

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
ФГАОУ ВО »СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра «Прикладная математика
и информатика»

ОТЧЕТ
о выполнении индивидуального задания № 4 часть 2
по дисциплине
«ЦИФРОВЫЕ ТЕХНОЛОГИИ И МЕДИАБЕЗОПАСНОСТЬ»
Специализированная мастерская «ЦИФРОВОЙ ОФИС.
ПРОМТ-ИНЖИНИРИНГ ДЛЯ ПОВСЕДНЕВНЫХ ЗАДАЧ»

Вариант № 1

Выполнил:
студент группы ИИ/б-25-6-о
Заварзин А.В.

Проверили:
доцент кафедры ПМиИ
Ченгарь О.В.

Севастополь, 2025

Оглавление

Введение	4
Раздел 1. Подготовка текста гида по медиабезопасности	5
Шаг 1: Выбор цифровой угрозы.....	5
Шаг 2: Разработка исходного промта	6
Шаг 3: Тестирование промта	7
Шаг 4: Уточнение промта	9
Шаг 5: Сравнение ответов разных нейросетей.....	11
Шаг 6: Подготовка текста для гида	13
Выводы по работе	14
Раздел 2. Подготовка кейсов по медиабезопасности	15
Шаг 1: Поиск практического кейса по цифровой угрозе	15
Шаг 2: Разработка уточняющего промта по технологии RAG	18
Шаг 3: Разработка промта для подготовки информации для разных целевых групп	20
Выводы по работе	23
Раздел 3. Подготовка брендбука для гида кейсов по медиабезопасности	24
Шаг 4: Разработка концепции	24
Шаг 5: Создание метафорических иллюстраций	25
Шаг 6: Создание обложки гида	28
Шаг 7: Тематические иконки.....	32
Шаг 8: Анализ результатов и доработка	38
Выводы по работе	40

Раздел 4. Разработка UML-диаграмм для гида кейсов по медиабезопасности	41
Шаг 1: Подготовка и описание системы для диаграммы UseCase	41
Шаг 2: Генерация диаграммы прецедентов (Use Case).....	42
Шаг 3: Диаграмма классов (Class).....	44
Шаг 4: Диаграмма деятельности (Activity).....	50
Шаг 5: Диаграмма последовательности (Sequence)	52
Выводы по работе	55
Заключение	56
Список источников	57

Введение

Современное цифровое пространство, предоставляя неограниченные возможности для коммуникации, работы и доступа к информации, одновременно стало ареной для широкого спектра киберугроз. Среди них фишинг остаётся одной из наиболее распространённых, разрушительных и изощрённых техник социальной инженерии. Его опасность заключается не в эксплуатации уязвимостей программного обеспечения, а в манипуляции человеческим фактором — доверием, невнимательностью или недостатком знаний.

Фишинг-атаки имитируют легитимные коммуникации от известных организаций, коллег или знакомых с единственной целью — получить конфиденциальные данные: логины и пароли, банковские реквизиты, персональную информацию. Методы постоянно эволюционируют: от массовых рассылок писем до целевых атак на конкретных лиц или организации (spear-phishing), использования мессенджеров (смишинг) и телефонных звонков (вишинг).

Данный гид призван стать практическим инструментом для распознавания, предотвращения и противодействия фишинговым атакам. В нём систематизированы ключевые признаки фишинговых сообщений, описаны современные тактики злоумышленников и приведены чёткие алгоритмы действий при столкновении с угрозой. Цель — формирование осознанного и критического подхода к обработке входящей информации, что является фундаментом индивидуальной и корпоративной медиабезопасности.

Раздел 1. Подготовка текста гида по медиабезопасности

Шаг 1: Выбор цифровой угрозы

Согласно статье [Лаборатории «Касперского»](#) Фишинг - разновидность интернет-мошенничества, нацеленная на кражу конфиденциальной информации. В основном типичная фишинговая атака включает в себя отправку различными методами (например, через email, SMS, социальные сети, мессенджеры и пр.) ссылку на поддельную страницу ввода данных или страницу, с автоматической установкой вредоносного ПО.

С точки зрения злоумышленников фишинг разделется на массовый и целевой. Массовый фишинг рассыпается по всем доступным злоумышленникам адресам, тогда как целевой фишинг рассчитан на конкретных получателей, а подготовка к нему часто включает предварительный сбор данных о целях. Целевой фишинг, направленный на высокопоставленных лиц в компании, также называется китовый *фишинг* или *уэйлинг*.

Основной задачей фишинга является получение доступа к персональным данным жертвы, а также для получения финансовой выгоды.

Для заманивания пользователей на фишинговые сайты злоумышленники используют различные сообщения-«приманки», включая проблему с аккаунтом, сообщения от государственных органов, сообщения от представителей банка, специальные предложения, акции, розыгрыши, недоставленные письма или голосовые сообщения.

Борьба с фишингом очень проста – необходимо просто проверять информацию об отправителе письма, сверять корректность ссылок, не скачивать файлы из подозрительных писем и не вводить данные на подозрительных сайтах. В случаях, если пользователь не уверен в безопасности письма (например, от якобы сотрудника банка), необходимо позвонить на горячую линию банка и (или) посетить офис банка для того,

чтобы перепроверить информацию.

Шаг 2: Разработка исходного промта

- *Контекст*: необходимо указать, что я являюсь студентом первого курса, который работает над гидом по медиабезопасности для первокурсников.
- *Роль*: надо назначить ИИ роль эксперта по медиабезопасности, который может легко объяснить каждому человеку о поставленной проблеме без применения сложного профессионального сленга.
- *Инструкция*: надо попросить ИИ написать текст по следующему плану:
 - Дать описание фишинга
 - Выделить 3-5 признаков, по которым можно распознать фишинг
 - Дать 2-3 практических совета по защите
 - Обосновать достоверность информации
- *Специфика*: необходимо указать формат (маркированный список), объём текста (150-250 слов), стиль (дружелюбный, но предупредительный).
- *Целевая аудитория*: нужно указать, что текст предназначен для первокурсников.

Итоговый промт для нейросети DeepSeek будет выглядеть следующим образом:

Я студент первого курса, создаю цифровой гид по медиабезопасности для первокурсников. Моя цель – помочь им понять и избежать фишинговых писем от банков или служб доставки. Представь, что ты эксперт по кибербезопасности, который умеет объяснять сложные вещи простым языком.

Подготовь текст, который:

- Описывает, что такое фишинг-письма (что это, как работают).
- Указывает 3-5 признаков, по которым можно распознать фишинг.
- Обосновывает достоверность информации (на чем основаны выводы).
- Дает 3 практических совета, как защититься.

Текст должен быть в формате маркированного списка, объемом 150-250 слов, в дружелюбном, но предупреждающем тоне, без сложного жаргона.

Шаг 3: Тестирование промта

Нейросеть DeepSeek выдала следующий ответ:

Привет, первокурсник! Добро пожаловать в университетскую жизнь, где, к сожалению, кроме учебы, нужно быть начеку и в цифровом пространстве. Давай разберемся, что такое фишинг и как не попасться на удочку мошенников.

Что такое фишинг? Это мошеннические письма или сообщения, которые маскируются под официальные уведомления от банков, курьерских служб, соцсетей или даже вуза. Их цель — выманить у тебя конфиденциальные данные: логины, пароли, данные карты или коды из SMS. Работает это просто: тебя пугают или сулят выгоду, чтобы ты перешел по вредоносной ссылке и ввел свои данные на фальшивом сайте.

Как распознать угрозу? Обрати внимание на эти признаки:

- Давление и срочность. Сообщение создает искусственную панику: «Срочно подтвердите аккаунт!», «Ваша посылка заблокирована, счет будет аннулирован через 2 часа!». Это делается, чтобы ты действовал быстро, не думая.
- Подозрительные ссылки и адреса. Наведи курсор на ссылку (не кликая!), и ты увидишь настоящий адрес. Если он не совпадает с официальным сайтом банка или службы (например, ведет на best-bank-security.ru вместо sber.ru) — это стопроцентный фишинг.
- Ошибки и нетипичные приветствия. Официальные письма от крупных компаний тщательно проверяются. Обилие грамматических ошибок, странные обращения («Уважаемый клиент Сбера») — яркий красный флаг.
- Незапрашиваемые вложения. Никогда не открывай вложения в письмах от неизвестных отправителей — они могут содержать вирусы.

3 простых правила защиты:

1. Не переходи по ссылкам из писем и SMS. Если пришло уведомление от банка или службы доставки, открой официальное приложение на своем телефоне или сайт, введя адрес вручную. Там и проверь информацию.
2. Включи двухфакторную аутентификацию (2FA) везде, где это возможно. Это добавит дополнительный уровень защиты, даже если мошенники узнают твой пароль.
3. Доверяй, но проверяй. Сомневаешься в письме? Найди официальный раздел службы поддержки на сайте компании и позвони им, чтобы уточнить информацию.

Почему этой информации можно доверять? Эти правила являются золотым стандартом кибербезопасности и рекомендуются ведущими экспертами и организациями по всему миру, такими как Лаборатория Касперского и SafeNet. Они основаны на анализе миллионов кибератак каждый год.

На основе ответа нейросети был проведён анализ по следующим пунктам: *полнота, логика, достоверность, соответствие спецификации*.

