности. Я являюсь руководителем службы информационной безопасности в компании. Компания небольшая, около 500 рабочих мест. Ранее в этой компании небыло службы информационной безопасности, вопросами информационной безопасности занимались разные подразделения на несистематической основе. Разработай мне стратегию информационной безопасности.

Разработка стратегии информационной безопасности для небольшой компании требует комплексного подхода, который учитывает особенности бизнеса, риски и доступные ресурсы. Вот пошаговый план создания такой стратегии:

Шаг 1: Оценка текущего состояния

Прежде чем разрабатывать стратегию, необходимо понять текущее положение дел в вашей компании относительно информационной безопасности. Это включает:

- **Анализ инфраструктуры**: Определить используемые системы, сети, приложения и устройства.
- **Оценка существующих мер защиты**: Выяснить, какие меры уже применяются (антивирусы, брандмауэры, политики паролей и т.п.).
- **Выявление уязвимостей**: Провести аудит систем на предмет возможных слабых мест.
- **Определение рисков**: Понять, какие угрозы наиболее актуальны для вашего бизнеса (например, утечка данных, кибератаки, человеческий фактор).

Шаг 2: Определение целей и приоритетов

На этом этапе важно сформулировать конкретные цели и приоритеты, которых вы хотите достичь через внедрение стратегии информационной безопасности. Например:

- Обеспечение конфиденциальности, целостности и доступности информации.
- Минимизация финансовых потерь от инцидентов.
- Соответствие законодательным требованиям (например, ФЗ-152 «О персональных данных»).
- Повышение осведомленности сотрудников о вопросах информационной безопасности.

Шаг 3: Разработка политик и процедур

Создание четких политик и процедур является основой любой успешной программы информационной безопасности. Вам нужно разработать следующие документы:

- **Политика информационной безопасности**: Описывает общие принципы и подходы к защите информации.
- **Процедуры реагирования на инциденты**: Определяют шаги, которые должны быть предприняты при обнаружении инцидента.
- **Правила использования ИТ-ресурсов**: Регламентируют доступ к системам и данным.
- **План непрерывности бизнеса**: Включает меры по восстановлению работы после сбоев или атак.

Разработка стратегии ИБ. Как помогает?

Действуй как эксперт в области информаци
компании. Компания небольшая, около 500
просами информационной безопасности за
информационной безопасности.

Разработка стратегии информационной без
особенности бизнеса, риски и доступные ре

Шаг 1: Оценка текущего состояния

Прежде чем разрабатывать стратегию, необ
безопасности. Это включает:

- **Анализ инфраструктуры**: Определит
- **Оценка существующих мер защиты**
  т.п.).
- **Выявление уязвимостей**: Провести а
- **Определение рисков**: Понять, какие
  человеческий фактор).

Шаг 2: Определение целей и приорит

На этом этапе важно сформулировать конкр
мационной безопасности. Например:

- Обеспечение конфиденциальности, це
- Минимизация финансовых потерь от и
- Соответствие законодательным требов
- Повышение осведомленности сотрудни

Шаг 3: Разработка политик и процеду

Создание четких политик и процедур являет
работать следующие документы:

- **Политика информационной безопа**
- **Процедуры реагирования на инцид**
- **Правила использования ИТ-ресурсо**
- **План непрерывности бизнеса**: Вклю

Шаг 4: Внедрение технических средств защиты

После разработки политик и процедур следует внедрить технические средства защиты, соответствующие вашим целям и бюджету. Примеры таких средств:

- **Антивирусное ПО**.
- **Брандмауэр**.
- **Система обнаружения вторжений (IDS/IPS)**.
- **Шифрование данных**.
- **Многофакторная аутентификация (MFA)**.
- **Резервное копирование данных**.

Шаг 5: Обучение персонала

Один из самых важных аспектов информационной безопасности – это уровень осведомленности ваших сотрудников. Необходимо организовать регулярные тренинги и обучение по следующим темам:

- Основы информационной безопасности.
- Правила безопасного поведения в интернете.
- Признаки фишинговых атак и других видов социальной инженерии.
- Политики и процедуры компании в области информационной безопасности.

Шаг 6: Мониторинг и контроль

Постоянный мониторинг и анализ состояния информационной безопасности помогут своевременно выявлять новые угрозы и реагировать на них. Важно установить систему мониторинга событий безопасности (SIEM), которая будет собирать и анализировать логи различных систем.

Также стоит регулярно проводить тесты на проникновение (pentest) и аудиты безопасности, чтобы оценить эффективность принятых мер.

Шаг 7: Планирование развития

Информационная безопасность – это динамичная область, поэтому стратегия должна предусматривать возможность адаптации к новым угрозам и изменениям в бизнесе. Необходимо периодически пересматривать политику и процедуры, а также обновлять технические средства защиты.

Меры безопасности при работе с внешними AI моделями (сервисами)

- Для работы с нейросетью лучше использовать отдельную учетную запись в браузере (отдельный браузер)
- Не отправляйте чат-боту никакие критичные (персональные, конфиденциальные и т.п.) данные
- Не загружайте документы компании, личные значимые документы
- Отправляете код? Почистите его от конфиденциальных данных исключайте API-ключи, адреса серверов и другую информацию, выдающую структуру приложения и серверной инфраструктуры

Разработка стратегии ИБ. Как помогает?

ChatGPT

Действуй как эксперт в области информационной безопасности. Я являюсь руководителем службы информационной безопасности в компании. Компания небольшая, около 500 рабочих мест. Ранее в этой компании небыло службы информационной безопасности, вопросами информационной безопасности занимались разные подразделения на несистематической основе. Разработай мне стратегию информационной безопасности. Сделай это в формате таблицы

Ключевые обязанности CISO

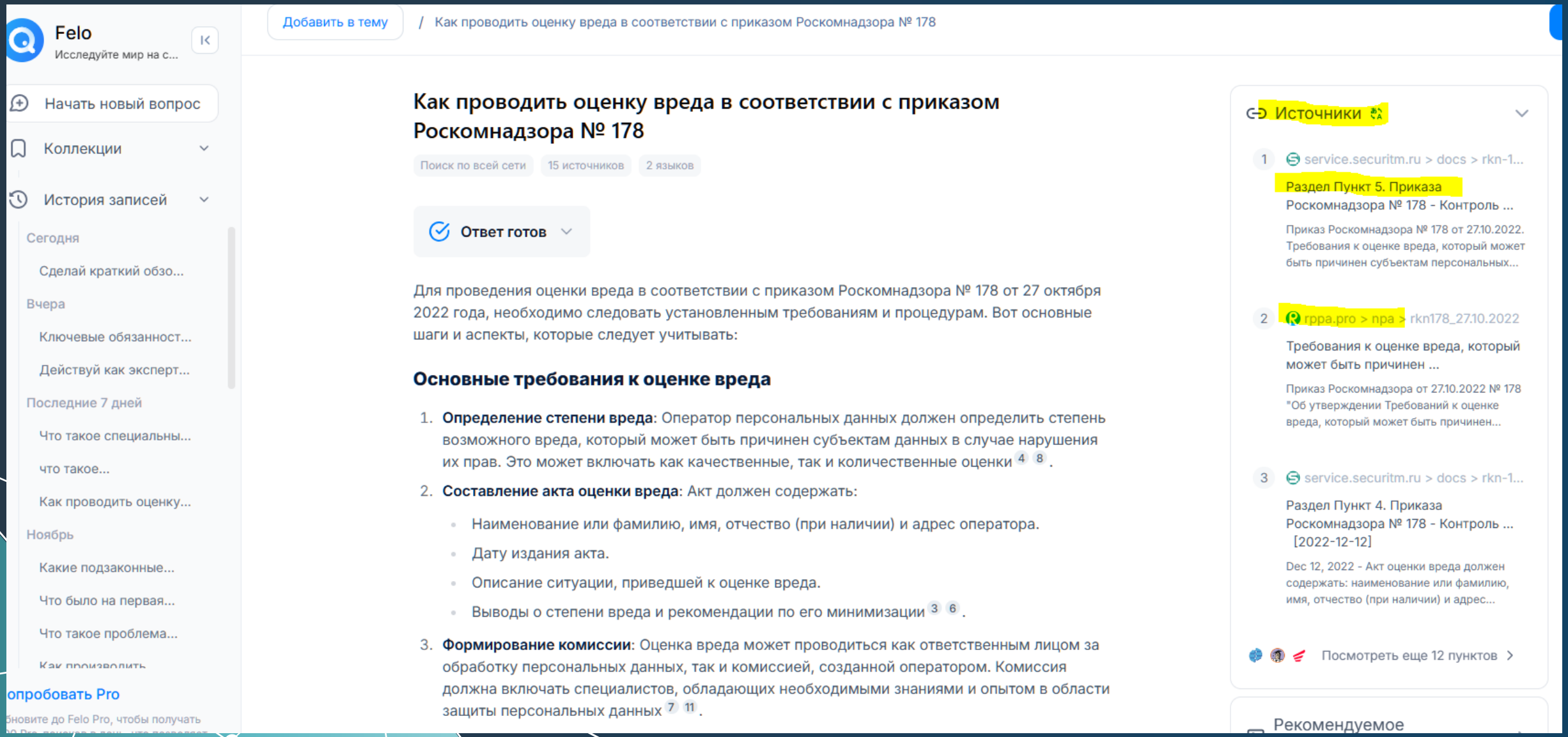
Комплаенс. Что помогает?

Большие языковые модели (LLM)

Примеры сервисов:

- Зарубежные: ChatGPT от OpenAI, Claude от Anthropic, Mistral, Llama, DeepSeek
- Поисковые: Yandex GPT, Perplexity, Felo
- Отечественные: Yandex GPT от Яндекса, Giga Chat от Сбера
- Локальные: Mistral, DeepSeek, Qwen, T-Lite (Pro), GigaChat

Комплаенс. Как помогает?



Комплаенс. Как помогает?

Найди мне опубликованные политики по информационной безопасности на русском языке

Поиск по всей сети | 20 источников | 2 языков | gpt-4o

Ответ готов

На русском языке существует множество опубликованных политик по информационной безопасности, которые могут быть полезны для организаций, стремящихся защитить свои информационные ресурсы. Вот несколько примеров и источников, где можно найти такие политики:

1. **Газпром**: Политика информационной безопасности ПАО «Газпром» включает основные цели и подходы к организации информационной безопасности, что может быть полезно для крупных корпораций [6].
2. **ЕМИАС**: Политика информационной безопасности информационной системы персональных данных ЕМИАС определяет основные цели и направления защиты персональных данных [7].
3. **АО «Содружество»**: Политика информационной безопасности этой компании доступна для скачивания и может служить примером для других организаций [9].
4. **ООО «Красота-групп»**: Целью политики является обеспечение безопасности объектов защиты от всех видов угроз, что может быть полезно для компаний, работающих в сфере услуг [15].

