

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

Константин Саматов



Усиленные люди

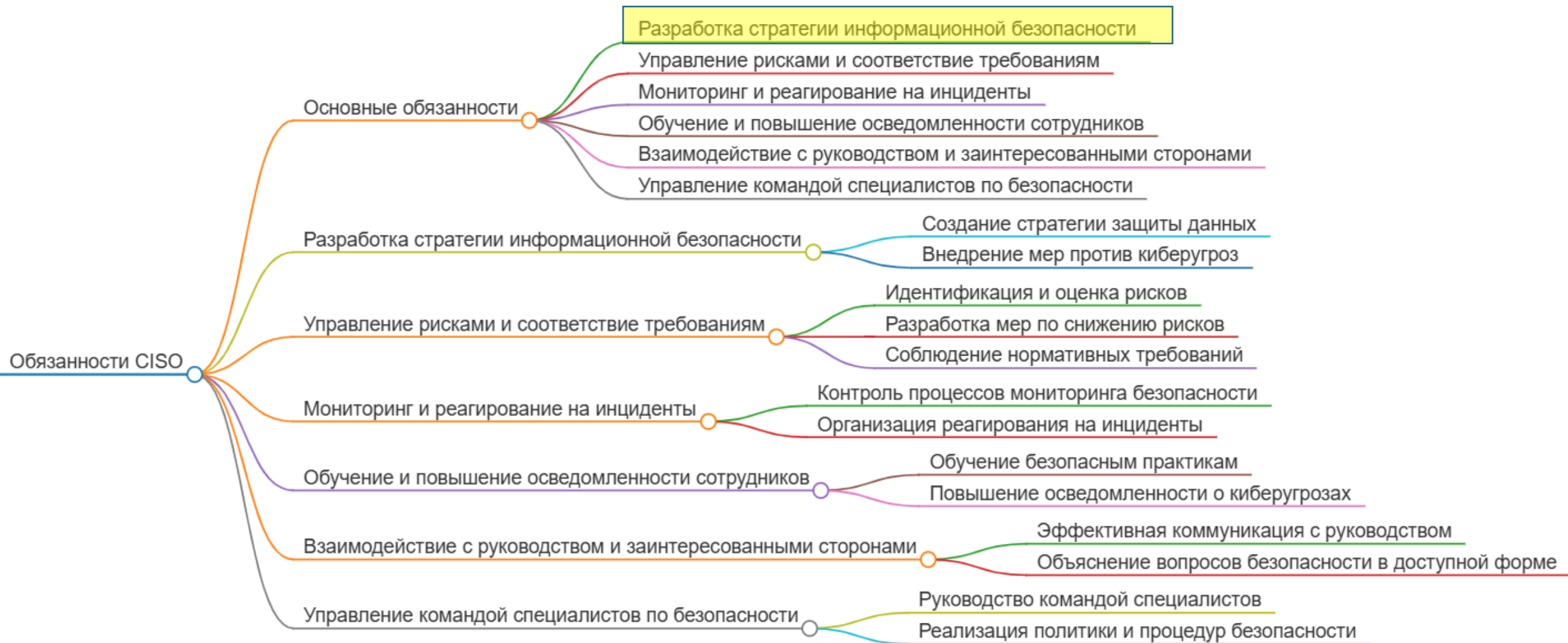
ГОНКА ЗА ЛИДЕРСТВО В ИИ ОБОСТРЯЕТСЯ



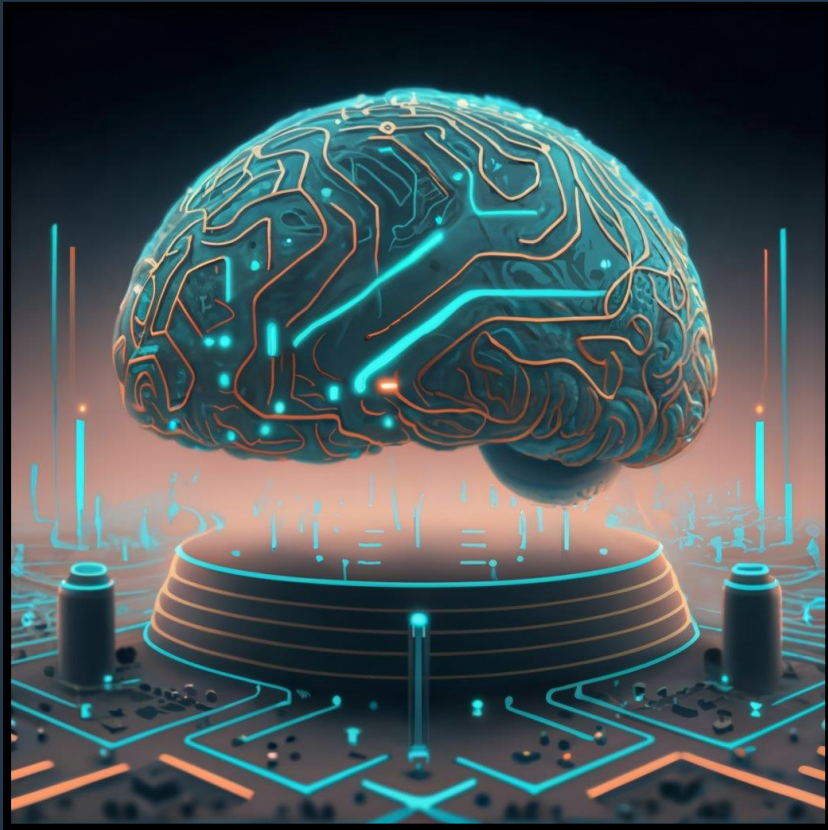
Россия должна стать мировым лидером не только по созданию, но и по масштабу применения, проникновению искусственного интеллекта во все без исключения сферы нашей жизни

Владимир Путин,
Президент Российской Федерации

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, Haulilo 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 не было 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 описывающих 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 правил управления реагирования на инциденты, копирование	Управление обновлениями	Внедрение автоматизированного процесса обновления ПО и ОС.	2 месяца	IT-отдел	Процесс обновления настроен.
		Многофакторная аутентификация	Внедрение MFA для критичных систем и доступа к корпоративной сети.	2 месяца	IT-отдел	Установлена многофакторная аутентификация.
3. Организационные меры		5. Обучение сотрудников				
Формирование структуры службы ИБ	Назначение сотрудников, распределение обязанностей, план работы	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 не было 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 информации компании. Компания небольшая, около 500 просами информационной безопасности за информационной безопасности.

- 🕒 Разработка стратегии информационной безопасности, особенности бизнеса, риски и доступные ресурсы.

Шаг 1: Оценка текущего состояния

Прежде чем разрабатывать стратегию, необходимо оценить текущее состояние безопасности. Это включает:

- **Анализ инфраструктуры:** Определит текущее состояние инфраструктуры.
- **Оценка существующих мер защиты** (т.п.).
- **Выявление уязвимостей:** Провести анализ уязвимостей.
- **Определение рисков:** Понять, какие риски являются наиболее значимыми с точки зрения человеческого фактора).