1. *Полнота.* Нейросеть DeepSeek раскрыла тему, дала описание проблемы. Привела примеры проявления фишинга и предложила несколько способов предотвращения фишинга.
2. *Логика.* Нейросеть рассуждала и дала довольно логический ответ. Противоречий в её тексте не обнаружено. Советы не являются ошибочными.
3. *Достоверность.* Нейросеть DeepSeek указала источники информации (в конце ответа написаны 2 источника, на которые она опиралась: «Лаборатория Касперского» и организация «SafeNet». Оба источника – достоверны). Также в её ответе присутствует логика в действиях по предотвращению фишинга.
4. *Соответствие спецификации.* Нейросеть DeepSeek не справилась с объёмом текста (из поставленных в условиях границах 150-250 слов она выдала ответ объёмом в 320 слов). Формат и стиль соответствуют

требованию в промте. Язык общения подходит для первокурсников: в тексте не используется сложный сленг, а сам ответ довольно дружелюбен, но содержит и предупредительную спецификацию.

Теперь необходимо сравнить ответ нейросети с базовой информацией из Шага 1. В ответе нейросети DeepSeek не обнаружено несовпадений с описанием проблемы, способами её решения и примерами проявления. Также отсутствуют ошибочные суждения.

Шаг 4: Уточнение промта

Анализируя ответ нейросети DeepSeek, был сделан вывод: нейросеть не справилась с объёмом текста. Но в целом её ответ удовлетворяет условия выполнения задачи по созданию гида.

Для исправления объёма текста был сформирован новый промт с уточнением, в котором было чётко указана граница в 150-250 слов:

Я студент первого курса, создаю цифровой гид по медиабезопасности для первокурсников. Моя цель – помочь им распознавать фишинговые письма от банков или служб доставки. Представь, что ты эксперт по кибербезопасности, который объясняет просто и понятно.

Подготовь текст:

– Опиши, что такое фишинг-письма (что это, как работают, пример реальной ситуации).

– Укажи 3-5 конкретных признаков фишинга (например, подозрительные ссылки, орфографические ошибки).

– Дай 3 практических совета, как защититься (например, что проверить перед кликом).

– Обоснуй достоверность, ссылаясь на общизвестные факты или стандарты, а также на исследования крупных ИТ-компаний, занимающихся кибербезопасностью и оставь ссылки на статьи, которые послужат опорой для написания гида.

Текст – маркированный список, с чётким объёмом 150–250 слов, дружелюбный, но предупреждающий тон, только простые слова.

Ответ нейросети DeepSeek на уточнённый промт:

На основе ответа, полученного после ввода уточнённого промта, было проведено сравнение. Вывод сравнения: нейросеть DeepSeek Что такое фишинг?

Это мошенническая рассылка, где вам под видом банка, курьера или

соцсети присылают письмо или сообщение. Цель — выманить ваши логины, пароли или данные карты. Представьте: вы получаете письмо от «Службы доставки» о проблеме с посылкой. Вас просят нажать на ссылку и «подтвердить данные», а на сайте ввести адрес и данные карты для «проверки». Это ловушка!

Как его сразу распознать? Вот главные признаки:

- Подозрительный адрес отправителя: Присмотритесь к email. Письмо от «СберБанка» будет не с ящика sberbank-help@gmail.com, а с официального домена, например, @sberbank.ru.
- Ссылки, ведущие не туда: Наведите курсор на кнопку (не нажимая!). Во всплывающей подсказке вы увидите настоящий адрес. Если это не сайт банка, а набор случайных букв — это обман.
- Ощущение срочности и угрозы: «Срочно обновите данные, иначе счет заблокируется!». Так создают панику, чтобы вы перестали мыслить здраво.
- Орфографические ошибки и странный стиль: Крупные компании тщательно проверяют свои письма.

3 простых правила защиты:

1. Не кликайте сразу. Всегда проверяйте отправителя и ссылки.
2. Не паникуйте. Ни один настоящий банк не будет блокировать счет через email.
3. Вводите данные только на официальных сайтах. Наберите адрес сайта вручную в браузере или перейдите из приложения.

Почему это важно?

По данным Kaspersky, фишинг — причина более 90% утечек данных. Это не «страшилки», а ежедневная реальность.

Источники для углубленного изучения:

- Статья о фишинге от Лаборатории Касперского (<https://www.kaspersky.ru/resource-center/threats/spam-phishing>) исправила свою ошибку в объеме текста, а также добавила ссылку,

указывающую на источник, на который опирается гид.

Шаг 5: Сравнение ответов разных нейросетей

Для сравнения результата работы разных нейросетей была выбрана вторая нейросеть YandexGPT. Она примечательная тем, что её алгоритм работы выстроен немного иначе, чем у DeepSeek и Grok. Также на выбор повлиял интерес к сравнению зарубежной и отечественной нейросети, ведь YandexGPT – российская разработка.

В качестве промта был введён уточнённый промт из Шага 4.

Ответ нейросети YandexGPT:

Фишинговые письма — это мошеннические сообщения, которые выглядят как настоящие письма от банков, служб доставки или других организаций. Они созданы для того, чтобы заставить вас раскрыть личные данные, например, пароли или номера банковских карт. Фишинговые письма часто содержат ссылки на поддельные сайты, которые имитируют настоящие.

Признаки фишинга:

- подозрительные ссылки, которые не соответствуют адресу организации;
- орфографические и грамматические ошибки в тексте письма;
- слишком настойчивые просьбы выполнить какое-то действие (например, срочно перейти по ссылке);
- просьбы подтвердить личные данные;
- неожиданное предложение о крупных суммах или выгодных условиях.

Советы, как защититься:

1. Не переходите по ссылкам из подозрительных писем. Лучше самостоятельно зайдите на официальный сайт организации через проверенный браузер.
2. Проверяйте адрес отправителя: убедитесь, что письмо действительно отправлено с официального адреса банка или службы доставки.
3. Будьте осторожны с просьбами подтвердить личные данные —

настоящие организации не будут просить вас делать это через письмо.

Достоверность: информация основана на общепринятых фактах и рекомендациях экспертов по кибербезопасности. Для более подробной информации можно обратиться к статьям на сайтах крупных ИТ-компаний, таких как Microsoft, Google, Norton и других.

Проведём сравнение ответов двух нейросетей по пунктам *полнота, логика, достоверность, соответствие спецификации*:

1. *Полнота.* Обе нейросети дали довольно полный ответ, с описанием проблемы фишинга, примерами его проявления и способами решения проблемы фишинга.
2. *Логика.* В работе обеих нейросетей не было выявлено нелогический советов и примеров. Также не были обнаружены ложные сведения и советы.
3. *Достоверность.* Все две нейросети указали источники, на которые опирались, при написании гида, но нейросеть DeepSeek указала ссылку на конкретную страницу (статью), что даёт понимание того, как и на что опиралась нейросеть при написании ответа.
4. *Соответствие спецификации.* Обе нейросети соблюдали структуру гида, привели примеры проявления фишинга и дали 3 совета для решения проблемы фишинга. Также обе нейросети справились с объёмом слов в тексте (216 слов у DeepSeek и 177 слов у YandexGPT).

На основе сравнения ответов двух нейросетей (DeepSeek и YandexGPT), можно сделать вывод, что нейросеть DeepSeek справилась со своей задачей чуть лучше, но и YandexGPT выполнила большинство условий, за исключением указания конкретных ссылок на статьи, на которые она опиралась при ответе.

Шаг 6: Подготовка текста для гида

Гид будет составлен на основе ответа нейросети DeepSeek, ведь она дала более полный ответ на поставленную задачу. Итоговый ответ нейросети будет отредактирован и дополнен с точки зрения орфографии и корректности описания, примеров и советов по решению проблемы.

Итоговый вариант гида:

Что такое фишинг?

Фишинг - это мошенническая рассылка, где Вам под видом банка, курьера или соцсети присылают письмо или сообщение. Цель — выманить Ваши логины, пароли или данные карты. Представьте: Вы получаете письмо от «Службы доставки» о проблеме с посылкой. Вас просят нажать на ссылку и «подтвердить данные», а на сайте ввести адрес и данные карты для «проверки». Это ловушка!

Как его сразу распознать? Вот главные признаки:

- Подозрительный адрес отправителя: Присмотритесь к email. Письмо от «СберБанка» будет не с ящика sberbank-help@gmail.com, а с официального домена, например, @sberbank.ru.
- Ссылки, ведущие не туда: Наведите курсор на кнопку (не нажимая!). Во всплывающей подсказке вы увидите настоящий адрес. Если это не сайт банка, а набор случайных букв — это обман.
- Ощущение срочности и угрозы: «Срочно обновите данные, иначе счет заблокируется!». Так создают панику, чтобы вы перестали мыслить здраво.
- Орфографические ошибки и странный стиль: Крупные компании тщательно проверяют свои письма.

3 простых правила защиты:

1. Не кликайте сразу. Всегда проверяйте отправителя и ссылки.
2. Не паникуйте. Ни один настоящий банк не будет блокировать счет через email и без Вашего подтверждения.

3. Вводите данные только на официальных сайтах. Наберите адрес сайта вручную в браузере или перейдите из официального приложения банка или службы доставки.

Почему фишинг - это важно?

По данным Kaspersky, фишинг — причина более 90% утечек данных. Это не «страшилки», а ежедневная реальность.

Источники для углубленного изучения:

Статья о фишинге от Лаборатории Касперского (
<https://www.kaspersky.ru/resource-center/threats/spam-phishing>)

Выводы по работе

В ходе работы были рассмотрены варианты написания гида с использованием нейросетей и собственно найденных источников информации. Также в ходе выполнения работы были изучены методы и правила взаимодействия с нейросетями и источниками информации из сети Интернет. Ещё были получены практические навыки работы с нейросетями, работы с проверкой ответов нейросетей и работы с написанием и редактированием промтов для нейросетей.