Эти документы обычно содержат правила и рекомендации по защите информации, включая меры по предотвращению несанкционированного доступа, утечки данных и других угроз. Они могут быть адаптированы под нужды конкретной организации в зависимости от ее структуры и специфики деятельности.

Комплаенс. Как помогает?

Найди мне опубликованные политики безопасности на русском языке

Поиск по всей сети | 20 источников | 2 языков | gpt-4o

Ответ готов

На русском языке существует множество опубликован
безопасности, которые могут быть полезны для органи
информационные ресурсы. Вот несколько примеров и
политики:

1. **Газпром**: Политика информационной безопасности
   цели и подходы к организации информационной бе
   крупных корпораций [6].
2. **ЕМИАС**: Политика информационной безопасности
   данных ЕМИАС определяет основные цели и напра
3. **АО «Содружество»**: Политика информационной бе
   скачивания и может служить примером для других
4. **ООО «Красота-групп»**: Целью политики является
   защиты от всех видов угроз, что может быть полез
   услуг [15].

Эти документы обычно содержат правила и рекоменда
меры по предотвращению несанкционированного дост
могут быть адаптированы под нужды конкретной орган
специфики деятельности.

Акционерное Общество «Содружество»
Пригородная Пассажирская Компания

Информационная служба
8 800 550 53 93

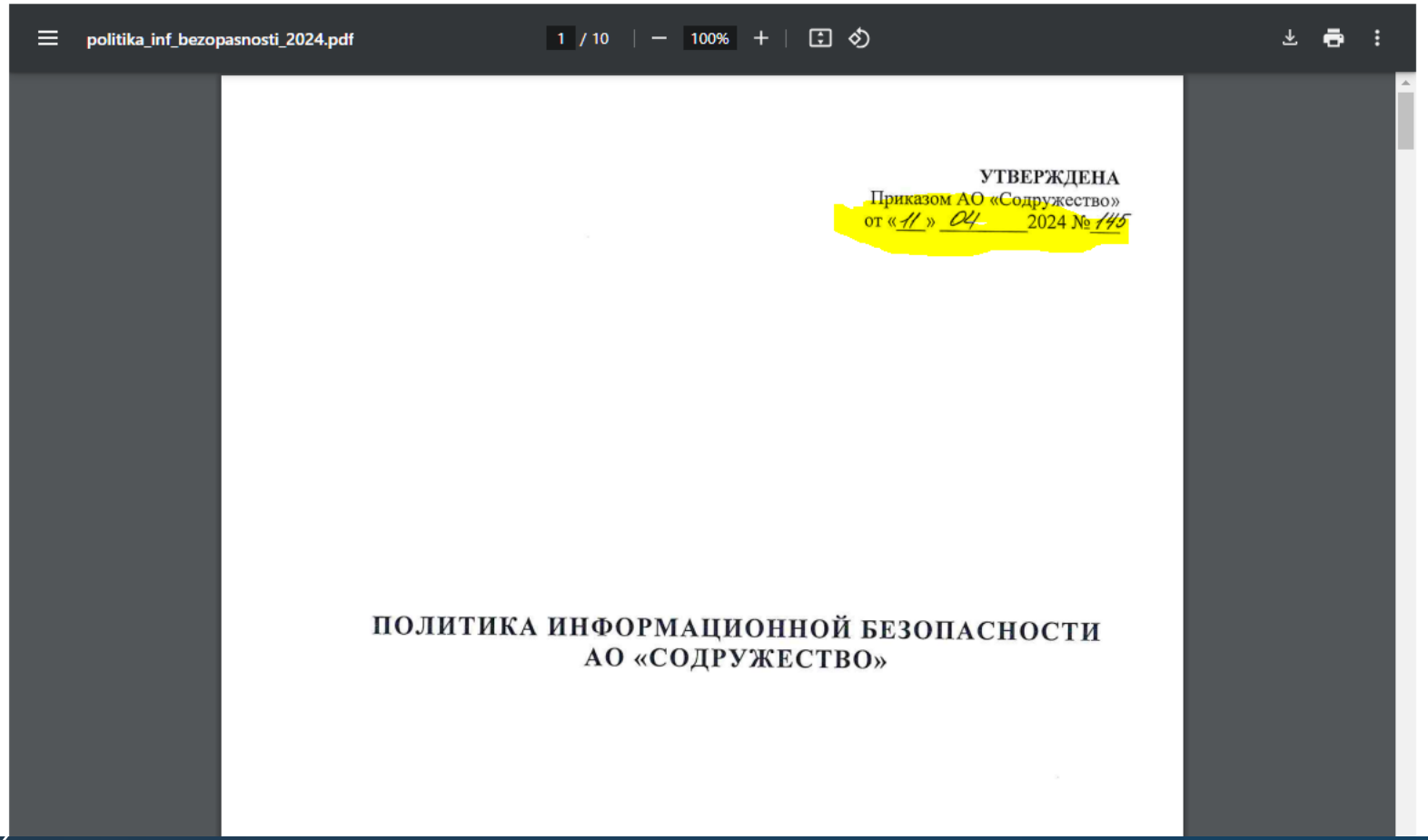
ВЕРСИЯ ДЛЯ СЛАБОВИДЯЩИХ

Пассажирам | Туризм | Тендеры | О компании

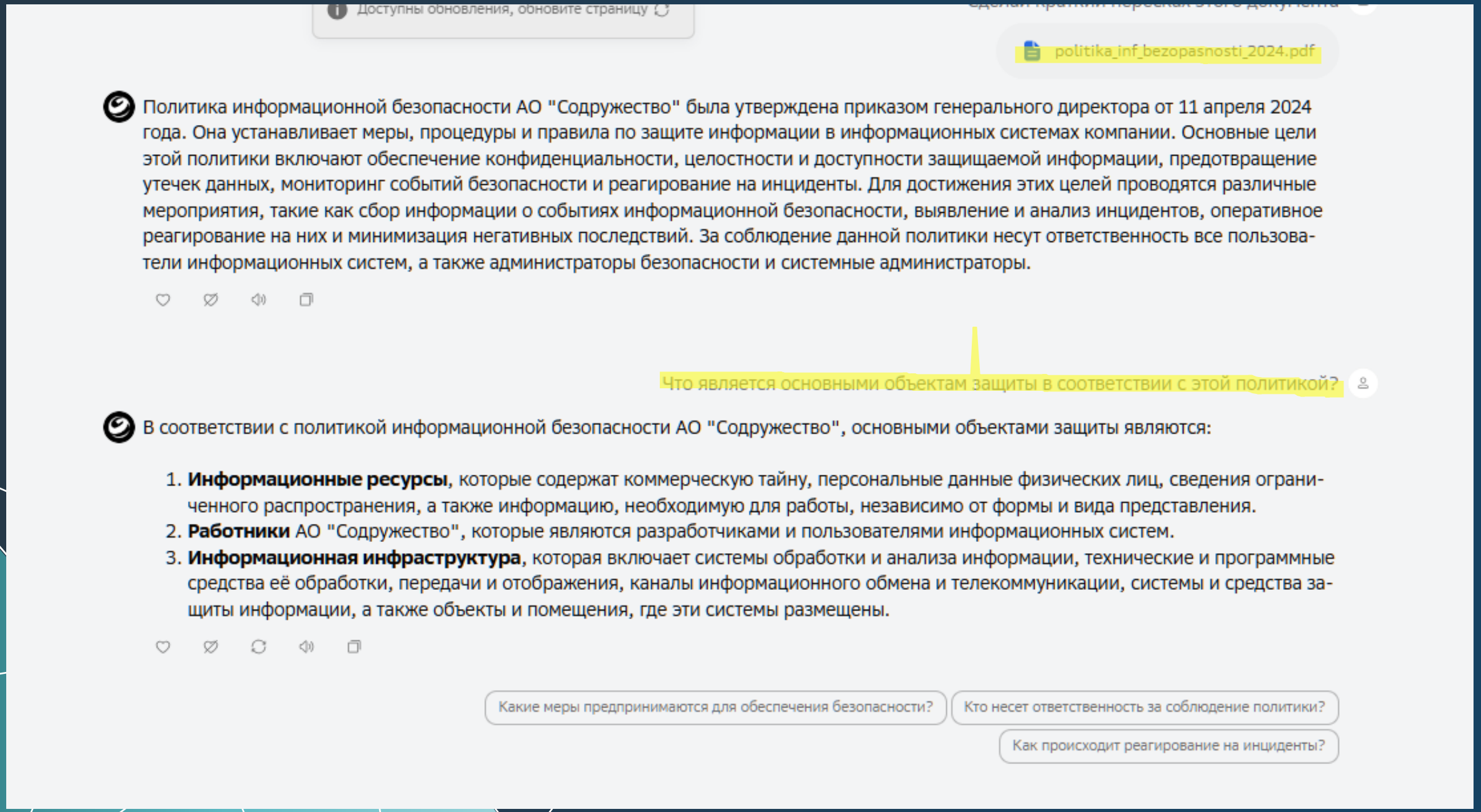
Главная › Компания ›

Политика информационной безопасности АО «Содружество»