Шаг 2: Определение целей и приоритетов

На этом этапе важно сформулировать конкретные цели и приоритеты в области информационной безопасности. Например:

- Обеспечение конфиденциальности, целостности и доступности информации.
- Минимизация финансовых потерь от инцидентов.
- Соответствие законодательным требованиям.
- Повышение осведомленности сотрудников.

Шаг 3: Разработка политик и процедур

Создание четких политик и процедур является основой для эффективной работы. Следует разработать следующие документы:

- **Политика информационной безопасности.**
- **Процедуры реагирования на инциденты.**
- **Правила использования ИТ-ресурсов.**
- **План непрерывности бизнеса:** Включает в себя планы восстановления и обеспечения непрерывности бизнеса.

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)



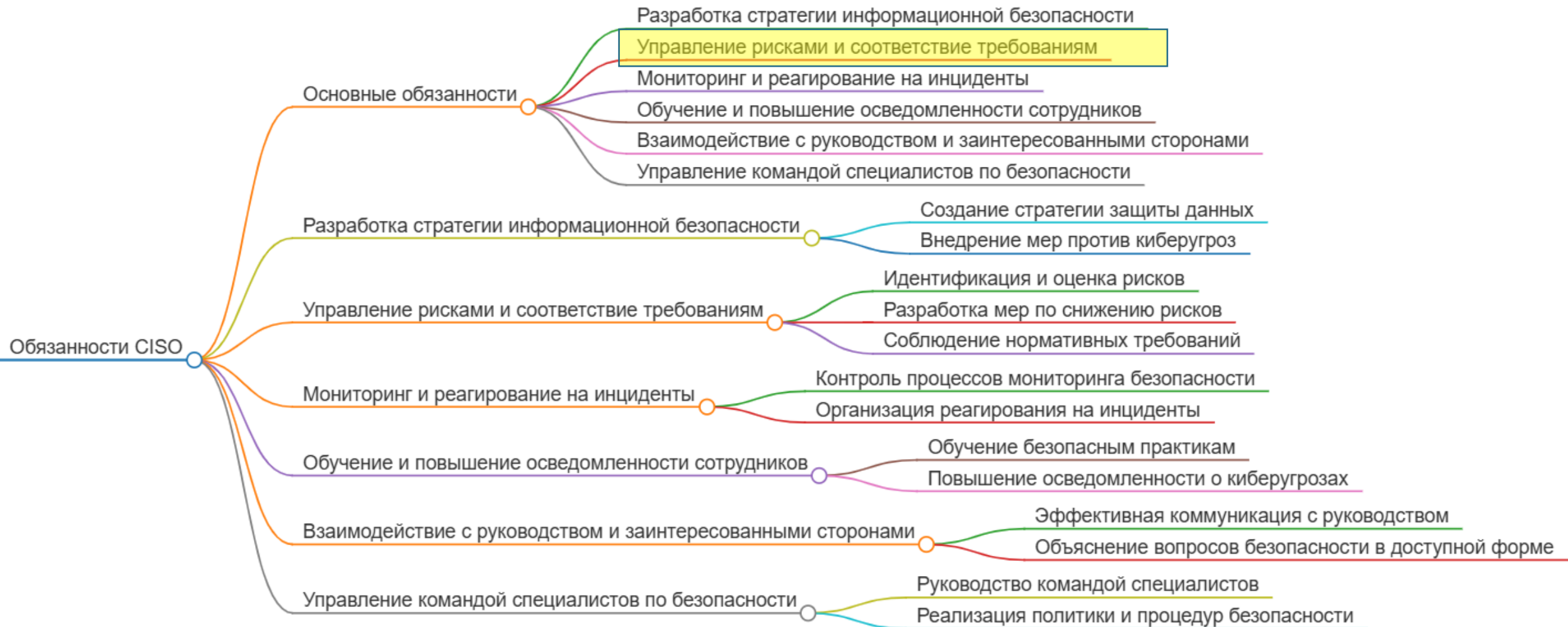
- Для работы с нейросетью лучше использовать отдельную учетную запись в браузере (отдельный браузер)
- Не отправляйте чат-боту никакие критичные (персональные, конфиденциальные и т.п.) данные
- Не загружайте документы компании, личные значимые документы
- Отправляете код? Почистите его от конфиденциальных 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 не было 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?

**Felo**
Исследуйте мир на с...

Добавить в тему

/ Как проводить оценку вреда в соответствии с приказом Роскомнадзора № 178

Начать новый вопрос

Коллекции

История записей

Сегодня

Сделай краткий обзор...

Вчера

Ключевые обязанности...

Действуй как эксперт...

Последние 7 дней

Что такое специальные...

что такое...

Как проводить оценку...

Ноябрь

Какие подзаконные...

Что было на первом...

Что такое проблема...

Как проанализировать...

попробовать Pro

Обновите до Felo Pro, чтобы получать...

Как проводить оценку вреда в соответствии с приказом Роскомнадзора № 178

Поиск по всей сети 15 источников 2 языков

Ответ готов

Для проведения оценки вреда в соответствии с приказом Роскомнадзора № 178 от 27 октября 2022 года, необходимо следовать установленным требованиям и процедурам. Вот основные шаги и аспекты, которые следует учитывать:

Основные требования к оценке вреда

- Определение степени вреда:** Оператор персональных данных должен определить степень возможного вреда, который может быть причинен субъектам данных в случае нарушения их прав. Это может включать как качественные, так и количественные оценки ^{4 8}.
- Составление акта оценки вреда:** Акт должен содержать:
 - Наименование или фамилию, имя, отчество (при наличии) и адрес оператора.
 - Дату издания акта.
 - Описание ситуации, приведшей к оценке вреда.
 - Выводы о степени вреда и рекомендации по его минимизации ^{3 6}.
- Формирование комиссии:** Оценка вреда может проводиться как ответственным лицом за обработку персональных данных, так и комиссией, созданной оператором. Комиссия должна включать специалистов, обладающих необходимыми знаниями и опытом в области защиты персональных данных ^{7 11}.

Источники

1 service.securitm.ru > docs > rkn-1...
Раздел Пункт 5. Приказа
Роскомнадзора № 178 - Контроль ...
Приказ Роскомнадзора № 178 от 27.10.2022.
Требования к оценке вреда, который может
быть причинен субъектам персональных...

2 gpra.pro > nra > rkn178_27.10.2022
Требования к оценке вреда, который
может быть причинен ...
Приказ Роскомнадзора от 27.10.2022 № 178
"Об утверждении Требований к оценке
вреда, который может быть причинен...

3 service.securitm.ru > docs > rkn-1...
Раздел Пункт 4. Приказа
Роскомнадзора № 178 - Контроль ...
[2022-12-12]
Дес 12, 2022 - Акт оценки вреда должен
содержать: наименование или фамилию,
имя, отчество (при наличии) и адрес...