Раздел 2. Подготовка кейсов по медиабезопасности

Шаг 1: Поиск практического кейса по цифровой угрозе

Для описания трёх реальных кейсов о случаях применения фишинга был использован следующий промпт, который в последствии был загружен в нейросеть Grok:

Ты преподаватель по кибербезопасности, найди три примера мошенничества с помощью фишинга. Примеры должны быть из надежных источников, каждый с гиперссылкой на источник

Кейс 1: Фишинговая кампания с использованием Google Forms против пользователей криптокошельков

Описание:

Злоумышленники рассылали жертвам, в основном владельцам криптокошельков, письма с уведомлением о «подозрительной активности». В письме содержалась ссылка на форму, внешне неотличимую от легитимной Google Forms. Форма запрашивала мнемоническую фразу (сид-фразу) от кошелька, что является сверхконфиденциальной информацией. Получив ее, мошенники получали полный контроль над кошельком и выводили все средства.

Ключевые признаки фишинга:

- Использование доверенного бренда (Google) для прикрытия.
- Запрос критически важных данных, которые настоящий сервис никогда не запрашивает по почте.
- Целевой характер атаки (таргетинг на конкретную группу пользователей).

Источник:

Компания Halborn, специализирующаяся на безопасности блокчейн-проектов, детально разобрала эту атаку. Ссылка на статью Halborn "Crypto Wallet Phishing Scam Using Google Forms":

<https://www.halborn.com/blog/post/warning-active-metamask-phishing-campaign>.

Кейс 2: Массовый фишинг через поддельные уведомления от Microsoft

Описание:

Одна из самых распространенных и успешных фишинговых схем. Пользователи получают письмо, якобы от Microsoft, с предупреждением о «неудачных попытках входа» или «необходимости проверить активность». Ссылка в письме ведет на фишинговый сайт, который в точности копирует страницу входа Microsoft. Когда пользователь вводит свои учетные данные, они сразу же перехватываются злоумышленниками. Эти логины и пароли затем используются для кражи данных, рассылки спама или атак на корпоративные сети.

Ключевые признаки фишинга:

- Создание ощущения срочности и угрозы («Ваша учетная запись будет заблокирована!»).
- Поддельный адрес отправителя и домен сайта, похожий, но не идентичный настоящему (например, microsoft-security.com вместо microsoft.com).
- Запрос учетных данных после перехода по ссылке из письма.

Источник:

Cofense (ранее PhishMe) — ведущий поставщик решений для защиты от фишинга. Их база знаний содержит множество подобных примеров. Ссылка на описание фишинга Microsoft в блоге Cofense: <https://cofense.com/knowledge-center-hub/real-phishing-email-examples>.

Кейс 3: Целевой фишинг (китобойный) на сотрудников через LinkedIn

Описание:

В этой целевой атаке, известной как «китобойный промысел» (whaling), мошенники тщательно выбирали высокопоставленных сотрудников компаний. Используя LinkedIn, они собирали информацию о целевых лицах (имя, должность, круг общения). Затем жертве приходило изощренное письмо, якобы от генерального директора или другого руководителя, с просьбой срочно перевести крупную сумму денег на определенный счет для «секретной сделки». Из-за авторитета отправителя и убедительности письма многие сотрудники выполняли указание, не перепроверяя информацию.

Ключевые признаки фишинга:

- Высокая персонализация (использование реальных имен и должностей).
- Социальная инженерия (имитация авторитетной фигуры).
- Тема, требующая конфиденциальности и безотлагательных действий, в обход стандартных процедур.

Источник:

ФБР (Federal Bureau of Investigation) регулярно публикует предупреждения о схемах бизнес-компрометации через электронную почту (BEC). Их пресс-релизы основаны на реальных расследованиях. Ссылка на пресс-релиз ФБР о схемах BEC: <https://www.ic3.gov/PSA/2024/PSA240911>.

Шаг 2: Разработка уточняющего промт по технологии RAG

Для подробного разбора и комментирования вышеприведённых практических кейсов по фишингу был разработан уточняющий промпт по технологии RAG:

```
<documents>
```

```
  <document id="1">
```

Источник: Компания Halborn, специализирующаяся на безопасности блокчейн-проектов, детально разобрала эту атаку.

Описание: Злоумышленники рассылали жертвам, в основном владельцам крипто кошельков, письма с уведомлением о «подозрительной активности». В письме содержалась ссылка на форму, внешне неотличимую от легитимной Google Forms. Форма запрашивала мнемоническую фразу (сид-фразу) от кошелька, что является сверхконфиденциальной информацией. Получив ее, мошенники получали полный контроль над кошельком и выводили все средства.

```
  </document>
```

```
  <document id="2">
```

Источник: Cofense (ранее PhishMe) — ведущий поставщик решений для защиты от фишинга.

Описание: Одна из самых распространенных и успешных фишинговых схем. Пользователи получают письмо, якобы от Microsoft, с предупреждением о «неудачных попытках входа» или «необходимости проверить активность». Ссылка в письме ведет на фишинговый сайт, который в точности копирует страницу входа Microsoft. Когда пользователь вводит свои учетные данные, они сразу же перехватываются злоумышленниками. Эти логины и пароли затем используются для кражи данных, рассылки спама или атак на корпоративные сети.

```
  </document>
```

```
  <document id="3">
```

Источник: ФБР (Federal Bureau of Investigation).

Описание: В этой целевой атаке, известной как «китобойный промысел» (whaling), мошенники тщательно выбирали высокопоставленных сотрудников компаний. Используя LinkedIn, они собирали информацию о целевых лицах (имя, должность, круг общения). Затем жертве приходило изощренное письмо, якобы от генерального директора или другого руководителя, с просьбой срочно перевести крупную сумму денег на определенный счет для «секретной сделки». Из-за

авторитета отправителя и убедительности письма многие сотрудники выполняли указания, не перепроверяя информацию.

</document>

</documents>

Инструкция для ассистента:

1. Используй ТОЛЬКО информацию из предоставленных документов.

2. Если в документах нет ответа на вопрос – сообщи, что информация отсутствует.

3. Для каждого факта указывай номер документа-источника в квадратных скобках, например [1].

4. Отвечай на русском языке, просто и понятно для новичков.

Вопрос пользователя:

"Вы получаете письмо от «Службы безопасности Microsoft» с логотипом. В письме сказано, что о «неудачных попытках входа» или «необходимости проверить активность», и для ее проверки нужно «подтвердить данные» по ссылке. Ссылка ведет на сайт security-of-microsoft.com. Это фишинг?"

Нейросеть DeepSeek дала следующий ответ:

Да, это классический фишинг. Вот как это работает, основываясь на предоставленных документах:

Схема атаки: Вы получили письмо, которое в точности повторяет одну из самых распространенных и успешных фишинговых схем, описанных экспертами [2].

Метод обмана: В письме используется предлог "неудачных попыток входа" или "необходимости проверить активность", чтобы вызвать у вас беспокойство и заставить действовать быстро, не думая [1].

Цель атаки: Ссылка в письме ведет на поддельный сайт, который выглядит как настоящая страница входа Microsoft. Если вы введете там свои логин и пароль, эти данные сразу же попадут к мошенникам [2]. Затем злоумышленники используют их для кражи вашей информации, рассылки спама от вашего имени или атак на корпоративные сети [2].

Что делать? Ни в коем случае не переходите по ссылке и не вводите свои данные. Настоящие компании, такие как Microsoft, никогда не рассылают

письма с просьбой "подтвердить" или "проверить" пароль по ссылке в подобном письме.

Простое правило: Всегда внимательно проверяйте адрес сайта, на который вас ведут. Название security-of-microsoft.com — это подделка, созданная чтобы обмануть доверие к бренду Microsoft. Удалите это письмо.

Шаг 3: Разработка промт для подготовки информации для разных целевых групп

Для представления информации о фишинге для разных целевых групп был разработан промпт на основе технологии Automatic Reasoning prompt. Получился следующий промт для нейросети DeepSeek:

Привет. Я студент первого курса. Я создаю свой гид по медиабезопасности по угрозе Фишинг.

Задача:

Представь, что ты — эксперт по кибербезопасности, который умеет адаптировать информацию под разные целевые аудитории.

Шаги решения:

- 1) Найди 3 реальных практический кейса противодействия угрозе "фишинг".
- 2) Для каждого кейса сформулируй алгоритмы противодействия на языке, понятном для каждой целевой аудитории (Школьник 7 класса, Пожилой человек, Научный сотрудник).
- 3) Обоснуй почему кейсы подходят для аудитории.
- 4) Сформируй результаты в виде таблицы (колонки - аудитории, строки - кейсы).

Данный промпт был создан на основе технологии Automatic Reasoning prompt с элементами Role Promting. Он включает в себя чётко поставленную задачу и шаги решения данной задачи. В задаче чётко описано, кто общается с нейросетью, какую роль должна взять на себя нейросеть, а также перечислены целевые аудитории, для которых предназначен гид. Также было написано условия, которое требует от нейросети сформулировать результаты в виде таблицы с чётким планом таблицы (колонки - аудитории, строки -

кейсы).