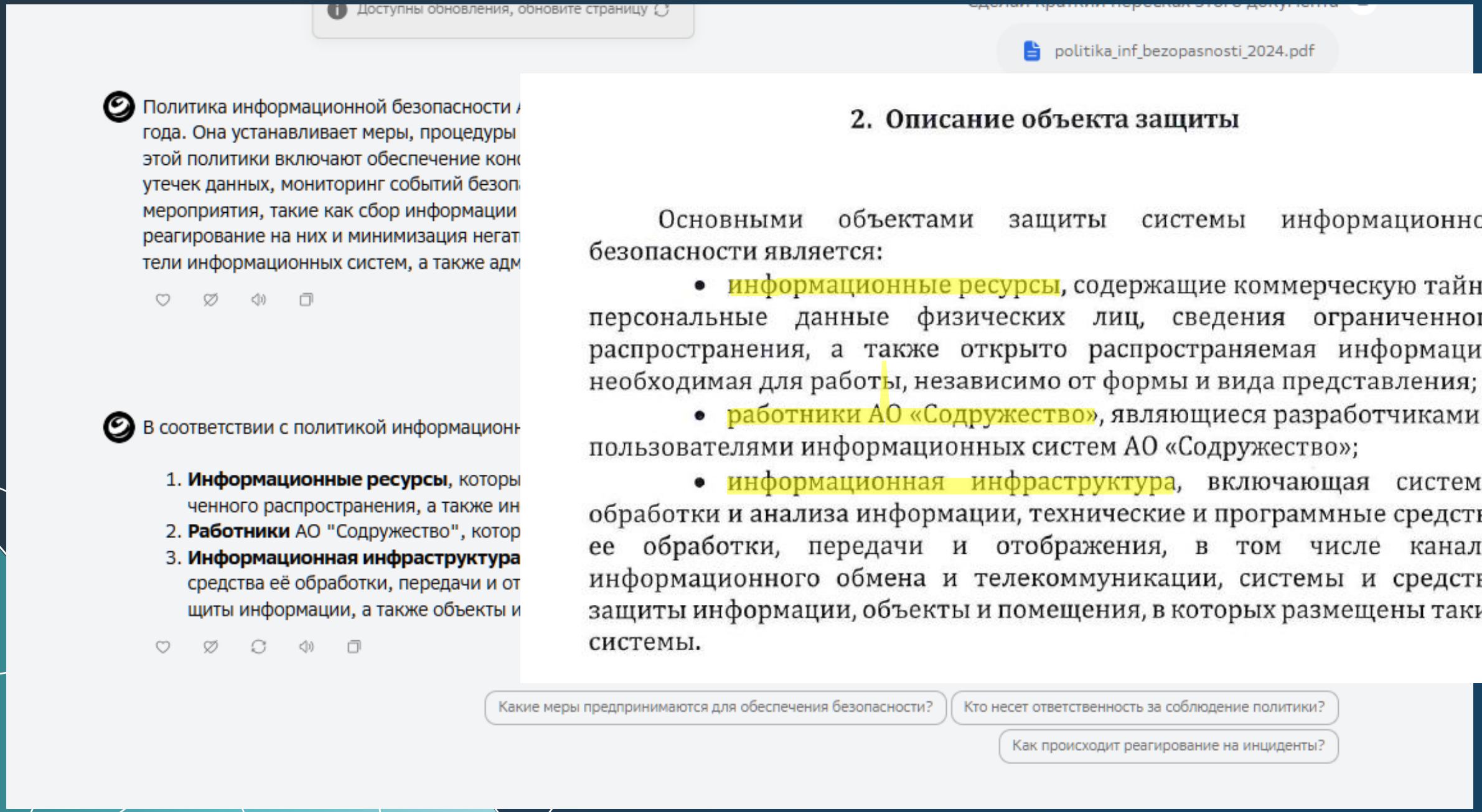
Политика информационной безопасности АО "Содружество" скачать .pdf



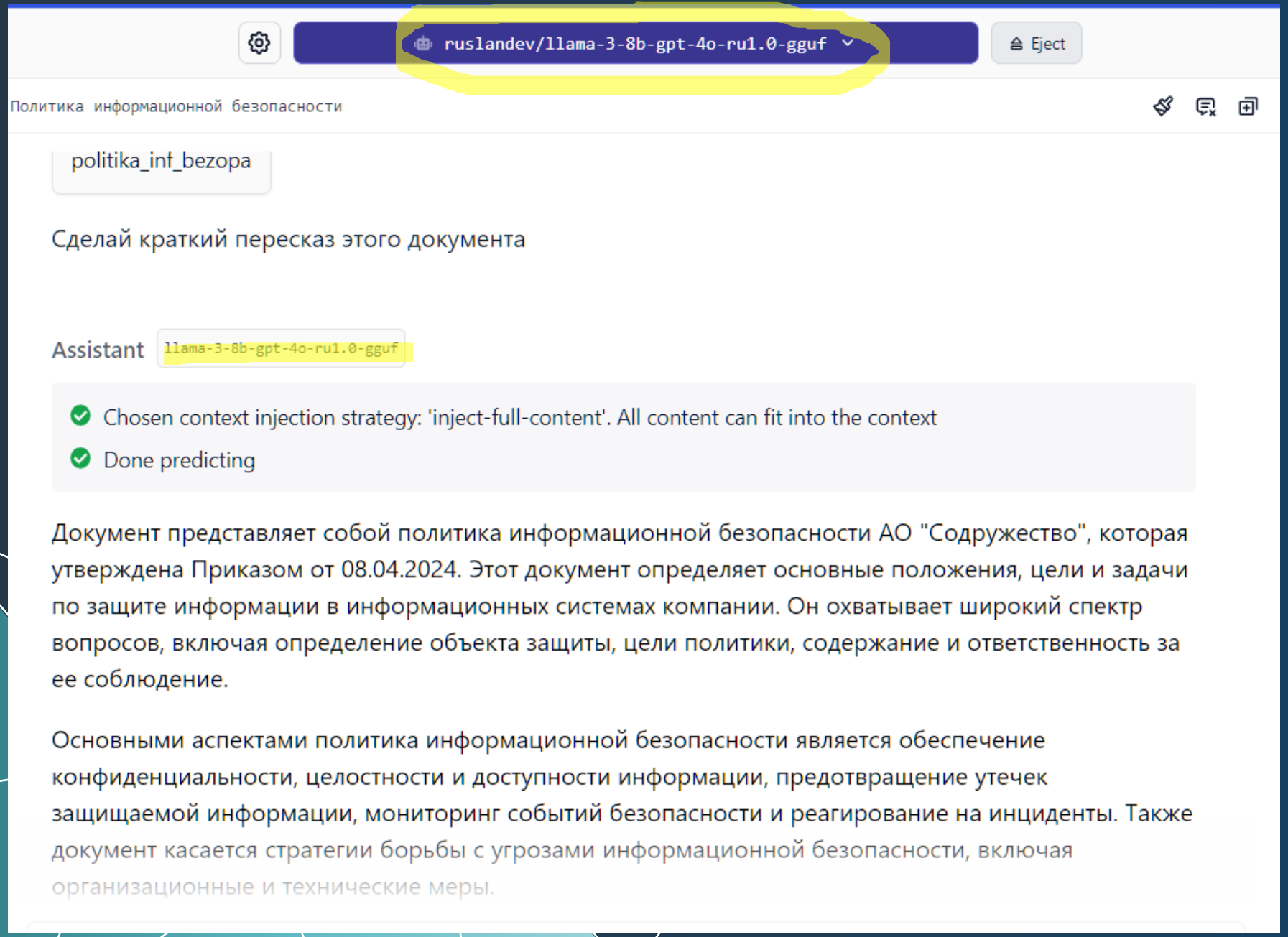
Комплаенс. Как помогает?



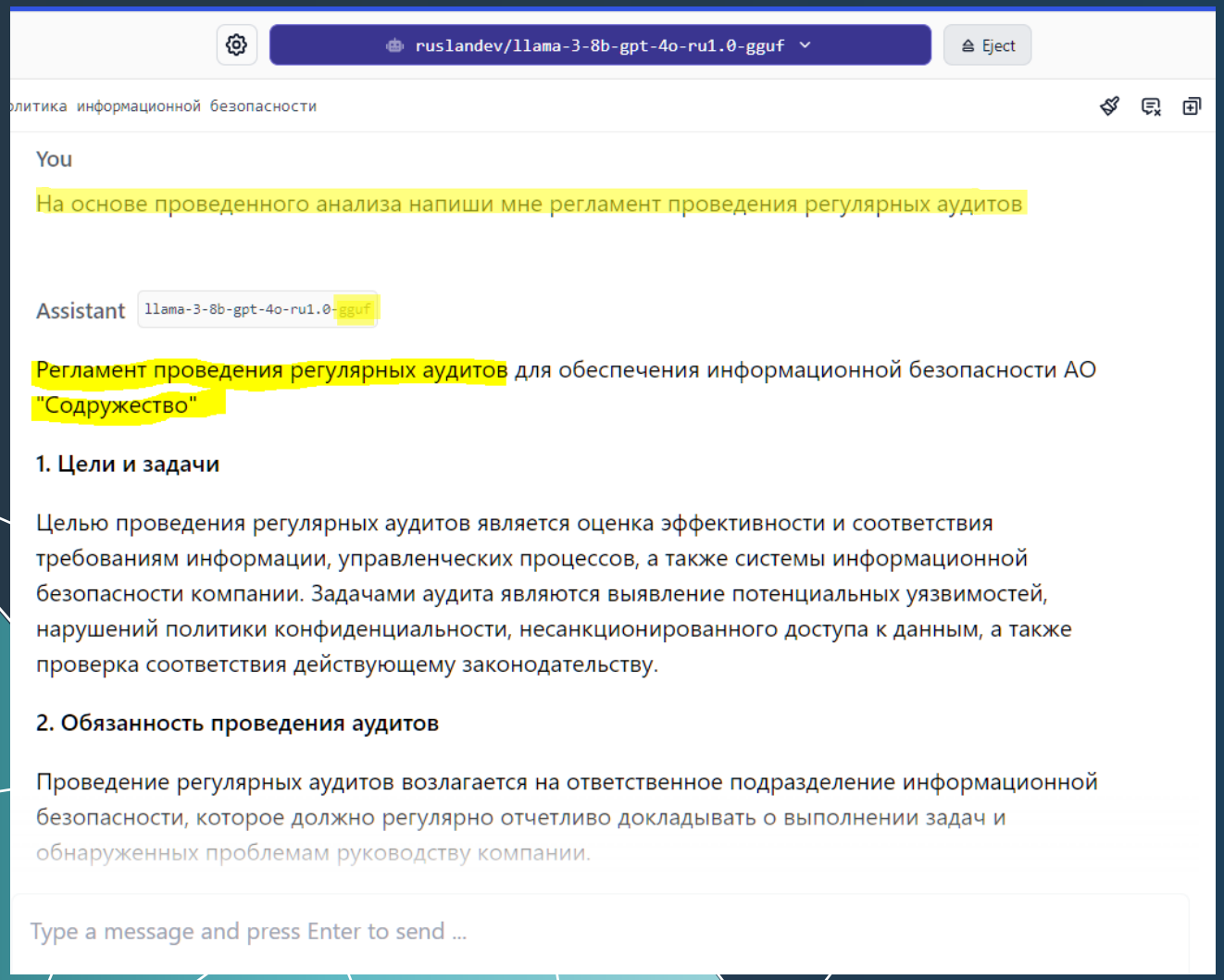
Комплаенс. Как помогает?