Посмотреть еще 12 пунктов >

Рекомендуемое

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 опубликованных политик безопасности, которые могут быть полезны для организации информационных ресурсов. Вот несколько примеров и политик:

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

Эти документы обычно содержат правила и рекомендации по предотвращению несанкционированного доступа. Они могут быть адаптированы под нужды конкретной организации в зависимости от 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](#)

politika_inf_bezопасnosti_2024.pdf

1 / 10

100%

УТВЕРЖДЕНА
Приказом АО «Содружество»
от «11» 04 2024 № 146

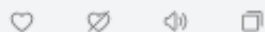
ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «СОДРУЖЕСТВО»

Комплаенс. Как помогает?

Доступны обновления, обновите страницу

politika_inf_bezопасnosti_2024.pdf

- Политика информационной безопасности АО "Содружество" была утверждена приказом генерального директора от 11 апреля 2024 года. Она устанавливает меры, процедуры и правила по защите информации в информационных системах компании. Основные цели этой политики включают обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение утечек данных, мониторинг событий безопасности и реагирование на инциденты. Для достижения этих целей проводятся различные мероприятия, такие как сбор информации о событиях информационной безопасности, выявление и анализ инцидентов, оперативное реагирование на них и минимизация негативных последствий. За соблюдение данной политики несут ответственность все пользователи информационных систем, а также администраторы безопасности и системные администраторы.



Что является основными объектами защиты в соответствии с этой политикой?

- В соответствии с политикой информационной безопасности АО "Содружество", основными объектами защиты являются:

1. **Информационные ресурсы**, которые содержат коммерческую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также информацию, необходимую для работы, независимо от формы и вида представления.
2. **Работники** АО "Содружество", которые являются разработчиками и пользователями информационных систем.
3. **Информационная инфраструктура**, которая включает системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, каналы информационного обмена и телекоммуникации, системы и средства защиты информации, а также объекты и помещения, где эти системы размещены.



Какие меры предпринимаются для обеспечения безопасности?

Кто несет ответственность за соблюдение политики?

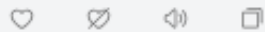
Как происходит реагирование на инциденты?

Комплаенс. Как помогает?

Доступны обновления, обновите страницу

politika_inf_bezopasnosti_2024.pdf

Политика информационной безопасности 2024 года. Она устанавливает меры, процедуры этой политики включают обеспечение конфиденциальности данных, мониторинг событий безопасности, мероприятия, такие как сбор информации, реагирование на них и минимизация негативного воздействия на информационные системы, а также администрирование.



В соответствии с политикой информационной безопасности:

1. **Информационные ресурсы**, содержащие конфиденциальную информацию, а также информацию ограниченного распространения, а также информацию, подлежащую защите;
2. **Работники** АО "Содружество", имеющие доступ к информации, подлежащей защите;
3. **Информационная инфраструктура**, включающая средства её обработки, передачи и отображения, а также объекты и помещения, в которых размещены такие средства.



2. Описание объекта защиты

Основными объектами защиты системы информационной безопасности является:

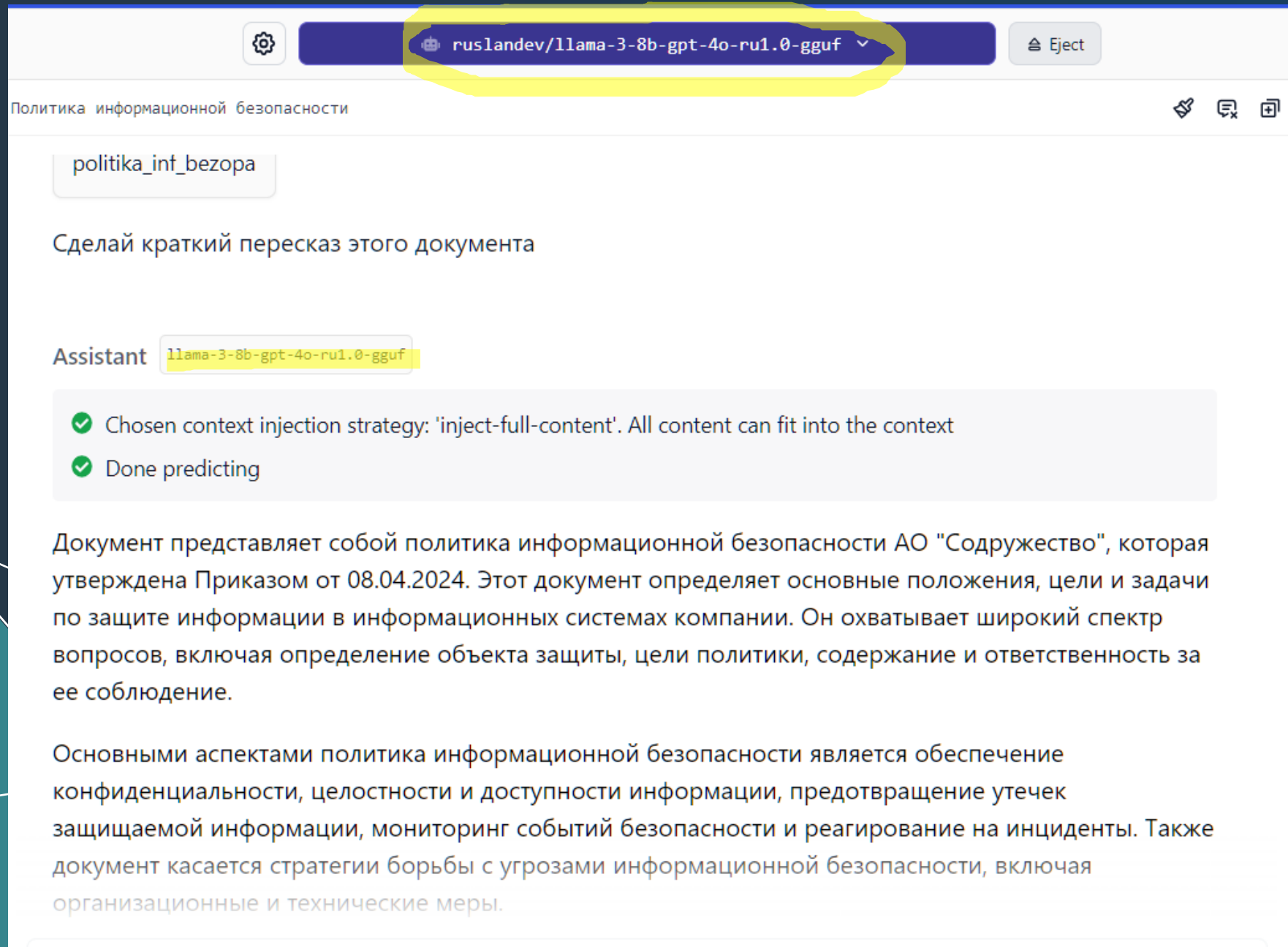
- **информационные ресурсы**, содержащие коммерческую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы, независимо от формы и вида представления;
- **работники АО «Содружество»**, являющиеся разработчиками и пользователями информационных систем АО «Содружество»;
- **информационная инфраструктура**, включающая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Какие меры предпринимаются для обеспечения безопасности?