Результатом выполнения вышеприведённого промта стала следующая таблица:

Таблица 2.1 – Информация для разных целевых групп

	ШКОЛЬНИК 7-ГО КЛАССА	ПОЖИЛОЙ ЧЕЛОВЕК	НАУЧНЫЙ РАБОТНИК
1 Кейс	<p>Алгоритм «Друг или самозванец?»:</p> <ol style="list-style-type: none"> Стоп! Получил ссылку «посмотри, это прикол» от друга? Не торопись кликать. Проверь язык. Тебе пишут «Привет, как дела?» а через минуту «Вот ссылка на халявные голды»? Так не бывает, это бот. Спроси голосом. Набери друга или напиши ему в другом чате: «Ты мне ссылку кидал?». 99%, что он скажет «Нет». Удали подозрительное сообщение и пожалуйся на спам. 	<p>Алгоритм «Проверь знакомого»:</p> <ol style="list-style-type: none"> Не спеши. Внук в сообщении просит срочно перевести деньги за неотложную операцию? Позвони по известному тебе номеру. Набери его личный номер, который у тебя давно записан, и спроси, всё ли в порядке. Задай контрольный вопрос, который знаете только вы двое (например, кличка домашнего питомца). Не переводи деньги и не переходи по ссылкам, пока лично не убедишься. 	<p>Алгоритм «Целевая атака на сотрудника»:</p> <ol style="list-style-type: none"> Верифицируй источник. Получил письмо от «коллеги» с просьбой скачать «проект документа» по ссылке? Проверь email-адрес отправителя до символа. Часто меняют 1 букву (например, @rnc.com вместо @mc.com). Используй альтернативный канал связи. Позвони коллеге по телефону или напишите в корпоративном мессенджере, чтобы подтвердить отправку. Проанализируйте URL. Наведи курсор на ссылку (не кликая!) и посмотри адрес в строке статуса браузера. http://secure-bank.ru.com — это не сайт bank.ru. Домен-обманка стоит перед основным. Используйте корпоративный антифишинг. Все подозрительные письма - report в ИТ-отдел.
2 Кейс	Алгоритм «Банк тебе не пишет просто так»:	Алгоритм «Банк звонит? Перезвони сам!»:	Алгоритм «Компрометация рабочих учетных данных»:

	ШКОЛЬНИК 7-ГО КЛАССА	ПОЖИЛОЙ ЧЕЛОВЕК	НАУЧНЫЙ РАБОТНИК
	<p>1. Запомни: настоящий банк никогда не будет в СМС просить перейти по ссылке и ввести номер карты, CVV-код или пароль. Никогда!</p> <p>2. Не верь срочности. «Счет заблокируют через 5 минут!» — это ложь, чтобы ты запаниковал.</p> <p>3. Проверь официально. Если волнуешься, не кликай по ссылке! Возьми родительскую карту, найди номер службы поддержки на её обороте и позвони сам.</p>	<p>1. Ничего не говори. Если тебе звонят, представляются банком и просят назвать код из СМС, ПИН или CVV — это 100% мошенники. Просто положи трубку.</p> <p>2. Не набирай кодоры. Если просят набрать цифры в телефоне («для проверки линии»), не делай этого.</p> <p>3. Используй официальный номер. Возьми свою банковскую карту, найди на обороте телефон горячей линии и перезвони туда сам. Спроси, звонили ли они тебе. Тебе скажут правду.</p>	<p>1. Принцип нулевого доверия. Письмо/СМС от «службы ИТ-поддержки» с требованием срочно сменить пароль, переходя по ссылке? Не делайте этого. Это классический фишинг для кражи корпоративных доступов.</p> <p>2. Сверяйтесь с регламентом. Узнайте, как официально происходит смена паролей в вашей организации. Обычно — через внутренний портал, а не по ссылкам из почты.</p> <p>3. Проверьте сертификат сайта. Если всё же перешли (на свой страх и риск), перед вводом данных убедитесь, что соединение защищено (https:// и замок в адресной строке), а сертификат выдан вашей организацией.</p>
3 Кейс	<p>Алгоритм «Письмо с подвохом»:</p> <p>1. Посмотри на адрес отправителя. Пришло письмо от «YouTube Support», а адрес pomoshch-youtube@gmail.com? Это фейк! Официальные письма приходят с домена компании (например, @youtube.com).</p> <p>2. Не качай вложения. «Вам штраф», «Ваш аккаунт взломали, скачайте файл для проверки» — это вирус.</p>	<p>Алгоритм «Письмо от государства»:</p> <p>1. Не верь угрозам. Письма от «налоговой», «полиции» или «суда» с угрозами ареста или штрафа, если вы не перейдете по ссылке и не оплатите — это обман.</p> <p>2. Не открывай вложения. В них могут быть вирусы.</p> <p>3. Проверь через госуслуги. Если беспокоишься, зайди</p>	<p>Алгоритм «Фишинг под видом научного сервиса»:</p> <p>1. Внимание к деталям. Письмо от «Elsevier», «Springer» или «Google Scholar» о проблеме с аккаунтом? Проверьте домен отправителя. Официальный домен Elsevier — @elsevier.com, а не @elsevier-security.com.</p> <p>2. Не передавайте данные для доступа к институтским подпискам. Их кража — прямая угроза репутации и</p>

ШКОЛЬНИК 7-ГО КЛАССА	ПОЖИЛОЙ ЧЕЛОВЕК	НАУЧНЫЙ РАБОТНИК
3. Зайди в аккаунт напрямую. Не через ссылку в письме, а через приложение или официальный сайт. Если там всё в порядке — письмо было фейком.	на официальный сайт или в приложение «Госуслуги» (не по ссылке из письма!) и проверяй уведомления там. Или сходи лично в ближайшее отделение.	безопасности организации. 3. Используйте двухфакторную аутентификацию (2FA) везде, где это возможно. Даже если мошенник украдет ваш логин и пароль, без кода с телефона они будут бесполезны.

Выводы по работе

В ходе работы были рассмотрены варианты написания гида с использованием нейросетей и собственно найденных источников информации. Также были изучены основные технологии написания промптов. По итогу выполнения работы была составлена таблица-гид с 3 практическими кейсами, в которых представлены алгоритмы для трёх целевых аудиторий (школьники, пожилые люди и научные сотрудники). В ходе работы были получены практические навыки работы с нейросетями, а именно: написание промптов с помощью нескольких технологий, а также дальнейшая обработка ответов нейросети и их анализ на наличие ошибок.

Раздел 3. Подготовка брендбука для гида кейсов по медиабезопасности

Шаг 4: Разработка концепции

На основании выбранной темы разработайте визуальную концепцию для брендбука гида, которая будет объединять все создаваемые элементы:

Цветовая палитра:

- Основной: Тёмно-синий #2E5BFF (доверие, серьёзность)
- Акцент опасности: Красный #FF4757 (предупреждение, угроза)
- Поддерживающий: Голубой #26E8C8 (технологичность)
- Фон: Светло-серый #F5F7FA (нейтральность)

Стиль иллюстраций:

- Выбираем плоский дизайн с изометрическими элементами - современно, понятно, технологично.

Общее настроение:

- Выбираем серьёзное, но доступное настроение - предупреждаем об опасности, но не пугаем.

Шаг 5: Создание метафорических иллюстраций

1. Рыболовный крючок в форме конверта с приманкой

Для получения иллюстрации был написан следующий промт для нейросети Шедеврум (YandexART):

Рыболовный крючок в форме почтового конверта, плоский дизайн иллюстрация, центрированная композиция, мягкий градиентный фон, синяя и красная цветовая схема, минималистичный стиль, чистые линии, векторная графика, без текста, профессиональный вид, современный

Выбран вариант с крючком, выполненным в форме конверта на синем градиентном фоне (Рис. 2.1). Метафора считывается мгновенно: письмо = приманка на крючке. Цветовая схема (синий + красный) соответствует выбранной палитре, стиль - плоский дизайн без текста. Изображение работает автономно, не требует подписей.



Рисунок 3.1- Рыболовный крючок в форме конверта с приманкой (Шедеврум, YandexART 2.7)

2. Письмо с маской, скрывающее истинное лицо отправителя

Для получения иллюстрации был написан следующий промт для нейросети Шедеврум (YandexART) и Kandinsky:

Письмо с маской, подразумевающее что оно было отправлено анонимным злоумышленником, плоский дизайн иллюстрация, центрированная композиция, мягкий градиентный фон, синяя и красная цветовая схема, минималистичный стиль, чистые линии, векторная графика, без текста, профессиональный вид, современный

Выбраны варианты с маской, подразумевающее что оно было отправлено анонимным злоумышленником, на синем градиентном фоне (Рис. 2.2 и Рис. 2.3). Метафора считывается мгновенно: маска = злоумышленник, который хочет остаться анонимным. Цветовая схема (синий + красный) соответствует выбранной палитре, стиль - плоский дизайн без текста. Изображение работает автономно, не требует подписей.



Рисунок 3.2 - Письмо с маской, скрывающее истинное лицо отправителя (Kandinsky, Kandinsky 3.0)



Рисунок 3.3 - Письмо с маской, скрывающее истинное лицо отправителя (Шедеврум, YandexART 2.7)

3. Защитный щит, отражающий поток писем со знаками опасности

Для получения иллюстрации был написан следующий промт для нейросети Kandinsky (Kandinsky 3.0):

Защитный щит, отражающий поток писем со знаками опасности, плоский дизайн иллюстрация, центрированная композиция, мягкий градиентный фон, синяя и красная цветовая схема, минималистичный стиль, чистые линии, векторная графика, без текста, профессиональный вид, современный

Выбран вариант с щитом, отражающим поток писем с предупреждающими знаками (Рис. 2.4), подразумевающее что в каждом из этих писем находится фейковое содержание. Цветовая схема (синий + красный) соответствует выбранной палитре, стиль - плоский дизайн без текста. Изображение работает автономно, не требует подписей.