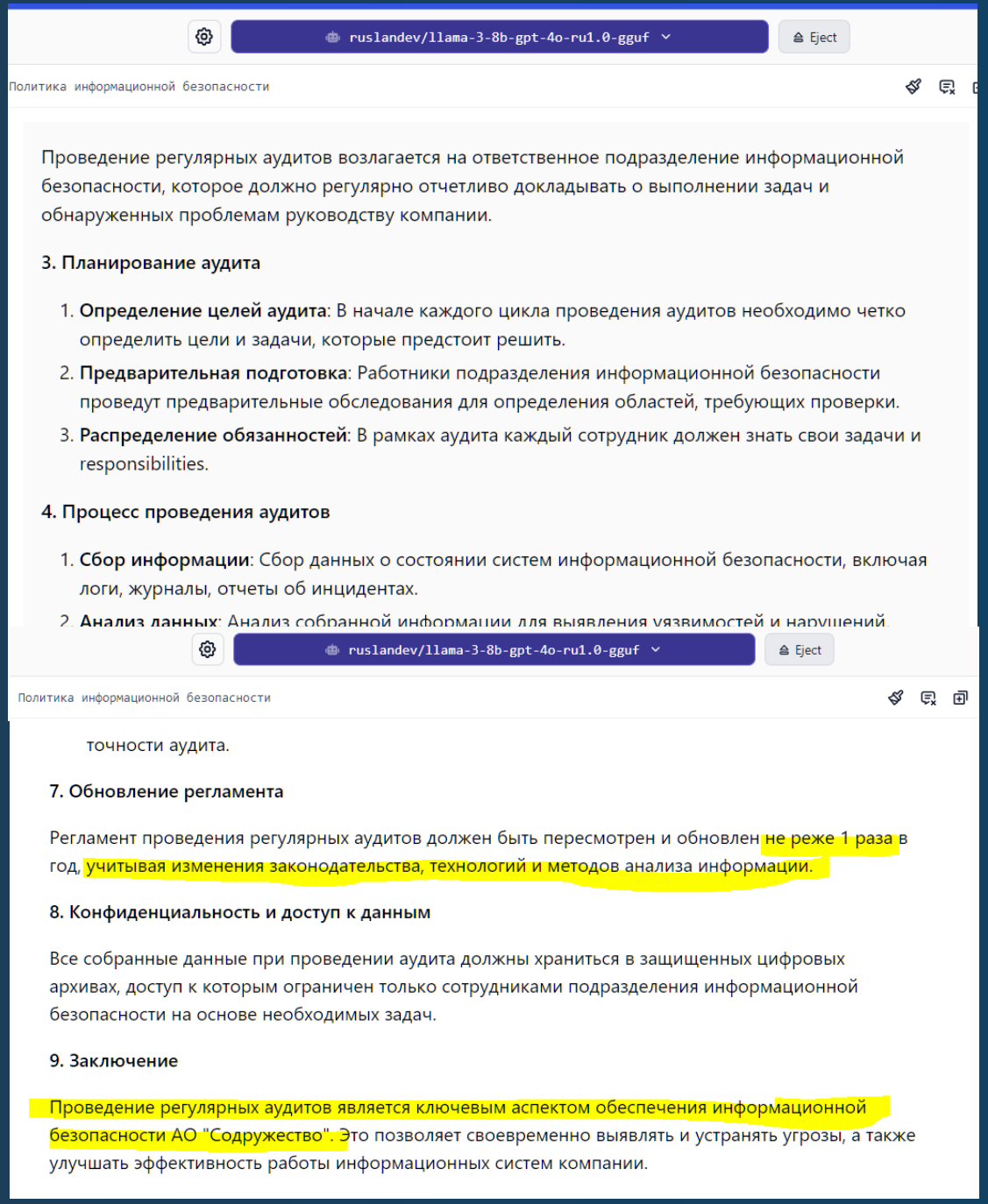


Комплаенс. Как помогает?



Комплаенс. Как помогает?





Ключевые обязанности CISO

Мониторинг и реагирование на инциденты.

Нейронные сети

- **Полносвязные сети (MLP):** анализ логов и отчетов.

Пример: Splunk использует MLP для обработки больших массивов данных.

- **Сверточные сети (CNN):** выявление вредоносного ПО в образах файлов.

Пример: анализатор изображений вирусов в Microsoft Defender.

- **Рекуррентные сети (RNN):** прогнозирование аномалий в последовательностях действий.

Пример: мониторинг активности пользователей в User Behavioral Analytics (UBA) системах.

Разработка плейбуков реагирования для типовых категорий событий ИБ

Действуй как эксперт центра мониторинга и реагирования на инциденты информационной безопасности. Напиши, какие типовые события ИБ бывают в крупной организации?

Thought for 19 seconds

В крупных организациях типовые события информационной безопасности (ИБ) можно классифицировать по нескольким категориям. Вот основные из них:

---

1. Вредоносная активность

- **Фишинг и социальная инженерия**:
  Письма, SMS или сообщения в мессенджерах, направленные на кражу учетных данных или установку вредоносного ПО.
- **Распространение вредоносного ПО**:
  Вирусы, черви, трояны, ransomware (шифровальщики), spyware.
- **Компрометация через уязвимости**:

Разработка плейбуков реагирования для типовых категорий событий ИБ

Действуй как эксперт центра мониторинга и реагирова
безопасности. Напиши, какие типовые события ИБ быв

Thought for 19 seconds

В крупных организациях типовые события информационн
классифицировать по нескольким категориям. Вот основн

---

1. Вредоносная активность

- **Фишинг и социальная инженерия**:
  Письма, SMS или сообщения в мессенджерах, направл
  установку вредоносного ПО.
- **Распространение вредоносного ПО**:
  Вирусы, черви, трояны, ransomware (шифровальщики),
- **Компрометация через уязвимости**:

Напиши мне, что такое плэйбуки?

Thought for 8 seconds

Playbook (плейбук) в контексте информационной безопасности — это детализированный пошаговый сценарий или инструкция, описывающая **действия команды SOC (Security Operations Center)** для реагирования на конкретный тип инцидента или угрозы. Это «руководство к действию», которое помогает стандартизировать процессы, минимизировать человеческие ошибки и ускорить устранение угроз.

Основные компоненты плейбука:

1. **Триггеры**
   Условия, при которых запускается плейбук (например, обнаружение подозрительного файла, множественные попытки входа, срабатывание сигнатуры вредоносного ПО).
2. **Этапы реагирования**
   Последовательность шагов:
   - **Идентификация** — подтверждение инцидента (анализ логов, проверка IoC).

Разработка плейбуков реагирования для типовых категорий событий ИБ

Типовые события ИБ в организациях

```html
                    <li>Сдерживание: блокировка каналов</li>
                    <li>Ликвидация: шифрование данных</li>
                </ul>
                <strong>Роли:</strong> DLP-аналитик, юрист<br>
                <strong>Инструменты:</strong> CASB, DLP<br>
                <strong>Коммуникация:</strong> Отчет регулятору
            </td>
        </tr>

        <!-- Добавьте остальные строки по аналогии -->

    </table>

    <p style="color: #666; margin-top: 20px;">* Полная версия таблицы включает все 12 категорий, кроме IoT/OT и физических инцидентов.</p>
</body>
</html>
```

Run HTML

Как использовать:

1. Скопируйте весь код в текстовый редактор (например, Notepad++ или VS Code).
2. Сохраните файл с расширением `.html` (например, `playbooks.html`).
3. Откройте файл в браузере — таблица будет отформатирована с:
   - Границами

DeepSeek

Плейбуки для типовых ИБ-инцидентов

Событие	Плейбук
Вредоносная активность	**Триггеры:** • Срабатывание сигнатур EDR/антивируса • Пользователь сообщает о фишинге **Этапы:** • Идентификация: анализ в песочнице • Сдерживание: изоляция хоста • Ликвидация: удаление вредоносного ПО **Роли:** SOC, инженер ИБ **Инструменты:** EDR, SIEM **Коммуникация:** Уведомление сотрудников
Несанкционированный доступ	**Триггеры:** • Brute Force-попытки • Вход с необычной геолокации **Этапы:** • Идентификация: анализ логов • Сдерживание: блокировка аккаунта • Ликвидация: включение MFA **Роли:** SOC, администраторы **Инструменты:** SIEM, IAM **Коммуникация:** Уведомление владельца аккаунта
Утечки данных	**Триггеры:** • DLP-алерт • Жалобы клиентов

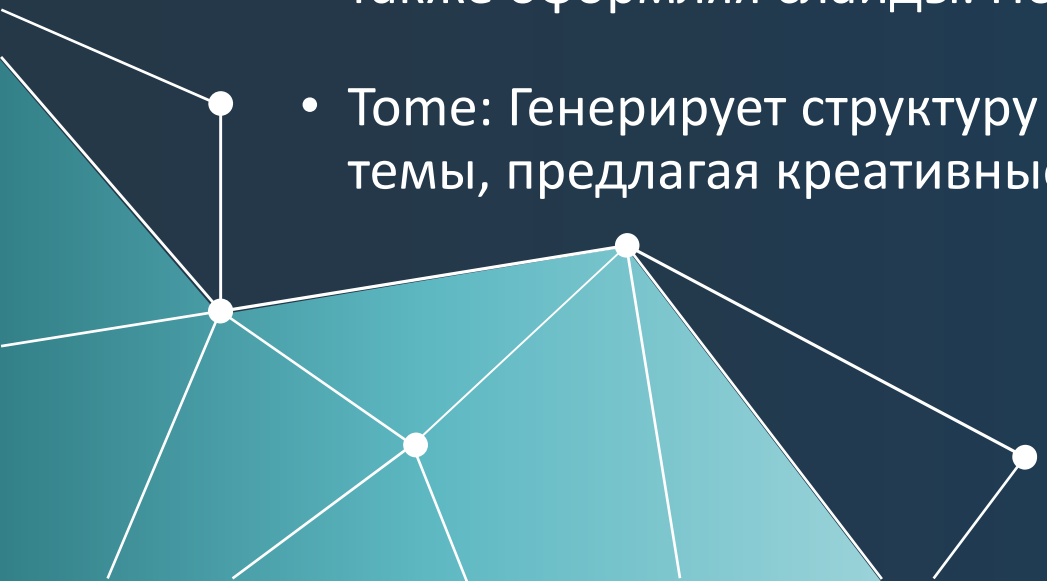
Ключевые обязанности CISO

Взаимодействие с руководством и заинтересованными сторонами. Что помогает?