Кто несет ответственность за соблюдение политики?

Как происходит реагирование на инциденты?

Комплаенс. Как помогает?



Политика информационной безопасности

politika_int_bezopa

Сделай краткий пересказ этого документа

Assistant llama-3-8b-gpt-4o-ru1.0-gguf

- ✓ Chosen context injection strategy: 'inject-full-content'. All content can fit into the context
- ✓ Done predicting

Документ представляет собой политика информационной безопасности АО "Содружество", которая утверждена Приказом от 08.04.2024. Этот документ определяет основные положения, цели и задачи по защите информации в информационных системах компании. Он охватывает широкий спектр вопросов, включая определение объекта защиты, цели политики, содержание и ответственность за ее соблюдение.

Основными аспектами политика информационной безопасности является обеспечение конфиденциальности, целостности и доступности информации, предотвращение утечек защищаемой информации, мониторинг событий безопасности и реагирование на инциденты. Также документ касается стратегии борьбы с угрозами информационной безопасности, включая организационные и технические меры.

Комплаенс. Как помогает?

 ruslandev/llama-3-8b-gpt-4o-ru1.0-gguf 

Политика информационной безопасности

You

На основе проведенного анализа напиши мне регламент проведения регулярных аудитов

Assistant llama-3-8b-gpt-4o-ru1.0-gguf

Регламент проведения регулярных аудитов для обеспечения информационной безопасности АО "Содружество"

1. Цели и задачи

Целью проведения регулярных аудитов является оценка эффективности и соответствия требованиям информации, управленческих процессов, а также системы информационной безопасности компании. Задачами аудита являются выявление потенциальных уязвимостей, нарушений политики конфиденциальности, несанкционированного доступа к данным, а также проверка соответствия действующему законодательству.

2. Обязанность проведения аудитов

Проведение регулярных аудитов возлагается на ответственное подразделение информационной безопасности, которое должно регулярно отчетливо докладывать о выполнении задач и обнаруженных проблемам руководству компании.

Type a message and press Enter to send ...

 ruslandev/llama-3-8b-gpt-4o-ru1.0-gguf 

Политика информационной безопасности

Проведение регулярных аудитов возлагается на ответственное подразделение информационной безопасности, которое должно регулярно отчетливо докладывать о выполнении задач и обнаруженных проблемам руководству компании.

3. Планирование аудита

- 1. Определение целей аудита:** В начале каждого цикла проведения аудитов необходимо четко определить цели и задачи, которые предстоит решить.
- 2. Предварительная подготовка:** Работники подразделения информационной безопасности проведут предварительные обследования для определения областей, требующих проверки.
- 3. Распределение обязанностей:** В рамках аудита каждый сотрудник должен знать свои задачи и responsibilities.

4. Процесс проведения аудитов

- 1. Сбор информации:** Сбор данных о состоянии систем информационной безопасности, включая логи, журналы, отчеты об инцидентах.
- 2. Анализ данных:** Анализ собранной информации для выявления уязвимостей и нарушений.

 ruslandev/llama-3-8b-gpt-4o-ru1.0-gguf 

Политика информационной безопасности

точности аудита.

7. Обновление регламента

Регламент проведения регулярных аудитов должен быть пересмотрен и обновлен не реже 1 раза в год, учитывая изменения законодательства, технологий и методов анализа информации.

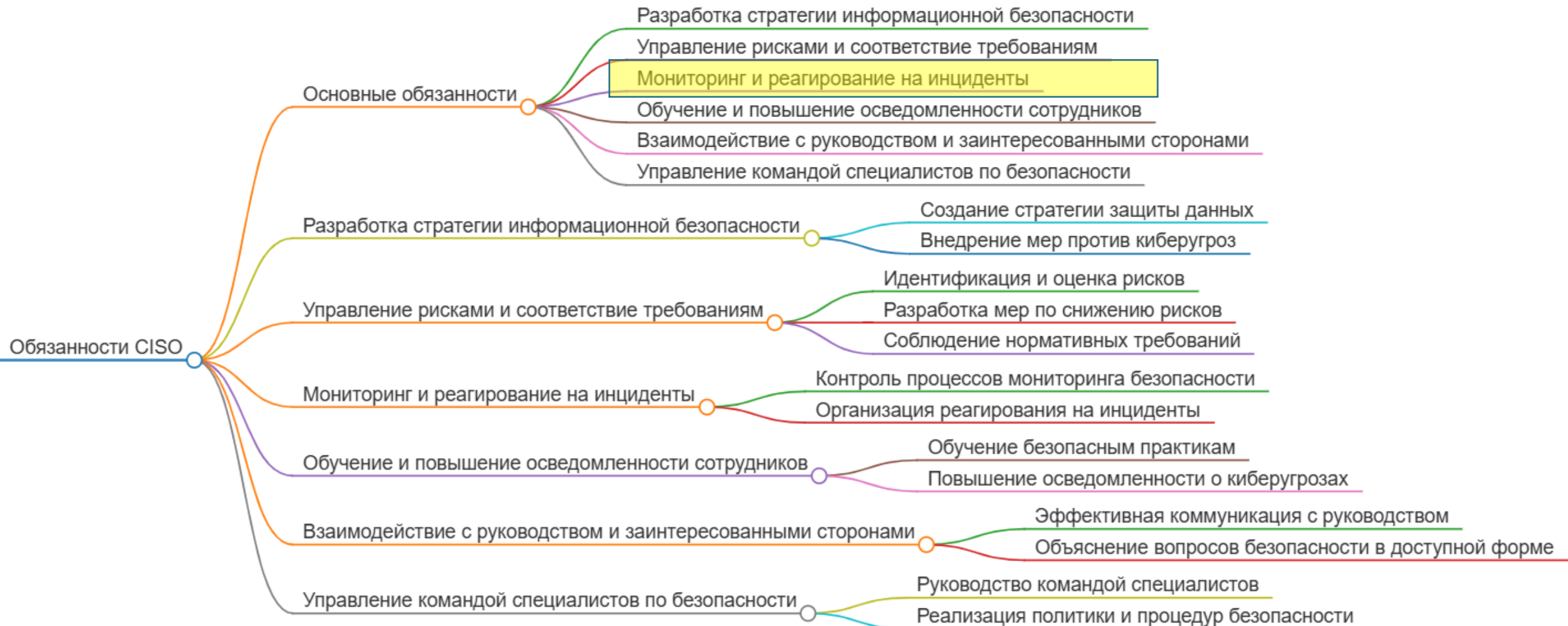
8. Конфиденциальность и доступ к данным

Все собранные данные при проведении аудита должны храниться в защищенных цифровых архивах, доступ к которым ограничен только сотрудниками подразделения информационной безопасности на основе необходимых задач.