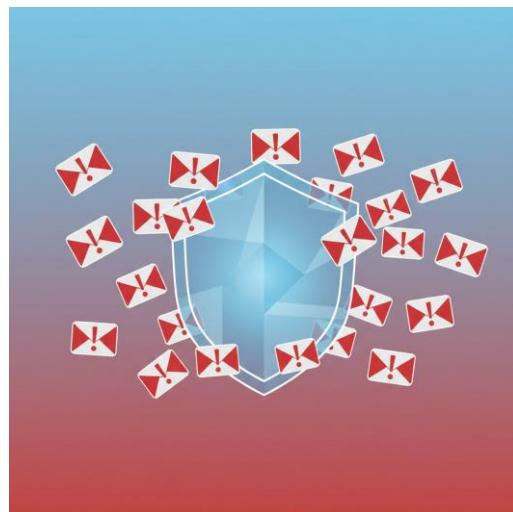


Рисунок 3.4- Защитный щит, отражающий поток писем со знаками опасности (Kandinsky, Kandinsky 3.0)

4. Увеличительное стекло над письмом, выявляющее поддельные элементы

Для получения третьей иллюстрации был написан следующий промт для нейросети Шедеврум (YandexART) и Kandinsky:

Увеличительное стекло над письмом, выявляющее в данном письме поддельные элементы, плоский дизайн иллюстрация, центрированная композиция, мягкий градиентный фон, синяя и красная цветовая схема, минималистичный стиль, чистые линии, векторная графика, без текста, профессиональный вид, современный

Выбран вариант с увеличительным стеклом над письмом, выявляющее в данном письме поддельные элементы (Рис. 2.5), подразумевающее что в каждом из этих писем находится незначительная опечатка, показывающая что данное письмо - фишинг. Цветовая схема (синий + красный) соответствует выбранной палитре, стиль - плоский дизайн без текста. Изображение работает автономно, не требует подписей.



Рисунок 3.5 - Увеличительное стекло над письмом, выявляющее поддельные элементы
(Шедеврум, YandexART 2.7)

Шаг 6: Создание обложки гида

Для генерации первой обложки, был создан следующий промт для нейросетей YandexART и Kandinsky:

Обложка гида по кибербезопасности, защитный щит отражает поток писем-стрел с крючками, центральная композиция, изометрическая перспектива, современный плоский дизайн, градиент от тёмно-синего к голубому фону, красные акценты на опасных элементах, чистое пространство для текста в верхней трети, профессиональный вид, без текста, векторный стиль

Данная обложка (Рис. 3.1) отражает смысл защиты от фишинга тем, что имеет символ щита, который ассоциируется с защитой, а также имеет явные красные направления, которые обозначают некий поток вредной информации.



Рисунок 3.6 – Первая обложка для гида (Шедеврум, YandexART 2.7)

Вторая обложка была сгенерирована с помощью YandexART по следующему промту:

Обложка гида по кибербезопасности, асимметричная композиция. Увеличительное стекло с неоновым голубым свечением анализирует поток абстрактных писем, одно из которых ярко-красное и помечено символом опасности. Композиция по правилу третей, лупа смешена вправо. Контрастная цветовая схема на тёмно-сером фоне. Много чистого пространства для текста слева. Современный плоский дизайн с элементами свечения, технологичная атмосфера, без текста, векторный стиль, высокое качество.

Данная обложка (Рис. 3.2) отображает тёмный цифровой мир под увеличительным стеклом, тем самым разгадывая ловушки фишинга. Тем самым гид по медиабезопасности раскрывает секреты борьбы с фишингом



Рисунок 3.7 – Вторая обложка для гида (Шедеврум, YandexART 2.7)

Для генерации третьей обложки был разработан следующий промт для нейросети Шедеврум (YandexART 2.7):

Обложка для технологического гида в стиле минималистичный 3D рендер. Сверху вниз движется хаотичный поток иконок-писем. Поток состоит из опасных красных иконок с символом черепа и безопасных синих иконок с символом галочки. По центру композиции расположен горизонтальный, полупрозрачный, светящийся синий силовой барьер (цифровая сетка-фильтр). Красные иконки-письма не могут пройти через барьер, они отскакивают от него или распадаются на пиксели. Синие иконки-письма проходят сквозь барьер и формируют упорядоченный поток в нижней части изображения. Чистый светло-серый фон, студийное освещение. Просторная чистая зона для текста в верхней трети. Без текста, высокое разрешение, профессиональный вид.

На третьей обложке (Рис. 3.3) — символическое изображение киберугроз: красные кубики с предупреждающими знаками заполняют цифровое пространство. Этот образ подчёркивает необходимость освоения правил медиабезопасности для защиты в интернете.

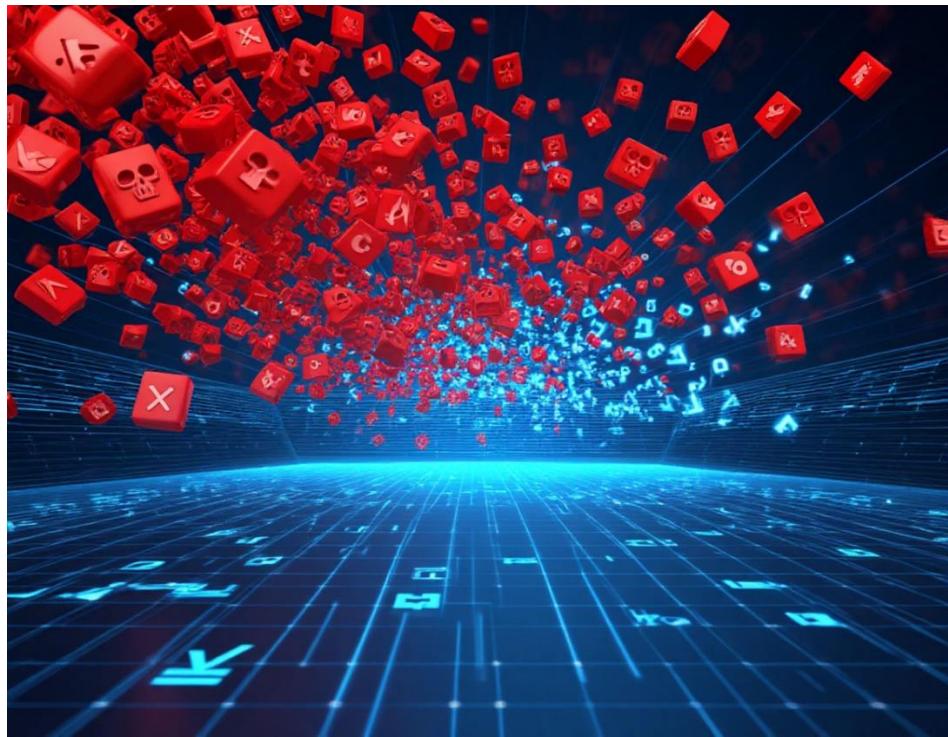


Рисунок 3.8 – Третья обложка для гида (Шедеврум, YandexART 2.7)

Выбран первый вариант с центральной композицией и щитом. Центральное расположение создаёт ощущение стабильности и надёжности, что важно для темы безопасности. Щит как универсальный символ защиты мгновенно считывается аудиторией. Цветовая схема (тёмно-синий + красные акценты) соответствует выбранной палитре и передаёт серьёзность угрозы при этом не пугая. Изометрическая перспектива добавляет современности и технологичности.

Шаг 7: Тематические иконки

- Иконка «предупреждение»

Исходный промт:

Иконка "Предупреждение". Ярко-красный равносторонний треугольник, внутри которого расположен белый восклицательный знак. Стиль иконки: минималистичный плоский дизайн, простые геометрические формы, толстые чистые линии. Иконка изолирована на чистом белом фоне. Профессиональная векторная графика, без текста, высокое качество.

Иконка «предупреждения» (Рис. 4.1) с красным треугольником и белым восклицательным знаком оптимальна для гида по медиабезопасности: красный цвет сигнализирует об опасности, треугольник традиционно обозначает предупреждение, восклицательный знак акцентирует внимание на необходимости быть бдительным. Компактный и универсальный дизайн соответствует концепции.



Рисунок 3.9 – Иконка «предупреждение» (Kandinsky, Kandinsky 3.0)

- Иконка «рекомендация»

Исходный промт:

Иконка "Рекомендация". Нейтрально-синий квадрат, внутри которого расположен палец вверх. Стиль иконки: минималистичный плоский дизайн, простые геометрические формы, толстые чистые линии. Иконка изолирована на чистом белом фоне. Профессиональная векторная графика, без текста, высокое качество.

Иконка с изображением «палец вверх» (Рис. 4.2) (символ лайка) оптимальна для использования в гиде по медиабезопасности. Символ мгновенно ассоциируется с одобрением, поддержкой и положительной

реакцией, эффективно выполняя функцию быстрой коммуникации — выражения симпатии к контенту. Компактный и интуитивно понятный дизайн соответствует задачам вовлечения пользователей.



Рисунок 3.10 - Иконка «рекомендация» (Шедеврум, YandexART 2.7)

- Иконка «запрет»

Исходный промт:

Иконка "Запрет". Ярко-красный круг, перечёркнутый справа налево. Стиль иконки: минималистичный плоский дизайн, простые геометрические формы, толстые чистые линии. Иконка изолирована на чистом белом фоне. Профессиональная векторная графика, без текста, высокое качество.

Иконка «Предупреждение» (Рис. 4.3) (красный треугольник с белым восклицательным знаком) выбрана за счёт чёткой визуальной семантики: красный цвет сигнализирует об опасности, треугольник традиционно ассоциируется с предупреждением, а восклицательный знак акцентирует внимание. Компактный дизайн мгновенно распознаётся и соответствует концепции оповещения о рисках или ошибках.



Рисунок 3.11 – Иконка «запрет» (Шедеврум, YandexART 2.7)

- Иконка «информация»

Исходный промт:

Иконка "Информация". Нейтрально-синий квадрат, внутри которого расположен "i". Стиль иконки: минималистичный плоский дизайн, простые геометрические формы, толстые чистые линии. Иконка изолирована на чистом белом фоне. Профессиональная векторная графика, без текста, высокое качество.