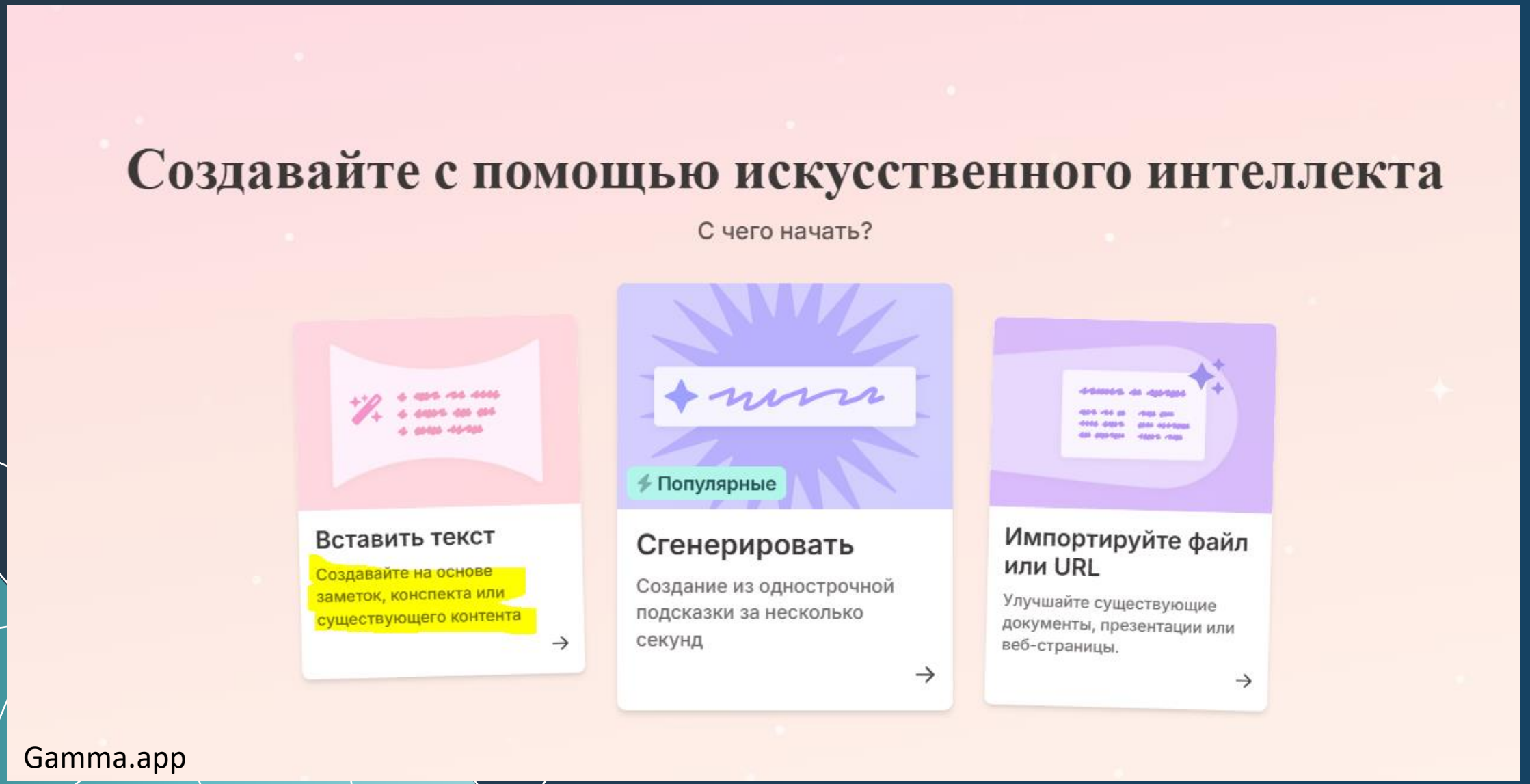
Нейросети для генерации презентаций

Эти нейросети предназначены для автоматизации создания презентаций. Они могут генерировать текст, подбирать изображения и оформлять слайды на основе заданной темы или контента. Примеры сервисов:

- Gamma: Позволяет создавать презентации с нуля, генерируя текст и изображения, а также оформляя слайды. Поддерживает работу на разных языках, включая русский.
- Tome: Генерирует структуру презентации и слайды на основе минимального описания темы, предлагая креативные дизайны



Взаимодействие с руководством и заинтересованными сторонами. Как помогает?

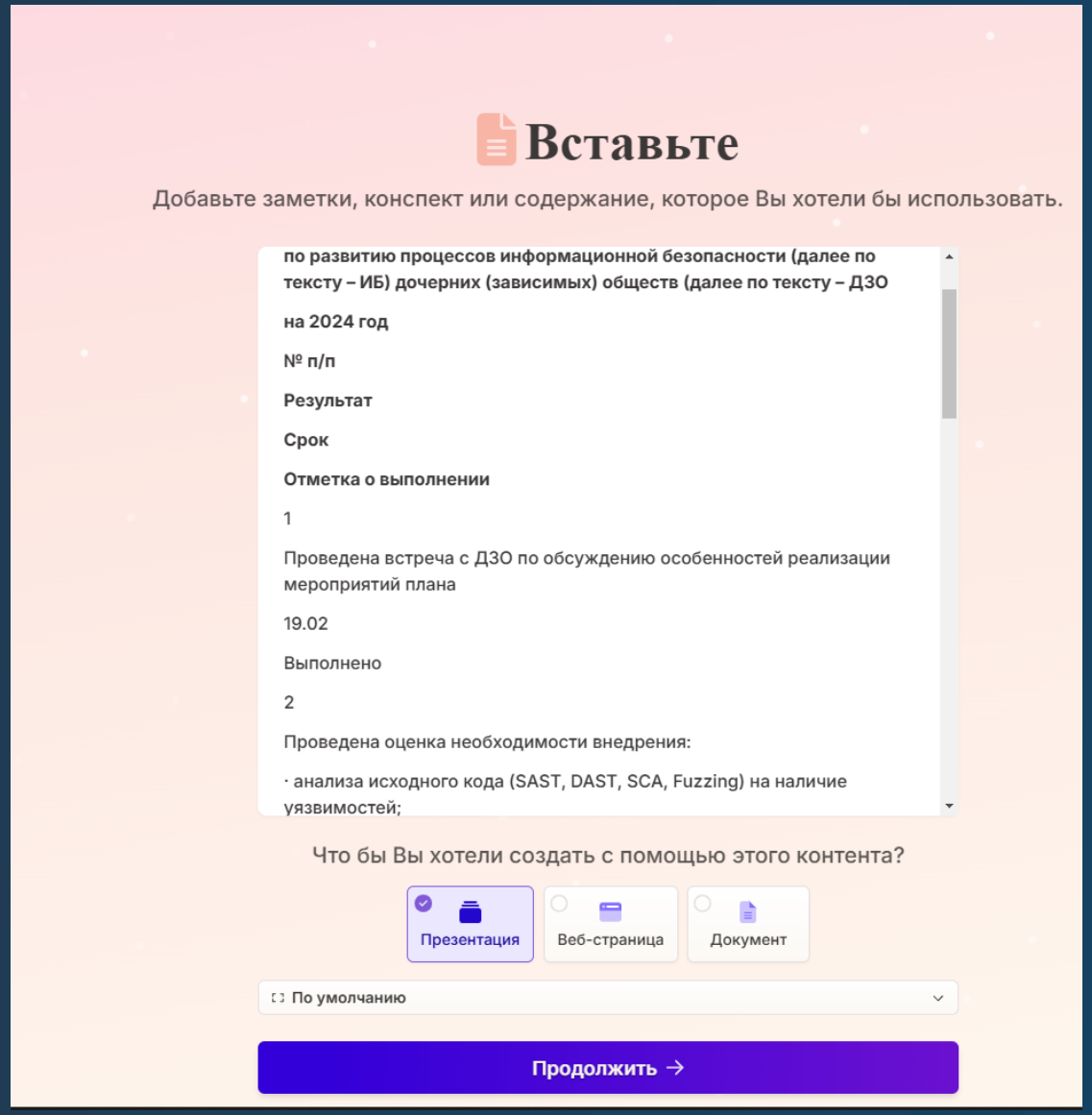


Gamma.app

Взаимодействие с руководством и заинтересованными сторонами. Как помогает?

3¤	• → Проведены·мероприятия·по·оценке·соответствия·требованиям·Федерального·закона·от·27.07.2006·№·152-ФЗ·«О·персональных·данных»¶ • → Подготовлен·отчет·и·план·реализации·мероприятий·по·устранению·выявленных·недостатков·(при·наличии)¤	01.05¤	Выполнено¤	¤
4¤	Разработан·и·утвержден·комплект·документов·по·ИБ,·включая·безопасность·персональных·данных·и·коммерческой·тайны·(корректировка·при·необходимости),·определенных·по·итогам·оценки·соответствия·требованиям·Федерального·закона·от·27.07.2006·N·152-ФЗ·«О·персональных·данных»··(пункт·3·настоящего·Плана)¤	01.09¤	Выполнено¤	¤
5¤	• → Подготовлен·типовой·раздел·по·ИБ·для·договоров¶ • → Подготовлено·распоряжение·о·проведении·анализа·договоров·и·включения·типового·раздела·по·ИБ¶ • → Проведен·анализ·договоров·с·третьими·сторонами·касающихся·информационных·активов·ДЗО¶ • → Внесены·корректировки·в·типовые·проекты·(шаблоны)·договоров·касающихся·информационных·активов·ДЗО·в·части·ИБ¤	01.09¤	Выполнено¤	¤
6¤	Не·менее·90%·работников·ДЗО·приняли·участие·в·антифишинговых·тренировках¤	21.10¤	Выполнено¤	¤

Взаимодействие с руководством и заинтересованными сторонами. Как помогает?



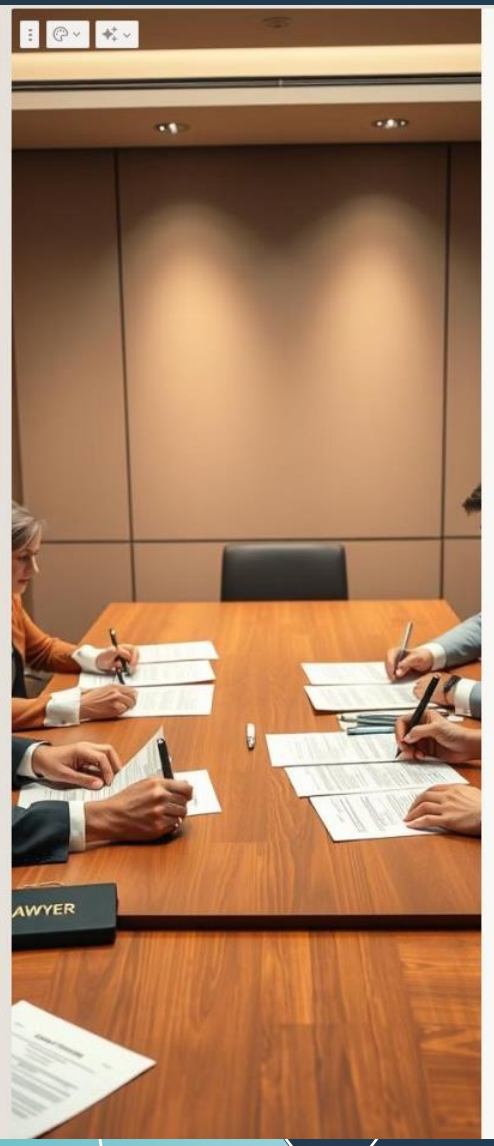
Взаимодействие с руководством и заинтересованными сторонами. Как помогает?