9. Заключение

Проведение регулярных аудитов является ключевым аспектом обеспечения информационной безопасности АО "Содружество". Это позволяет своевременно выявлять и устранять угрозы, а также улучшать эффективность работы информационных систем компании.

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 реагирования 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 плейбуки?



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


|                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Сдерживание: блокировка каналов</li> <li>Ликвидация: шифрование данных</li> </ul>                                |
| <p><strong>Роли:</strong> DLP-аналитик, юрист</p> <p><strong>Инструменты:</strong> CASB, DLP</p> <p><strong>Коммуникация:</strong> Отчет регулятору</p> |



!-- Добавьте остальные строки по аналогии -->



* Полная версия таблицы включает все 12 категорий, кроме IoT/OT и физических инцидентов.


```

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:

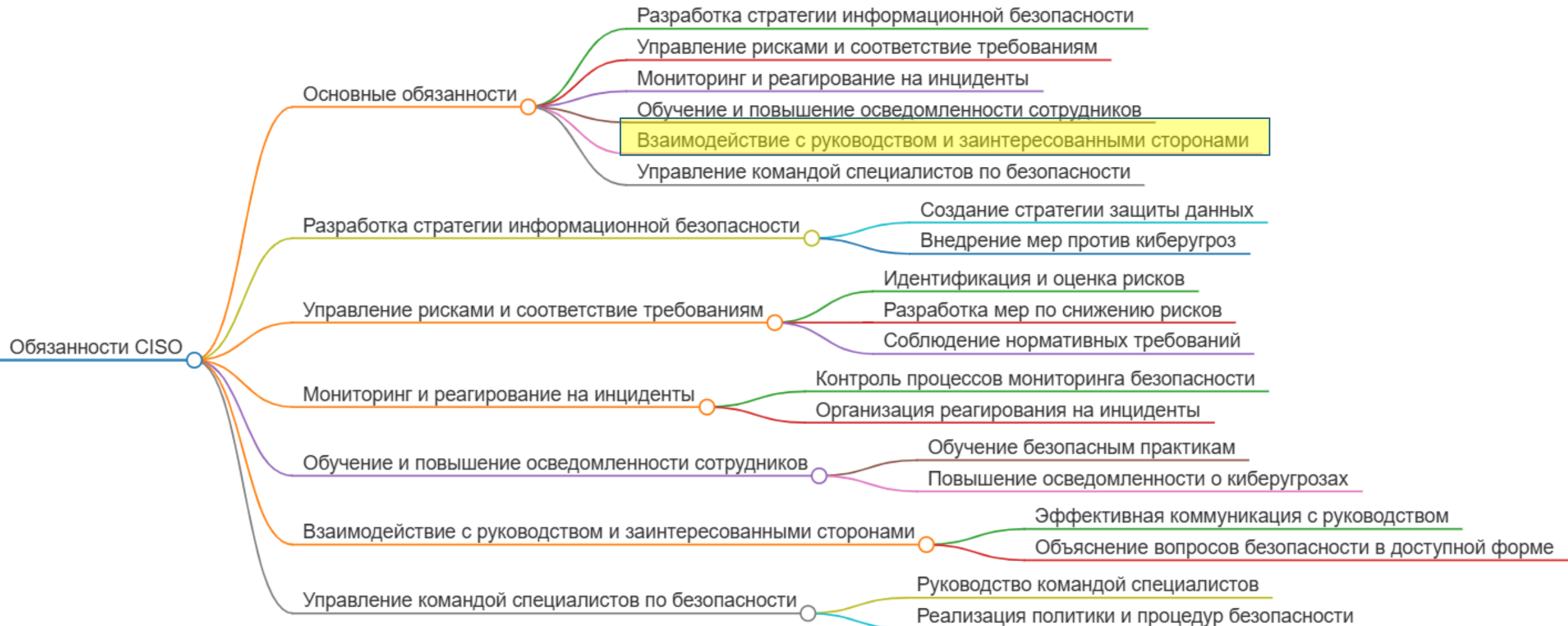
Границами

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?

Создавайте с помощью искусственного интеллекта