Иконка с буквой i (знак информации) (Рис. 4.4) в синей квадратной рамке лаконична и универсальна — мгновенно привлекает внимание, сигнализируя о необходимости ознакомиться с информацией. Синий цвет ассоциируется с доверием и спокойствием, смягчая акцент на предупреждении. Такой дизайн хорошо вписывается в концепции интерфейсов, где требуется выделить важные уведомления без излишней тревожности.



Рисунок 3.12 – Иконка «информация» (Kandinsky, Kandinsky 3.0)

- Иконка «проверка»

Исходный промт:

Иконка "Проверка". Ярко-жёлтый круг, внутри которого расположена лупа . Стиль иконки: минималистичный плоский дизайн, простые геометрические формы,

толстые чистые линии. Иконка изолирована на чистом белом фоне. Профессиональная векторная графика, без текста, высокое качество.

Иконка с изображением лупы на жёлтом фоне (Рис. 4.5) лаконично передаёт смысл «проверки» или «анализа» — лупа традиционно ассоциируется с детальным рассмотрением. Яркий жёлтый цвет привлекает внимание, подчёркивая важность действия. Такой дизайн органично вписывается в концепцию интерфейсов, где требуется обозначить функцию проверки данных или поиска несоответствий.



Рисунок 3.13 – Иконка «проверка» (Kandinsky, Kandinsky 3.0)

– Иконка «совет»

Исходный промт:

Иконка "Совет". Ярко-жёлтый круг, внутри которого расположена лампочка. Стиль иконки: минималистичный плоский дизайн, простые геометрические формы, толстые чистые линии. Иконка изолирована на чистом белом фоне. Профессиональная векторная графика, без текста, высокое качество.

Иконка с изображением (Рис. 4.6) лампочки на жёлтом фоне оптимальна для обозначения «совета» — лампочка традиционно ассоциируется с идеями, озарениями и полезными подсказками. Яркий жёлтый цвет усиливает ассоциацию с энергией и вниманием, делая иконку заметной. Такой дизайн органично соответствует концепции передачи рекомендаций или ценных советов в интерфейсах.



Рисунок 3.14 – Иконка «совет» (Шедеврум, YandexART 2.7)

– Иконка «чек-лист»

Исходный промт:

Иконка "чек-лист". Светло-серый квадрат, внутри которого расположен квадрат, внутри которого галочка. Стиль иконки: минималистичный плоский дизайн, простые геометрические формы, толстые чистые линии. Иконка изолирована на чистом белом фоне. Профессиональная векторная графика, без текста, высокое качество.

Иконка с галочкой (check mark) в квадрате (Рис. 4.7) — оптимальный выбор для «чек-листа», так как галочка является универсальным символом завершённости, подтверждения или выполнения задачи. Квадратная рамка усиливает ассоциацию с чекбоксом — стандартным элементом интерфейсов для отметки пунктов списка. Такой дизайн чётко соответствует концепции чек-листа: визуализация процесса отслеживания выполненных действий.



Рисунок 3.15 – Иконка «чек-лист» (Шедеврум, YandexART 2.7)

- Иконка «вопрос»

Исходный промт:

Иконка "вопрос". Синий круг, внутри которого расположен знак вопроса. Стиль иконки: минималистичный плоский дизайн, простые геометрические формы, толстые чистые линии. Иконка изолирована на чистом белом фоне. Профессиональная векторная графика, без текста, высокое качество.

Иконка с белым вопросительным знаком на синем круге (Рис. 4.8) — оптимальный выбор для обозначения «вопроса», так как вопросительный знак универсально ассоциируется с запросом информации, неопределённостью или необходимостью уточнения. Синий цвет фона вызывает доверие и спокойствие, не перегружая восприятие. Такой дизайн чётко соответствует концепции раздела/функции, связанной с поддержкой, справкой или поиском ответов.



Рисунок 3.16 – Иконка «вопрос» (Kandinsky, Kandinsky 3.0)

Шаг 8: Анализ результатов и доработка

Для анализа были выбраны 3 наиболее лучших картинки из каждого шага, а именно:

1. *Письмо с маской, скрывающей истинное лицо отправителя (Рис. 2.3)*
2. *Обложка гида с центральной композицией и щитом (Рис. 3.1)*
3. *Иконка «рекомендация» (Рис. 4.4)*

Оцениваться каждая картинка будет по сумме баллов, где: 25-21 – отлично, 20-16 – хорошо, 15-11 – удовлетворительно (переработка), 10 и ниже – неудовлетворительно (переработка).

Таблица 3.1 - оценивание первой из списка картинки:

Критерий	Оценка	Комментарий
Соответствие теме	5	Картинка безусловно полностью отражает тему фишинга. На ней чётко изображены символы фишинга и злоумышленника.
Визуальная согласованность	5	Нейросеть довольно неплохо справилась с выполнением задачи. Полностью поняла тему и необходимые знаки отличия для изображения злоумышленника, занимающегося фишингом.
Техническое качество	4	Нейросеть полностью выполнила все требования промта. От градиентного фона до символов мошенничества и фишинга.
Композиция	4	Цвета нейросеть подобрала очень хорошо, но часть картинки слегка сливаются с фоном.
Эмоциональное воздействие	5	Данная картинка вызывает нужные эмоции: предупреждает, но не пугает.
Итог	23	Нейросеть очень хорошо справилась со своей работой, полностью закрыв требования промта.

Таблица 3.2 - оценивание второй из списка картинки:

Критерий	Оценка	Комментарий
Соответствие теме	3	Тема фишинга затронута очень поверхностно, но в целом есть отображения кибербезопасности в виде щита.
Визуальная согласованность	4	Нейросеть реализовала задумку со щитом, но сгенерировала чёткие ссылки к фишингу.
Техническое качество	3	Нейросеть выполнила только часть промта. Выполнила только половину задумки, заложенной в промт.
Композиция	5	Цвета нейросеть подобрала очень хорошо, но часть картинки слегка сливаются с фоном.
Эмоциональное воздействие	4	Данная картинка вызывает нужные эмоции: предупреждает, но не пугает.
Итог	19	Нейросеть хорошо справилась со своей работой, но не закрыла полностью требования из промта.

Таблица 3.3 - оценивание третей из списка картинки:

Критерий	Оценка	Комментарий
Соответствие теме	5	Иконка полностью соответствует теме значка, обозначающего информацию.
Визуальная согласованность	4	Визуально иконка согласована с промтом, но буква «i» вышла заглавной. Цвет подобран отлично – нейтральный синий не вызывает чувство опасности.
Техническое качество	4	Нейросеть частично выполнила требования промта.
Композиция	5	Цвет подобран отлично – нейтральный синий
Эмоциональное воздействие	5	Данная картинка вызывает нужные эмоции: предупреждает, что тут находится важная информация.
Итог	23	Нейросеть идеально выполнила требования промта

Выводы по работе

В ходе проделанной работы была успешно достигнута поставленная цель – освоение техник промт-инжиниринга для создания визуального контента гида по цифровой безопасности с использованием генеративных нейросетей. Практическое решение комплекса задач позволило перейти от теоретического понимания принципов работы с ИИ к их осознанному применению для получения конкретных, стилистически согласованных результатов.

Ключевым стало формирование навыка составления эффективных промтов, которые представляют из себя от простых описаний к сложным, многослойным конструкциям. Была отработана формула, включающая контекст («цифровая безопасность»), объект («щит», «замок»), метафору («лабиринт для пароля»), четкое определение стиля («плоский векторный дизайн», «минимализм») и технические параметры. Такой подход позволил целенаправленно генерировать контент, соответствующий изначальному замыслу, и минимизировать количество случайных результатов.

В рамках решения задач последовательно была разработана визуальная концепция, определены цветовая палитра и стилистика, что стало основой для обеспечения согласованности всех элементов. Создание серии метафорических иллюстраций, обложки, набора иконок и инфографик подтвердило универсальность освоенных техник. Особое внимание уделялось условию отсутствия текста на изображениях, что потребовало развивать навык визуализации абстрактных понятий. Анализ и последующая итеративная доработка промтов на основе первичных результатов стали неотъемлемой частью процесса, позволившей значительно повысить качество и точность финального визуального контента.

Раздел 4. Разработка UML-диаграмм для гида кейсов по медиабезопасности

Шаг 1: Подготовка и описание системы для диаграммы UseCase

Система для диаграммы UseCase по угрозе «Фишинг» будет иметь следующий вид:

- Акторы (Действующие лица):
 - «Сотрудник»
 - «Администратор»
 - «Система анализа»
- Основные сущности (Объекты):
 - 2.1 Электронное письмо имеет атрибуты (отправитель, тема, статус)
 - 2.2 Отчет об инциденте имеет атрибуты (ID, уровень угрозы, описание)
 - 2.3 Правило фильтрации имеет атрибуты (условие, действие)
- Базовые процессы и сценарии:
 - Сотрудник может «Получать письма» и «Сообщать о фишинге»
 - Администратор «Управляет правилами», «Просматривает отчеты»
 - Система «Анализирует письма» (процесс включает проверку ссылок и текста, вынесение вердикта) и «Формирует отчеты»
- Жизненный цикл: «Отчет об инциденте» проходит состояния: «Новый» → «В обработке» → «Закрыт».

Эта простая система создает замкнутый цикл безопасности: сотрудник обнаруживает угрозу, система ее автоматически анализирует и классифицирует, а администратор принимает финальное решение, постоянно улучшая правила на основе поступающих отчетов.

Шаг 2: Генерация диаграммы прецедентов (Use Case)

Опираясь на систему для диаграммы UseCase в предыдущем шаге, был составлен промт для генерирования диаграммы прецедентов для нейросети DeepSeek:

Напиши качественный промт для нейросети, основываясь на этой информации:
 Ты квалифицированный специалист и профессионал в сфере UML-диаграмм, PlantUML.
 По теме «Системы обнаружения фишинга» напиши кратко информацию для диаграммы прецедентов Use-Case и напиши код на PlantUML для неё.