Разработка и утверждение комплекта документов по ИБ

В рамках реализации плана мероприятий по развитию ИБ был разработан и утвержден комплект документов по информационной безопасности, включая безопасность персональных данных и коммерческой тайны. Данный комплект документов был скорректирован с учетом результатов оценки соответствия требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Тип документа	Содержание	Описание
Политика информационной безопасности	Определяет основные принципы и правила обеспечения информационной безопасности в ДЗО.	Содержит общие положения, принципы, цели, задачи, а также ответственность сотрудников за соблюдение мер ИБ.
Порядок обработки персональных данных	Описывает порядок сбора, обработки, хранения, использования, уничтожения персональных данных.	Регламентирует процесс обработки персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
Инструкция по обеспечению информационной безопасности		Содержит подробные инструкции по обеспечению информационной безопасности на различных уровнях.

Взаимодействие с руководством и заинтересованными сторонами. Как помогает?



Разработка типового раздела по ИБ для договоров

В целях повышения уровня информационной безопасности в договорах с третьими сторонами был разработан типовой раздел по ИБ. Данный раздел включает в себя требования к обеспечению конфиденциальности, целостности и доступности информационных активов ДЗО, а также к обработке персональных данных.

1

Подготовка типового раздела

Разработка типового раздела по ИБ была основана на лучших практиках и требованиях законодательства в сфере информационной безопасности.

2

Подготовка распоряжения

Было подготовлено распоряжение о проведении анализа договоров с третьими сторонами и включении типового раздела по ИБ.

3

Анализ договоров

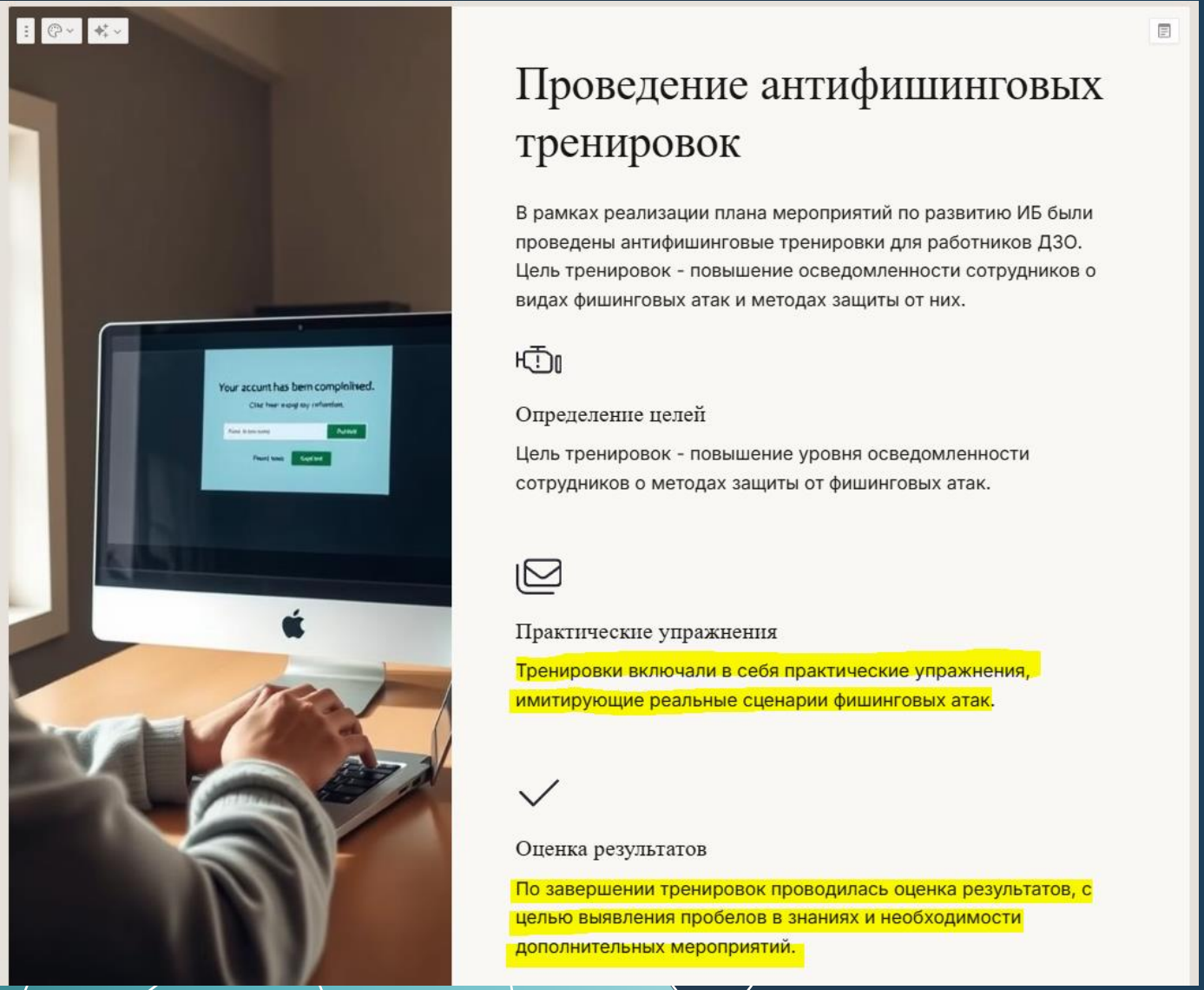
Проведен анализ договоров с третьими сторонами, касающихся информационных активов ДЗО.

4

Внесение корректировок

Были внесены корректировки в типовые проекты (шаблоны) договоров, касающихся информационных активов ДЗО, в части ИБ.

Взаимодействие с руководством и заинтересованными сторонами. Как помогает?



Проведение антифишинговых тренировок

В рамках реализации плана мероприятий по развитию ИБ были проведены антифишинговые тренировки для работников ДЗО. Цель тренировок - повышение осведомленности сотрудников о видах фишинговых атак и методах защиты от них.

Определение целей

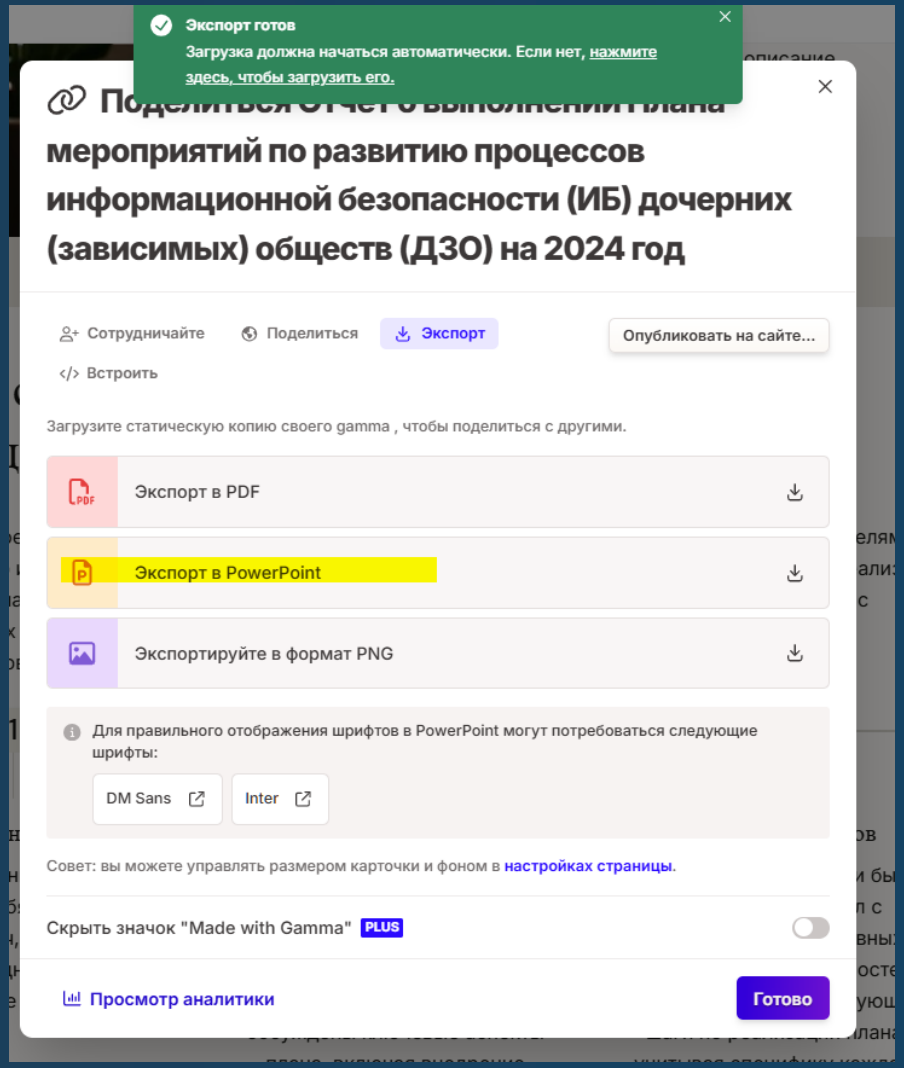
Цель тренировок - повышение уровня осведомленности сотрудников о методах защиты от фишинговых атак.

Практические упражнения

Тренировки включали в себя практические упражнения, имитирующие реальные сценарии фишинговых атак.

Оценка результатов

По завершении тренировок проводилась оценка результатов, с целью выявления пробелов в знаниях и необходимости дополнительных мероприятий.



Взаимодействие с руководством и заинтересованными сторонами. Что помогает?

Нейросети для генерации рисунков

Эти нейросети обучены на изображениях и способны создавать новые изображения на основе текстовых описаний или других изображений. Они используют методы генеративного моделирования для создания визуального контента.

Примеры сервисов:

- Зарубежные: DALL-E от OpenAI, Midjourney, Stable Diffusion
- Отечественные: Кандинский от Сбера, Шедеврум от Яндекса

Взаимодействие с руководством и заинтересованными сторонами. Как помогает?