С чего начать?



Вставить текст
Создавайте на основе заметок, конспекта или существующего контента

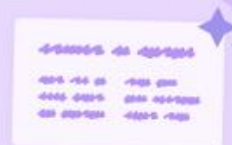
→



⚡ Популярное

Сгенерировать
Создание из однострочной подсказки за несколько секунд

→



Импортируйте файл или URL
Улучшайте существующие документы, презентации или веб-страницы.

→

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 <u>антифишинговых</u> тренировках□	21.10□	Выполнено□	□

Взаимодействие с руководством и заинтересованными сторонами. Как помогает?

 **Вставьте**

Добавьте заметки, конспект или содержание, которое Вы хотели бы использовать.

по развитию процессов информационной безопасности (далее по тексту – ИБ) дочерних (зависимых) обществ (далее по тексту – ДЗО на 2024 год

№ п/п

Результат

Срок

Отметка о выполнении

1

Проведена встреча с ДЗО по обсуждению особенностей реализации мероприятий плана

19.02

Выполнено

2

Проведена оценка необходимости внедрения:

- анализа исходного кода (SAST, DAST, SCA, Fuzzing) на наличие уязвимостей;

Что бы Вы хотели создать с помощью этого контента?

☒ Презентация

☐ Веб-страница

☐ Документ

По умолчанию

Продолжить →