Контекст системы:

Акторы: «Сотрудник», «Администратор», «Система анализа».

Сущности: «Электронное письмо» (атрибуты: отправитель, тема, статус), «Отчет об инциденте» (ID, уровень угрозы), «Правило фильтрации».

Процессы и сценарии: Сотрудник «Получает письма» и «Сообщает о фишинге». Администратор «Управляет правилами», «Просматривает отчеты». Система «Анализирует письма», «Формирует отчеты».

Жизненный цикл: «Отчет об инциденте» проходит состояния: «Новый» → «В обработке» → «Закрыт».

Полученный промт был загружен в нейросеть DeepSeek. DeepSeek сгенерировал следующий код для PlantUML описание диаграммы:

```
@startuml
left to right direction

actor "Сотрудник" as Employee
actor "Администратор" as Admin
actor "Система анализа" as System

rectangle "Модуль обнаружения фишинга" {
    usecase "Получает письма" as ReceiveEmails
    usecase "Сообщить о фишинге" as ReportPhishing
    usecase "Управлять правилами фильтрации" as ManageRules
}
```

```

usecase "Просматривать отчеты об инцидентах" as ViewReports

usecase "Анализировать письма" as AnalyzeEmails

usecase "Формировать отчет об инциденте" as GenerateReport

}

Employee --> ReceiveEmails

Employee --> ReportPhishing

Admin --> ManageRules

Admin --> ViewReports

System --> AnalyzeEmails

System --> GenerateReport

' Автоматический анализ при получении письма
ReceiveEmails ..> AnalyzeEmails : include

' Формирование отчета при ручном отчете и автоматическом анализе
ReportPhishing ..> GenerateReport : include
AnalyzeEmails ..> GenerateReport : include

@enduml

```

Текстовое описание диаграммы, полученное вместе с кодом PlantUML от нейросети DeepSeek:

Данная диаграмма прецедентов описывает модуль "Системы обнаружения фишинга" для корпоративной почты. Система обеспечивает автоматический анализ входящих писем, обработку ручных жалоб от сотрудников и управление правилами фильтрации администратором. Ключевые акторы включают Сотрудника (получение писем и отчет о фишинге), Администратора (управление правилами и просмотр отчетов) и

Систему анализа (автоматический анализ и формирование отчетов). Прецеденты связаны через отношения включения: анализ писем выполняется автоматически при получении, а отчет об инциденте формируется как при автоматическом обнаружении, так и при ручном сообщении о фишинге.

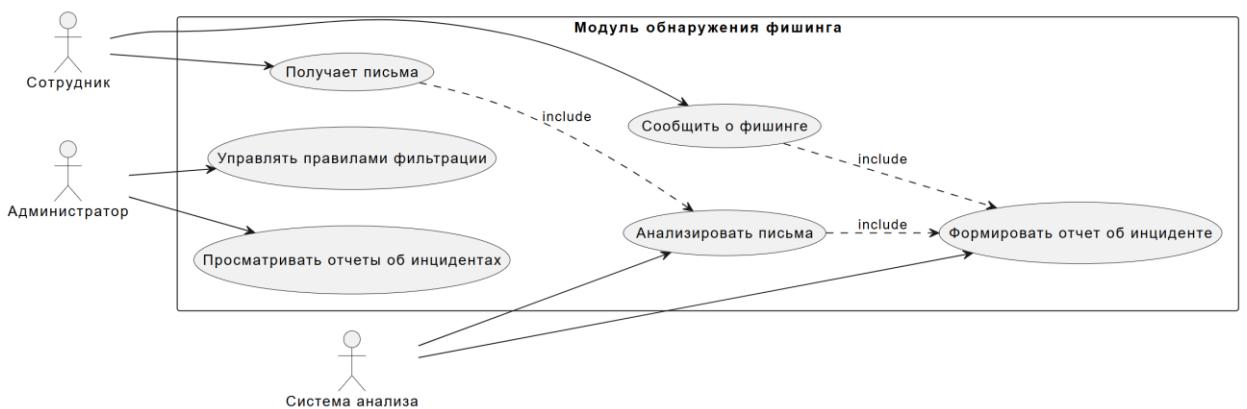


Рисунок 4.1– Диаграмма UseCase для угрозы «Фишинг-письма»

В результате реализации вышеприведённого кода PlantUML была получена следующая диаграмма, представленная на Рисунке 2.1

Шаг 3: Диаграмма классов (Class)

Опираясь на систему для диаграммы UseCase в предыдущем шаге, был составлен промт для генерирования диаграммы прецедентов для нейросети DeepSeek:

Напиши качественный промт для нейросети, основываясь на этой информации:
Ты квалифицированный специалист по кибербезопасности и профессионал в сфере UML-диаграмм, PlantUML. По теме «Системы обнаружения фишинга» напиши кратко информацию для диаграммы классов (Class Diagram) и напиши код на PlantUML для неё.

Контекст системы:

Акторы: «Сотрудник», «Администратор», «Система анализа».

Сущности: «Электронное письмо» (атрибуты: отправитель, тема, статус), «Отчет об инциденте» (ID, уровень угрозы), «Правило фильтрации».

Процессы и сценарии: Сотрудник «Получает письма» и «Сообщает о фишинге».

Администратор «Управляет правилами», «Просматривает отчеты». Система

«Анализирует письма», «Формирует отчеты».

Жизненный цикл: «Отчет об инциденте» проходит состояния: «Новый» -> «В обработке» -> «Закрыт».

Полученный промт был загружен в нейросеть DeepSeek. DeepSeek сгенерировал следующий код для PlantUMLи описание диаграммы:

```
@startuml

' Определение основных классов системы

class Пользователь {
    # id: Long
    # имя: String
    # email: String
    # датаРегистрации: Date
    + аутентифицировать()
    + получитьПрофиль()
}

class Сотрудник {
    - отдел: String
    - должность: String
    + получатьПисьма()
    + сообщитьОФишинге()
}

class АдминистраторБезопасности {
    - уровеньДоступа: Integer
    + управлятьПравиламиФильтрации()
    + просматриватьОтчеты()
}

class Письмо {
    - id: Long
}
```

```

- отправитель: String
- тема: String
- содержание: String
- датаПолучения: Date
- хэш: String
- меткаФишинг: Boolean

+ проверятьФишинг()
+ помечатьКакФишинг()

}

```

```

class ОтчетОбИнциденте {

- id: Long
- датаСоздания: Date
- статус: String {Новый, В обработке, Закрыт}
- типОбнаружения: String {Авто, Ручной}
- описание: String

+ создаватьОтчет()
+ обновлятьСтатус()
+ вычислятьСтатистику()

}

```

```

class ПравилоФильтрации {

- id: Long
- название: String
- условие: String
- действие: String
- приоритет: Integer
- активен: Boolean

+ активировать()
+ деактивировать()
+ проверятьПравило()

}

```

```
}
```

```
class СистемаАнализа {
    - id: Long
    - версия: String
    - настройки: String
    + анализироватьПисьма()
    + формироватьОтчет()
    + обучатьМодель()
}
```

' Определение отношений наследования

Пользователь <|-- Сотрудник

Пользователь <|-- АдминистраторБезопасности

' Определение основных ассоциаций

Сотрудник "1" -- "*" Письмо : получает

Сотрудник "1" -- "*" ОтчетОбИнциденте : создает

АдминистраторБезопасности "1" -- "*" ПравилоФильтрации : управляет

АдминистраторБезопасности "1" -- "*" ОтчетОбИнциденте : просматривает

Письмо "1" -- "0..1" ОтчетОбИнциденте : анализируется в

СистемаАнализа "1" -- "*" Письмо : анализирует

СистемаАнализа "1" -- "*" ОтчетОбИнциденте : формирует

ПравилоФильтрации "1" -- "*" Письмо : фильтрует

' Композиция - Правила являются частью Системы анализа

СистемаАнализа *-- "1..*" ПравилоФильтрации : содержит

' Агрегация - Отчеты могут существовать независимо от администраторов

```
АдминистраторБезопасности о-- "0..*" ОтчетОбИнциденте
```

```
@enduml
```

Текстовое описание диаграммы, полученное вместе с кодом PlantUML от нейросети DeepSeek:

Диаграмма классов модуля "Системы обнаружения фишинга" представляет ключевые сущности и их взаимосвязи. Основные классы включают Пользователь (абстрактный класс с наследниками Сотрудник и Администратор), Письмо (содержит информацию о входящем сообщении), ОтчетОбИнциденте (отслеживает статус обработки фишинга), ПравилоФильтрации (определяет критерии анализа) и СистемаАнализа (обрабатывает письма). Отношения между классами отражают бизнес-логику: система анализирует письма, создает отчеты, а администраторы управляют правилами фильтрации.