Действуй как промпт инженер. Напиши мне промпт для нейросети Stable Diffusion. Нужно чтобы нейросеть нарисовала открытку на день рождения руководителю центра мониторинга и реагирования на инциденты. Предложи несколько промптов

Конечно! Вот несколько вариантов промптов для создания открытки на день рождения руководителю центра мониторинга и реагирования на инциденты:

1. **Классическая поздравительная открытка:**

   > **"Birthday card for a leader of a Cybersecurity Incident Response Center, featuring a modern, sleek design with elements of cybersecurity: digital shield, binary code background, and soft, celebratory colors (like blue and gold). Text reads 'Happy Birthday to Our Guardian of Cybersecurity!' in elegant, professional font. Include subtle elements of technology and cyber defense without cluttering the design."**

2. **Современная и динамичная открытка с элементами киберзащиты:**

Взаимодействие с руководством и заинтересованными сторонами. Как помогает?

Теперь предложи рисунок на тему OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации,

Вот несколько идей для иллюстраций на тему протокола OSPF, которые можно использовать для визуализации принципов и работы динамической маршрутизации:

1. **Визуализация OSPF-сети:**

   > **"Illustration of an OSPF (Open Shortest Path First) routing protocol network, showing interconnected routers in a web-like, network topology. Each router has clear labels, with some paths highlighted to indicate the shortest routes calculated by the protocol. Use bright, high-contrast colors for nodes and connecting lines to make the topology and routes stand out. Background is subtle and technical, with elements like binary code or network grid patterns."**

2. **Интерфейсы и таблица маршрутизации OSPF:**

Взаимодействие с руководством и заинтересованными сторонами. Как помогает?

Проанализируй этот текст. Напиши мне промпты для графического офрмления этого текста. "День специалиста по безопасности, отмечаемый 12 ноября, является профессиональным праздником в России, который был учреждён в 2005 году. Этот день посвящён всем, кто занимается

Вот несколько идей для графического оформления текста про День специалиста по безопасности:

1. **Оформление заголовка и основной информации о празднике:**

   "Create a professional and sleek banner for 'Day of Security Specialist' celebrated on November 12 in Russia. Background features symbols of security, such as a digital shield, lock icons, and soft metallic colors (silver and blue). Title text in bold, with a small subheading about the holiday's significance. Include date and mention that it's a professional holiday since 2005, using a clean, modern font for clarity."

2. **История и значение праздника:**

   "Illustration on the history and importance of Security Specialist Day, showing a timeline or

Промпт инженеринг

- Есть такая профессия промпт инженер (промптер, жопотолог)
- Много курсов которые обучают этой профессии. Стоимость от 50 000 рублей (в среднем 150 000)

Чтобы стать промпт инженером:

- Знать структуру промптов
- Практиковаться

Структура промпта

Структура	Пример
Роль	Действуй как (Act Like): • Специалист по кибербезопасности • Эксперт по кибербезопасности • Эксперт по проведению тестирования на проникновения • Эксперт по менеджменту в информационной безопасности
Задача	• Составь мне саммари данного файла • Проведи сравнительный анализ антивирусов Касперский, Avast и Windows Defender
Контекст и детали	• Выдели основные важные для меня аспекты • Для сравнения используй следующие критерии: высокий процент и высокая скорость обнаружения вредоносного программного обеспечения, удобство использования: понятный интерфейс, отсутствие частых всплывающих сообщений, минимальное количество ложных срабатываний, минимальное влияние на производительность системы.
Формат результата	• Представь результат в форме таблицы • Сделай в формате тезисов (для презентации) • Пиши на русском
TOV	• Используй технический язык • Официальный/Репортер Новостей/Илон Маск

Congratulations!

Ключевые обязанности CISO

Управление командой специалистов

1. Подбор персонала и адаптация (HR-процессы)

ChatGPT (аналоги):

- Автоматизация обработки резюме: анализ данных кандидатов, формирование списков подходящих профилей.
- Проведение предварительных собеседований с помощью чат-ботов.
- Создание адаптационных материалов и сценариев для онбординга новых сотрудников.

14.11.2024

Роль онбординга в снижении текучести кадров в сфере ИБ

https://bisa.ru/stati

Управление командой специалистов

Действуй как эксперт в области HR. Подготовь мне адаптационный чеклист для нового специалиста по информационной безопасности. Новый специалист будет заниматься администрированием антивирусного программного средства

Адаптационный чеклист для нового специалиста по информационной безопасности

Должность: Администратор антивирусного программного средства
Цель: Ускорить адаптацию сотрудника, обеспечить его вовлечение в рабочий процесс и достижение максимальной эффективности.

---

1. Первый рабочий день

1.1. Встреча с куратором (HR/руководитель)

- Приветствие и знакомство.
- Ознакомление с планом адаптации.
- Передача welcome-пакета (документы, инструкции, памятки).

1.2. Оформление документов

- Подписание необходимых договоров и инструктажей (трудовой договор, NDA, политика ИБ).

1.3. Обзор компании и команды

- Рассказы о миссии, ценностях и структуре компании.

Управление командой специалистов

Действуй как эксперт в области HR. Подготовь мне адаптационный чеклист для нового специалиста по информационной безопасности. Новый специалист будет заниматься администрированием антивирусного программного средства

Адаптационный чеклист для нового специалиста по информационной безопасности

Должность: Администратор антивирусного программного средства
Цель: Ускорить адаптацию сотрудника, обеспечить его вовлечение в рабочий процесс и достижение максимальной эффективности.

---

1. Первый рабочий день

1.1. Встреча с куратором (HR/руководитель)

- Приветствие и знакомство.
- Ознакомление с планом адаптации.
- Передача welcome-пакета (документы, инструкции, памятки).

1.2. Оформление документов

- Подписание необходимых договоров и инструктажей (трудовой договор, NDA, поли ИБ).

1.3. Обзор компании и команды

- Рассказы о миссии, ценностях и структуре компании.

2. Первая неделя

2.1. Знакомство с антивирусным решением

- Изучение архитектуры антивирусного ПО, используемого в компании.
- Изучение политики обновления сигнатур и управления инцидентами.
- Тестовое выполнение базовых задач (например, проверка состояния обновлений).

2.2. Введение в процессы

- Ознакомление с основными процедурами:
  - Мониторинг состояния антивирусного ПО.
  - Анализ выявленных угроз и реагирование.
  - Регулярная отчетность.
- Обучение работе с журналами событий и отчетами антивирусного ПО.

2.3. Знакомство с документацией

- Чтение руководств пользователя и корпоративных регламентов.
- Обучение ведению журналов инцидентов.

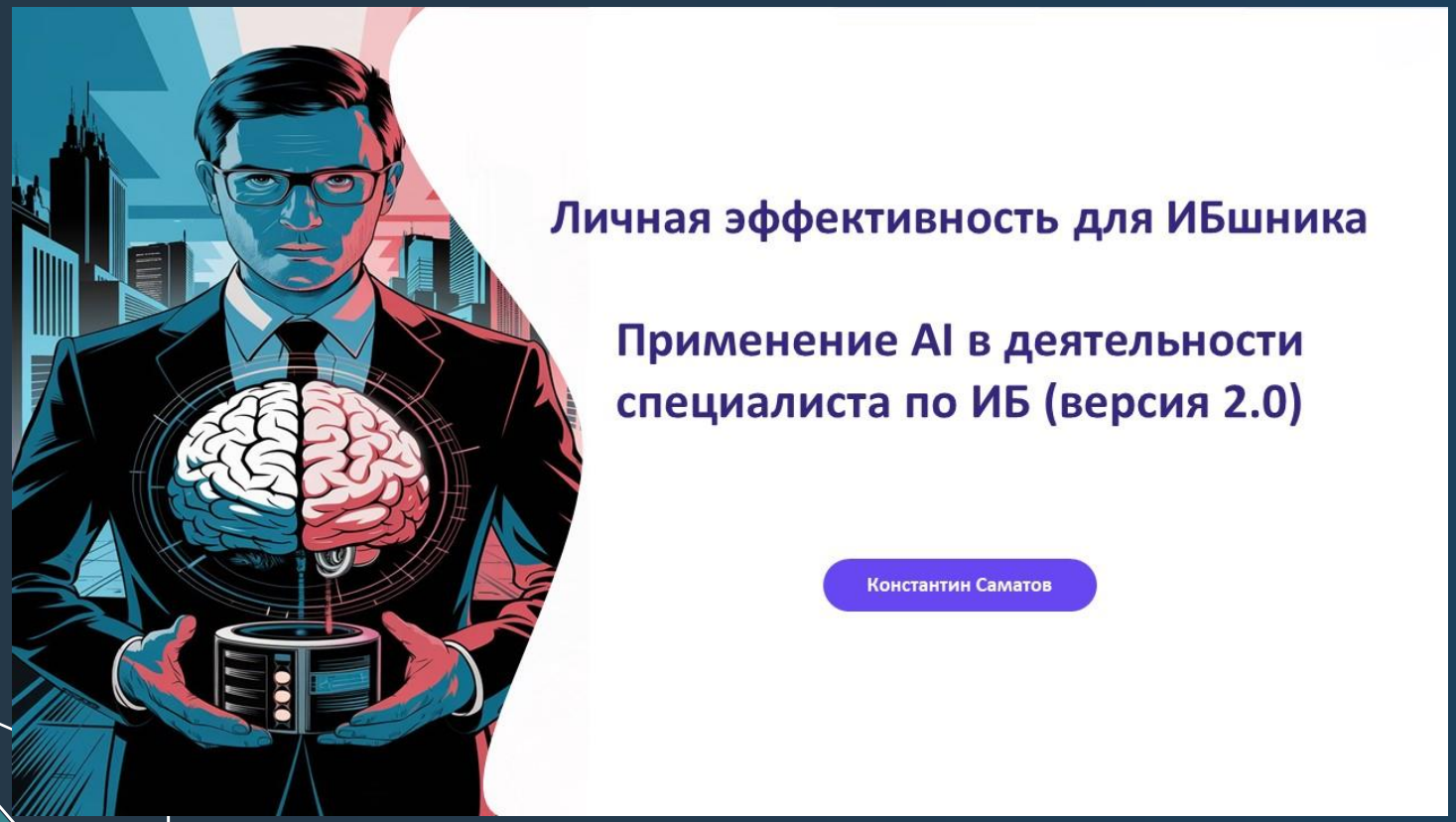
---

3. Первый месяц

3.1. Практическая работа

- Выполнение реальных задач под контролем наставника:
  - Настройка антивирусной политики.
  - Устранение ложных срабатываний.
  - Создание регулярных отчетов.

Управление командой специалистов



2. Мониторинг и поддержание вовлечённости

ChatGPT (аналоги):

Разработка опросов для оценки вовлечённости сотрудников и анализа их ответов.

Составление рекомендаций по улучшению морального климата в команде.