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

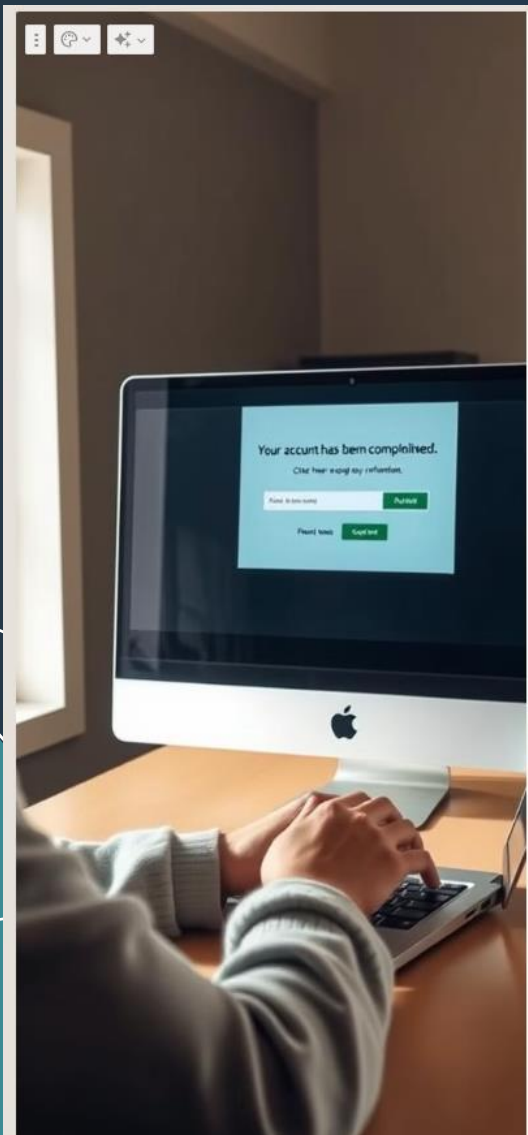
Проведен анализ договоров с третьими сторонами, касающихся информационных активов ДЗО.

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.

✓ Экспорт готов
Загрузка должна начаться автоматически. Если нет, [нажмите здесь, чтобы загрузить его.](#)

Поделился отчетом о выполнении плана мероприятий по развитию процессов информационной безопасности (ИБ) дочерних (зависимых) обществ (ДЗО) на 2024 год

Сотрудничайте Поделиться Экспорт Опубликовать на сайте...

</> Встроить

Загрузите статическую копию своего gamma, чтобы поделиться с другими.

- Экспорт в PDF
- Экспорт в PowerPoint
- Экспортируйте в формат PNG

Для правильного отображения шрифтов в PowerPoint могут потребоваться следующие шрифты:

DM Sans Inter

Совет: вы можете управлять размером карточки и фоном в [настройках страницы](#).

Скрыть значок "Made with Gamma" PLUS

[Просмотр аналитики](#) [Готово](#)

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 оформления 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!

CERTIFIED GPTLOGIST

Сертифицированный Жопотолог



Bitflect at Bic 9, GPTA loCILL GTPP uacF Ketao