Управление командой специалистов

Добрый день, коллеги!
Ниже, проект новости «О необходимости повышения бдительности при получении электронных писем и других сообщений» (в новогодние праздники).

Прошу рассмотреть на предмет предложений/замечаний.

О необходимости повышения бдительности при получении электронных писем и других сообщений

Уважаемые коллеги!

Напоминаем о необходимости соблюдения бдительности при получении электронных писем и сообщений в мессенджерах.

3. Культура и внутренняя коммуникация

Suno и Soundful (аналоги):

Создание музыки для корпоративных мероприятий или видеороликов.

Генерация аудиопосланий для корпоративных новостей.

ChatGPT (аналоги):

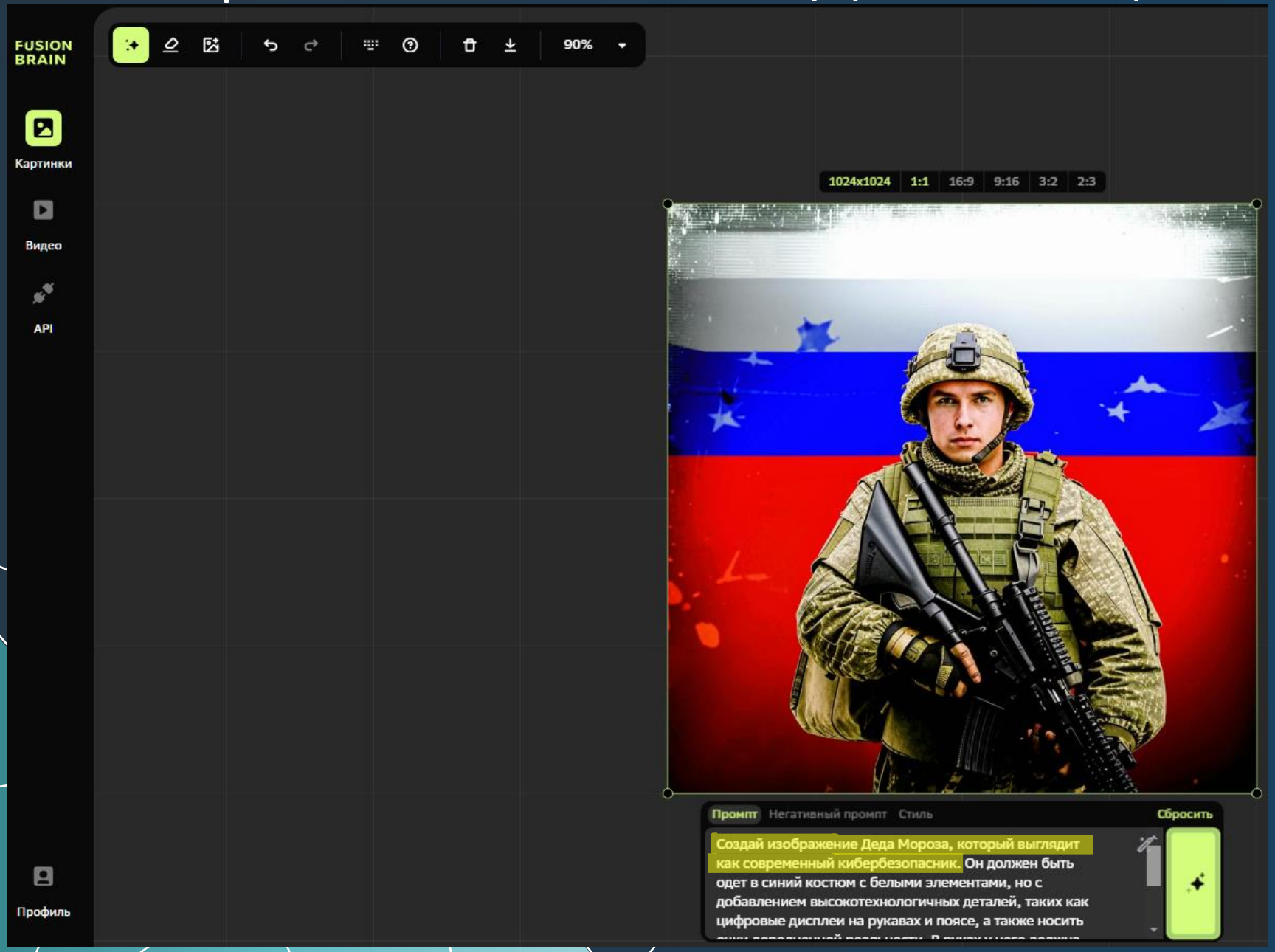
Создание текстов для корпоративных рассылок, слоганов или мотивационных сообщений.

Stable Diffusion (аналоги)

Подготовка поздравительных откртоок

Рисунки в рамках коммуникаций

Управление командой специалистов



3. Культура и внутренняя коммуникация

Suno и Soundful (аналоги):

Создание музыки для корпоративных мероприятий или видеороликов.

Генерация аудиопосланий для корпоративных новостей.

ChatGPT (аналоги):

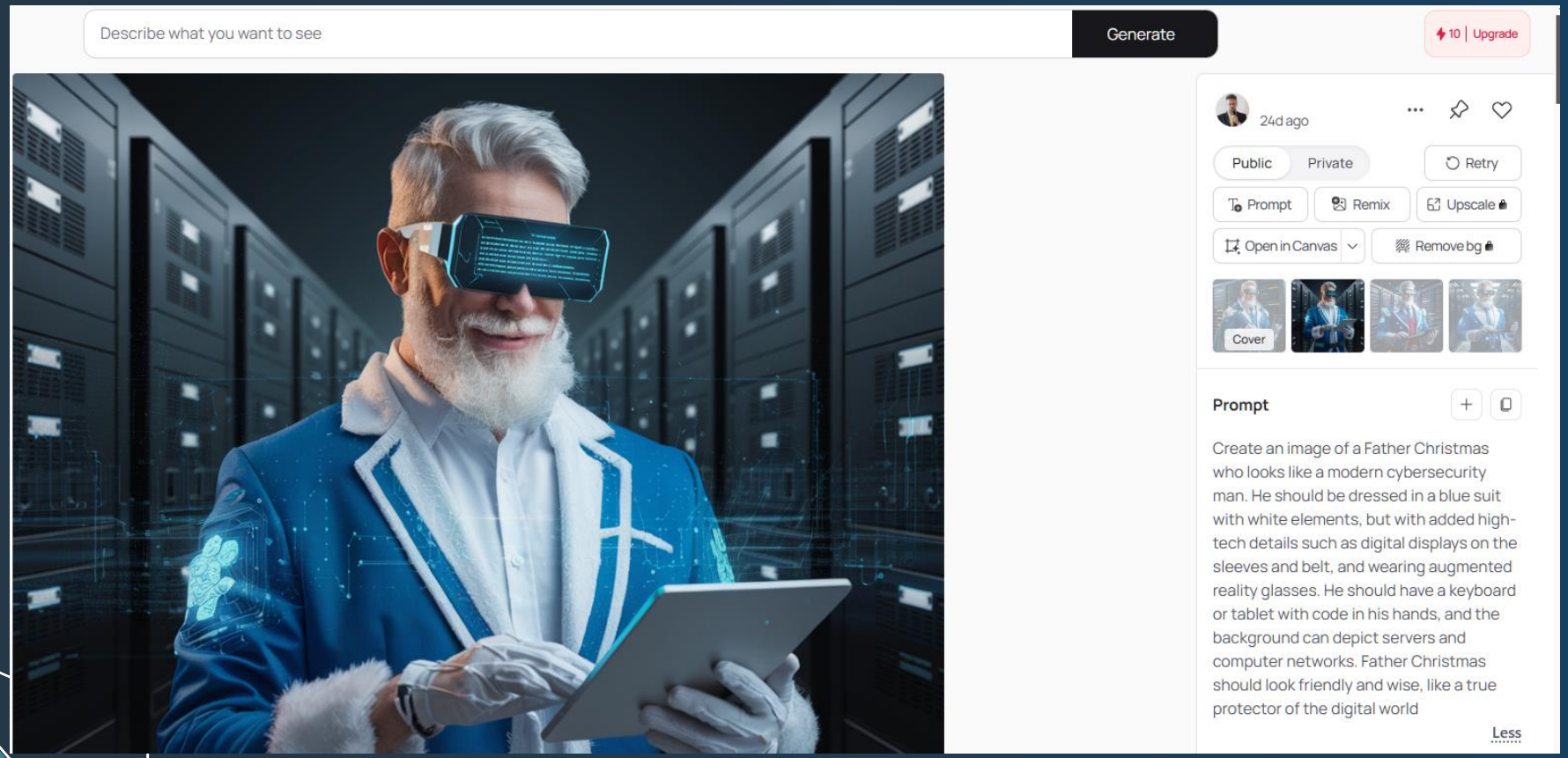
Создание текстов для корпоративных рассылок, слоганов или мотивационных сообщений.

Stable Diffusion (аналоги)

Подготовка поздравительных откртоk

Рисунки в рамках коммуникаций

Управление командой специалистов



3. Культура и внутренняя коммуникация

Suno и Soundful (аналоги):

Создание музыки для корпоративных мероприятий или видеороликов.

Генерация аудиопосланий для корпоративных новостей.

ChatGPT (аналоги):

Создание текстов для корпоративных рассылок, слоганов или мотивационных сообщений.

Stable Diffusion (аналоги)

Подготовка поздравительных откртоk

Рисунки в рамках коммуникаций

Ключевые обязанности CISO

Обучение и повышение осведомленности
Что помогает?

Канал в RuTube

Клип про СИБ

Клип про День ЗИ

Нейросети для генерации аудио

Эти нейросети способны синтезировать аудио, включая речь и музыку, на основе текстовых или других аудиовходов. Они используют сложные алгоритмы для создания реалистичного звука.

Примеры сервисов:

- SoundFul: Генерирует музыку в различных жанрах и стилях на основе текстовых описаний
- Suno: платформа для генерации песен

Обучение и повышение осведомленности
Что помогает?

Клип про День СБ

Курс кибергигиена для самых маленьких

Нейросети для генерации видео

Эти нейросети создают видеоконтент на основе текстовых описаний или других видеовходов. Они применяют методы глубокого обучения для создания анимаций и видеороликов.

Примеры сервисов:

RunwayML: Платформа для создания и редактирования видео с использованием ИИ, поддерживающая генерацию видео на основе текстовых подсказок.

Synthesia: Позволяет создавать видео с виртуальными аватарами, которые могут говорить на разных языках.

DeepBrain: Используется для создания анимационных видео и визуальных эффектов с помощью ИИ.

Спасибо за внимание!

Константин Саматов