GATEcnob AI

terminal.G010.10b 0:STOR010010R0111 GPICbugeisr0
all dig Biee dispe-P bllkay Rentary termiur to 0



Binary Code

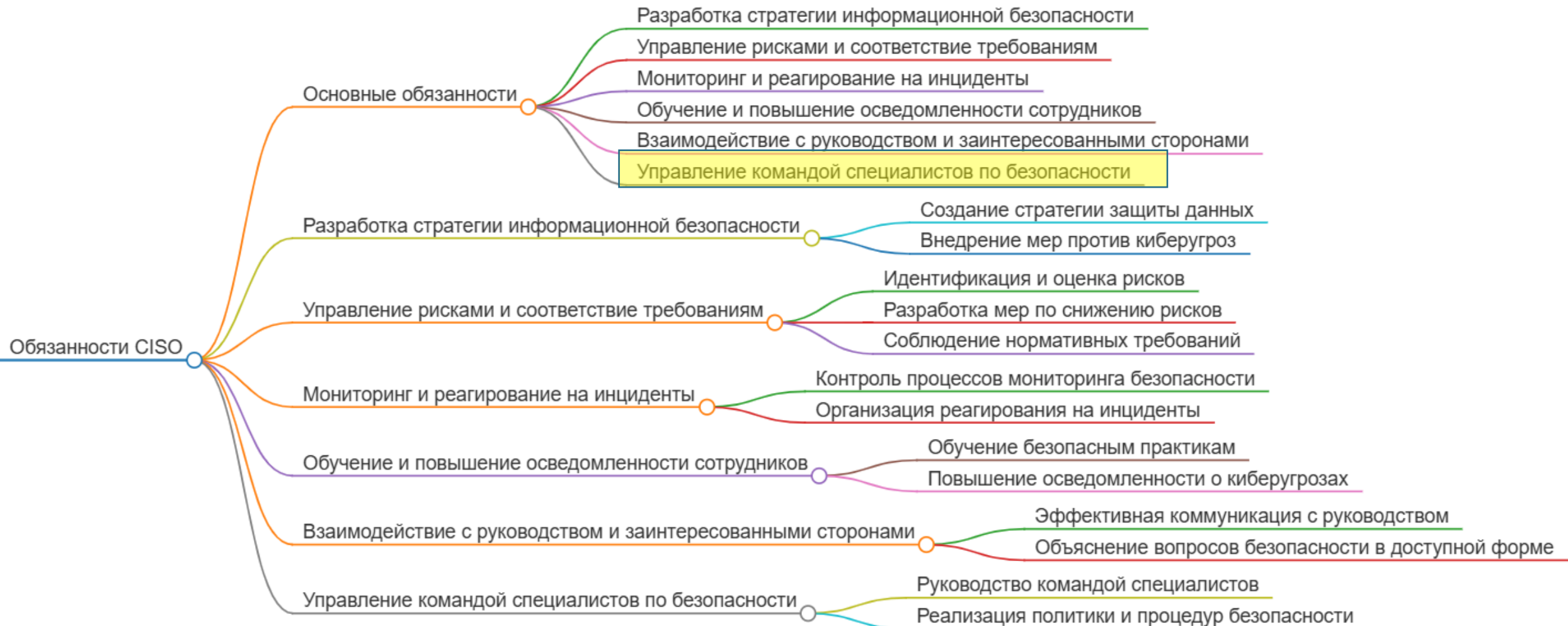
ACCESD OY CERTITLES TRBOO



Binary Rosel

CAOOSSED TO CSRTIDE TB00

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.

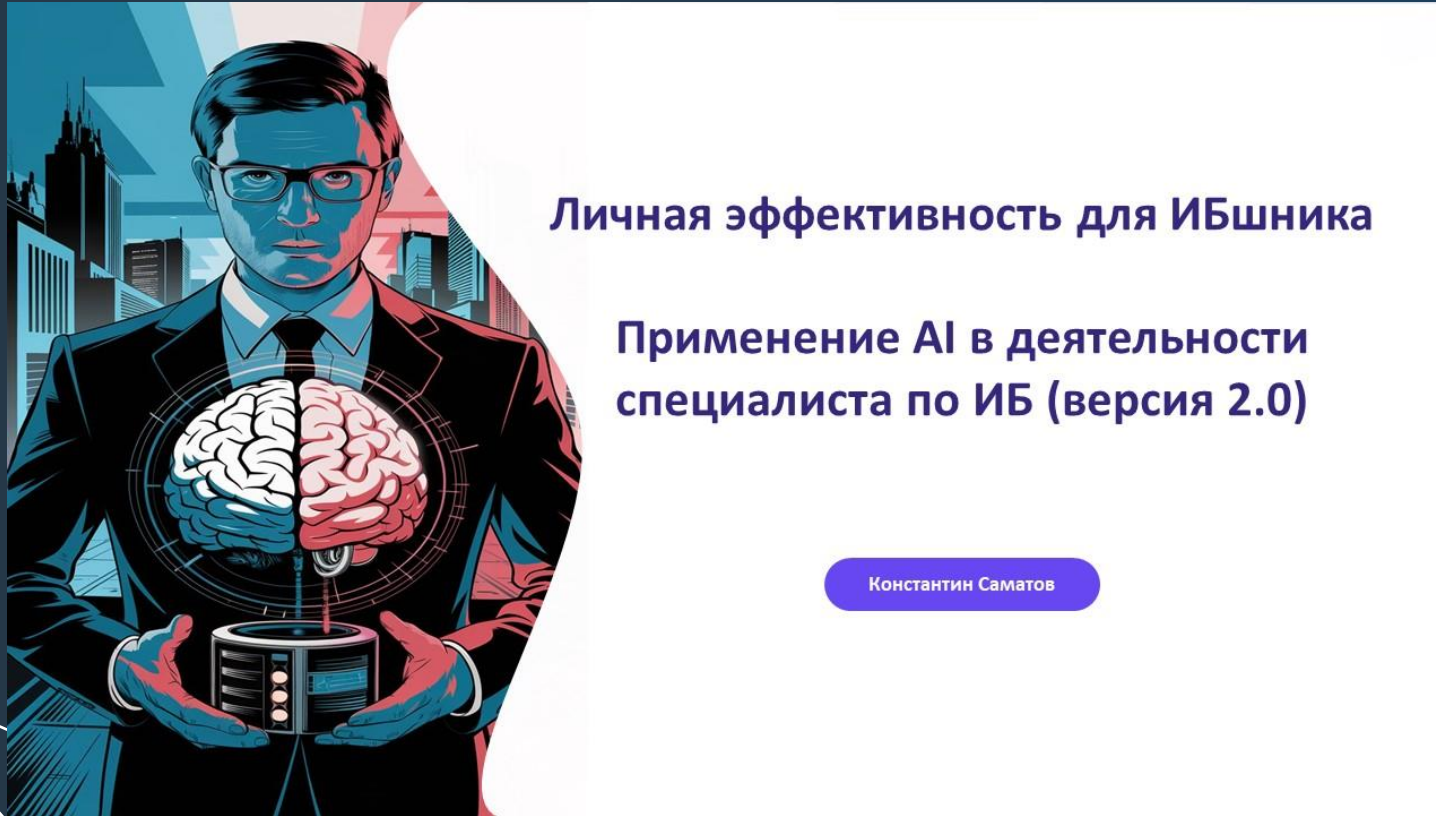
3. Первый месяц

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):

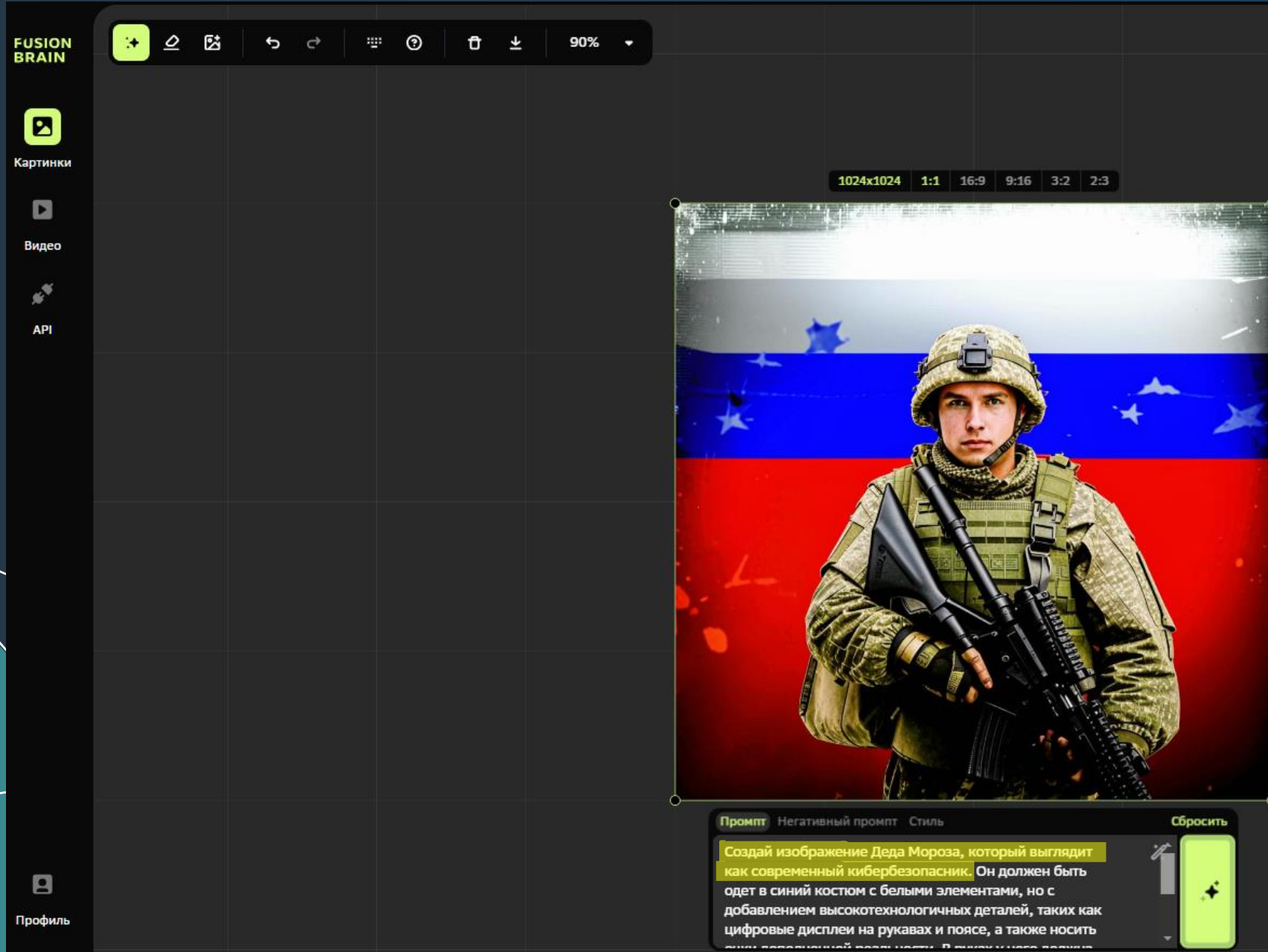
Создание текстов для корпоративных рассылок, слоганов или мотивационных сообщений.

Stable Diffusion (аналоги)

Подготовка поздравительных открыток

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):

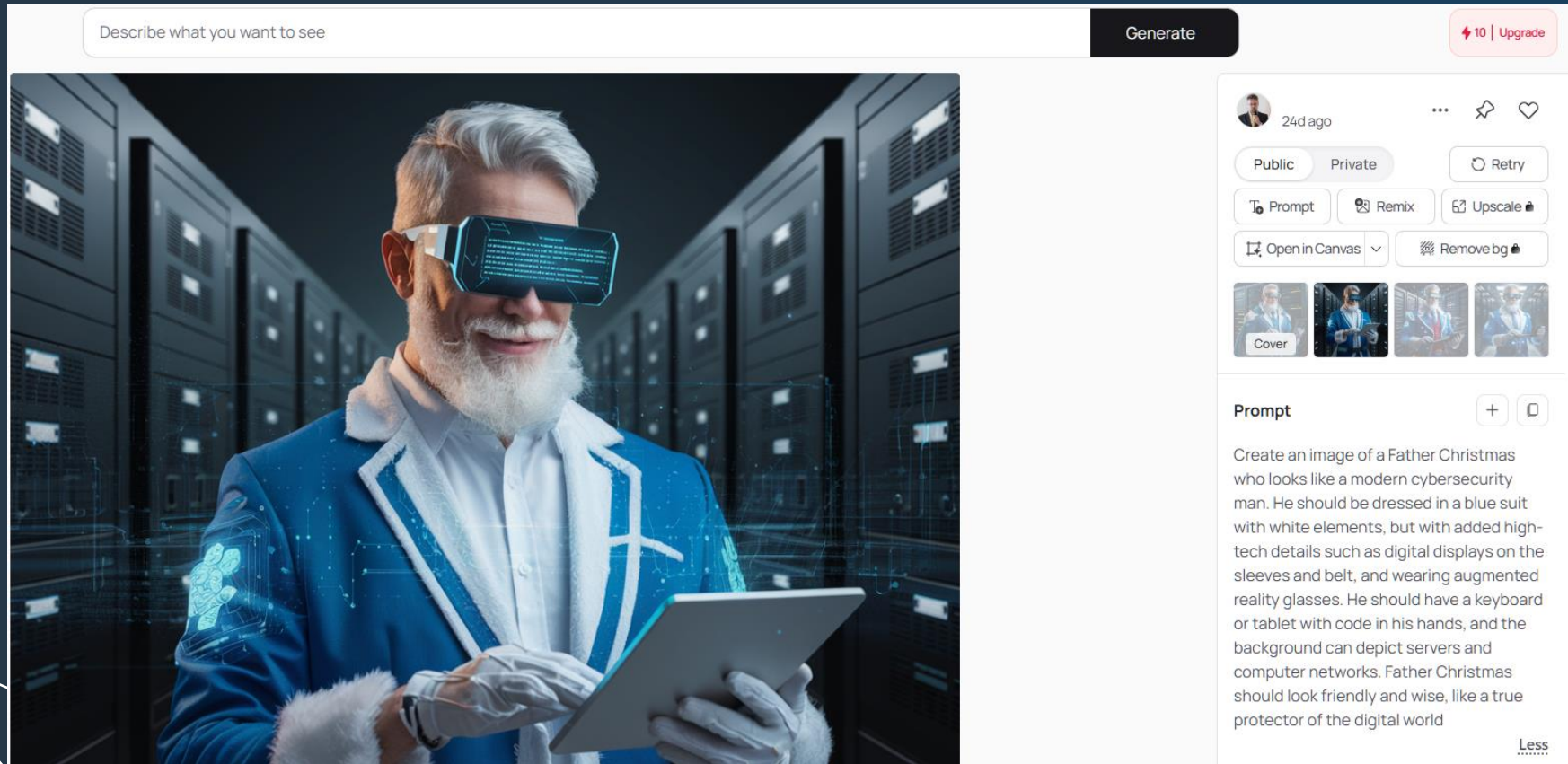
Создание текстов для корпоративных рассылок, слоганов или мотивационных сообщений.

Stable Diffusion (аналоги)

Подготовка поздравительных открыток

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):

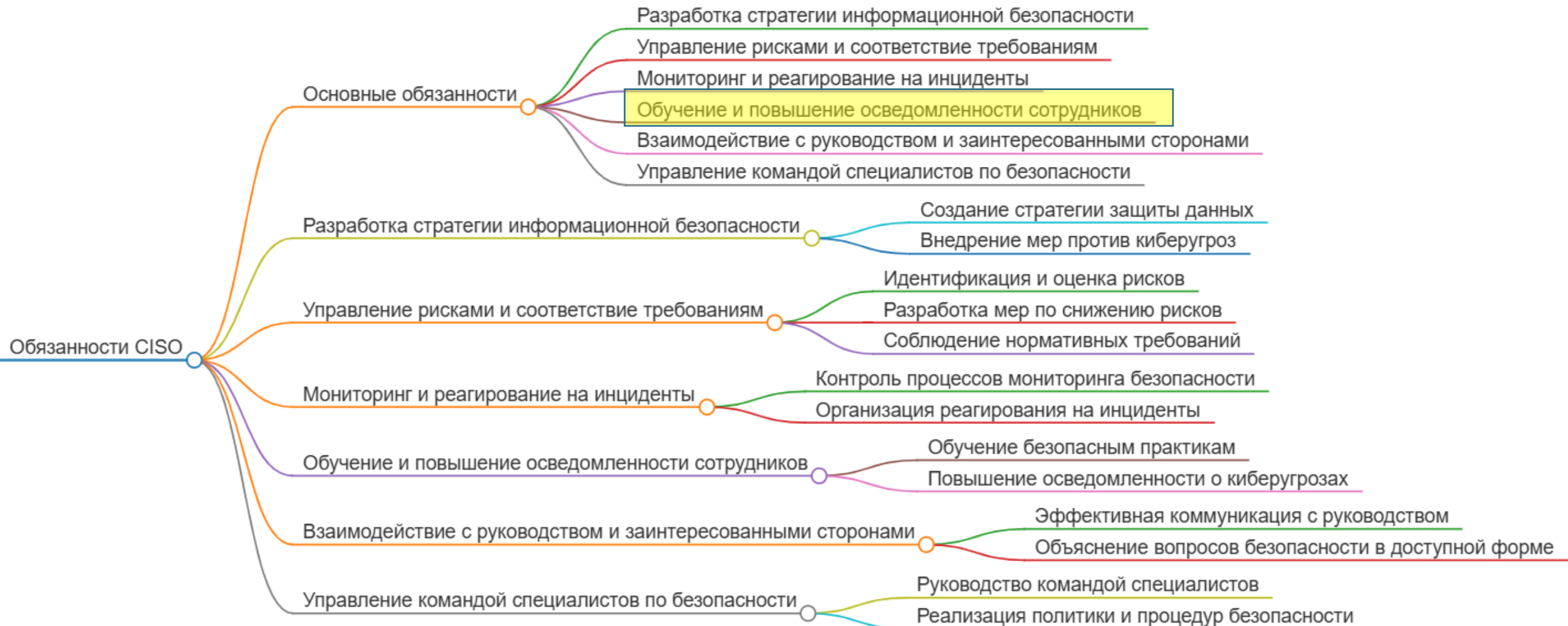
Создание текстов для корпоративных рассылок, слоганов или мотивационных сообщений.

Stable Diffusion (аналоги)

Подготовка поздравительных открыток

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