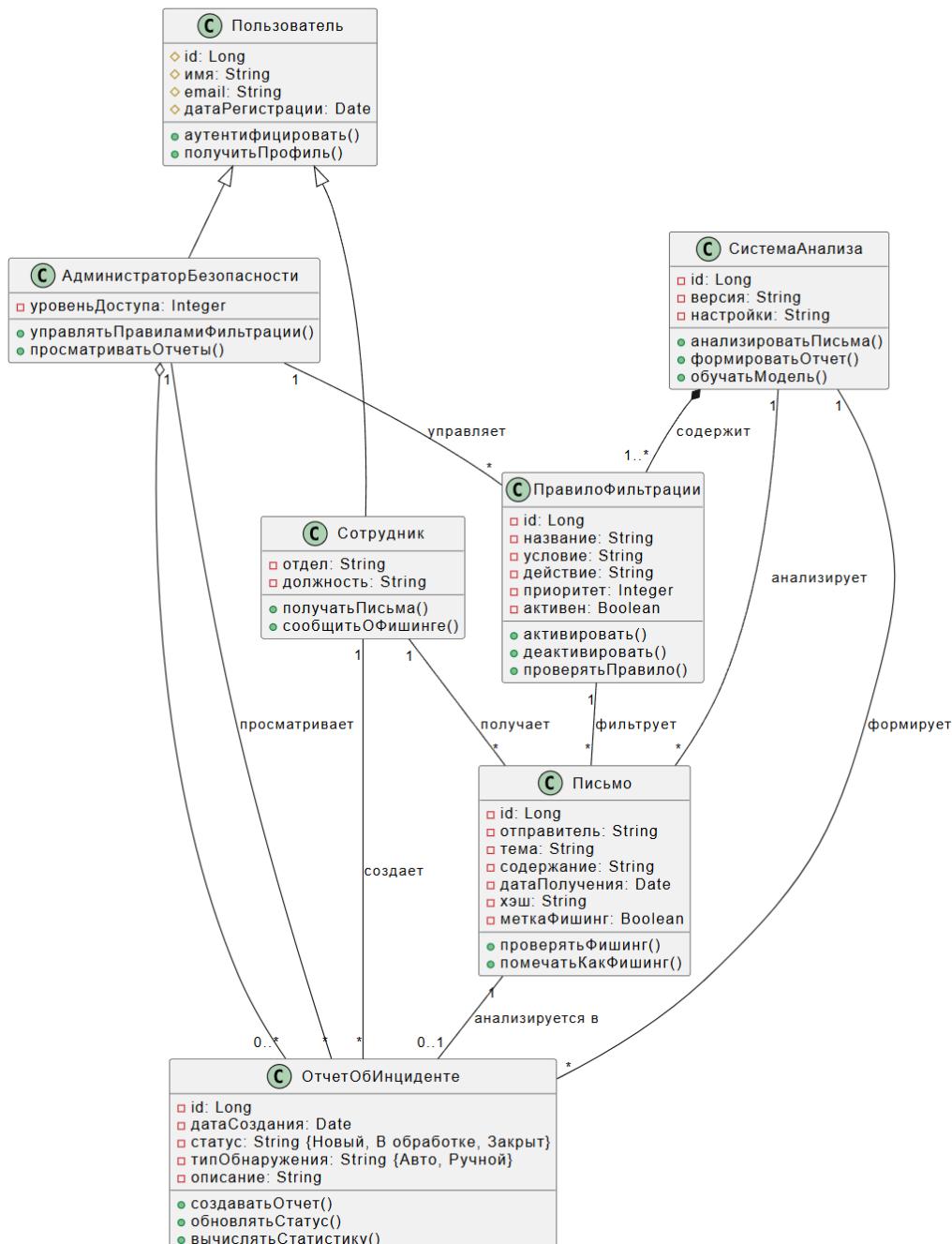


Рисунок 4.2 – Диаграмма Class для угрозы «Фишинг-письма»

В результате реализации вышеприведённого кода PlantUML была получена следующая диаграмма, представленная на Рисунке 3.1

Шаг 4: Диаграмма деятельности (Activity)

Для получения промта для генерации диаграммы деятельности был сформирован следующий промт для нейросети DeepSeek:

Напиши мне качественный промт для нейросети, основываясь на этой информации: "Ты квалифицированный системный аналитик. По теме "Системы обнаружения фишинга" напиши краткую информацию для диаграммы деятельности и напиши код на PlantUML для неё.

Контекст системы:

Акторы: "Сотрудник", "Администратор", "Система анализа".

Сущности: "Электронное письмо" (атрибуты: отправитель, тема, статус), "Отчет об инциденте" (ID, уровень угрозы), "Правило фильтрации".

Процессы и сценарии: Сотрудник "Получает письма" и "Сообщает о фишинге". Администратор "Управляет правилами", "Просматривает отчеты". Система "Анализирует письма", "Формирует отчеты".

Жизненный цикл: "Отчет об инциденте" проходит состояния: "Новый" -> "В обработке" -> "Закрыт".

Подробное описание процесса "Анализ входящего письма":

- 1) Процесс начинается.
- 2) Происходит действие "Получить письмо".
- 3) Далее "Извлечь ссылки и вложения".
- 4) Затем "Проверить по базе угроз".
- 5) После проверки идет условие: "Найдена угроза?".
- 6) Если да, то выполняется действие "Отправить в карантин"; Если нет, то выполняется "Доставить сотруднику".
- 7) Процесс завершается."

Полученный промт был загружен в нейросеть DeepSeek. DeepSeek сгенерировал следующий код для PlantUML и описание диаграммы:

```
@startuml
|Получение данных|
start
:Получить письмо;
:Извлечь ссылки и вложения;
```

```

|Анализ угроз|
:Проверить по базе угроз;

|Обработка результата|
if (Найдена угроза?) then (да)
    :Отправить в карантин;
else (нет)
    :Доставить сотруднику;
endif
stop
@enduml

```

Текстовое описание диаграммы, полученное вместе с кодом PlantUML от нейросети DeepSeek:

Процесс начинается с получения письма системой. Далее извлекаются все ссылки и вложения для анализа. На основном этапе проверки письмо сравнивается с базой известных угроз. В точке принятия решения система определяет, была ли обнаружена угроза. Если угроза найдена, письмо перемещается в карантин. Если угроз нет, письмо доставляется сотруднику. Процесс завершается после выполнения одного из этих действий.

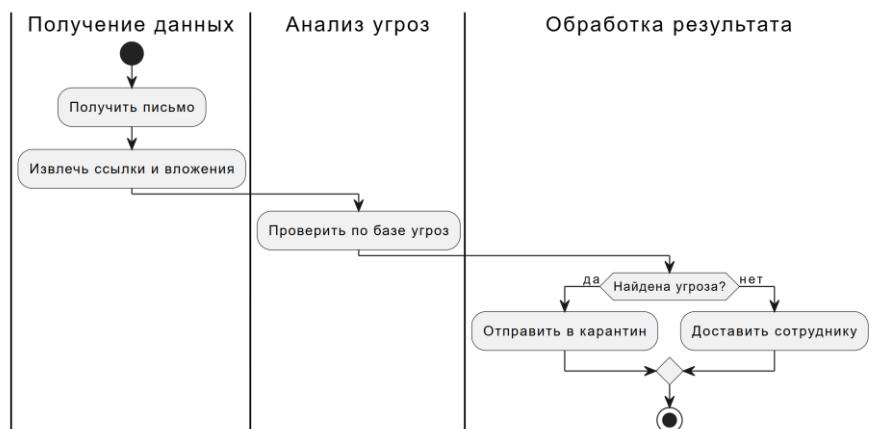


Рисунок 4.3 – Диаграмма Activity для угрозы «Фишинг-письма»

В результате реализации вышеприведённого кода PlantUML была получена следующая диаграмма, представленная на Рисунке 4.1

Шаг 5: Диаграмма последовательности (Sequence)

Для получения промта для генерации диаграммы последовательности был сформирован следующий промт для нейросети DeepSeek:

Напиши мне качественный промт для нейросети, основываясь на этой информации: "Ты квалифицированный специалист по компьютерной безопасности. По теме "Системы обнаружения фишинга" напиши краткую информацию для диаграммы последовательности и напиши код на PlantUML для неё.

Контекст системы:

Акторы: "Сотрудник", "Администратор", "Система анализа".

Сущности: "Электронное письмо" (атрибуты: отправитель, тема, статус), "Отчет об инциденте" (ID, уровень угрозы), "Правило фильтрации".

Процессы и сценарии: Сотрудник "Получает письма" и "Сообщает о фишинге". Администратор "Управляет правилами", "Просматривает отчеты". Система "Анализирует письма", "Формирует отчеты".

Жизненный цикл: "Отчет об инциденте" проходит состояния: "Новый" -> "В обработке" -> "Закрыт".

Полученный промт был загружен в нейросеть DeepSeek. DeepSeek сгенерировал следующий код для PlantUML и описание диаграммы:

```
@startuml
' Диаграмма последовательности обработки фишингового инцидента
title Сценарий "Обработка подозрительного письма и эскалация инцидента"

actor "Сотрудник" as Employee
actor "Администратор" as Admin
participant "Система анализа" as System

' Начало сценария: сотрудник получает письмо
Employee -> System: Сообщить о подозрительном письме\n(отправитель, тема)
note right of Employee: Письмо получено, статус: не проверен
```

```

' Система анализирует письмо

System -> System: Анализ письма по правилам фильтрации

note right of System: Проверка отправителя и темы\пна соответствие
фишинговым шаблонам


' Создание отчета об инциденте

System -> System: Создать отчет об инциденте\n(ID, уровень угрозы)

note right of System: Статус отчета: "Новый"


' Уведомление администратора

System -> Admin: Уведомить о новом инциденте


' Администратор обрабатывает инцидент

Admin -> System: Просмотреть отчет об инциденте

System --> Admin: Возврат деталей отчета и письма

Admin -> System: Изменить статус отчета на "В обработке"

note right of Admin: Статус отчета обновлен


' Дополнительные действия администратора

Admin -> System: Обновить правила фильтрации (при необходимости)

note right of Admin: Блокировка подобных угроз в будущем


' Завершение инцидента

Admin -> System: Закрыть инцидент\n(изменить статус на "Закрыт")

System --> Admin: Подтверждение закрытия

note right of System: Статус письма и отчета обновлен


@enduml

```

Текстовое описание диаграммы, полученное вместе с кодом PlantUML от нейросети DeepSeek:

Сотрудник получает подозрительное электронное письмо и инициирует процесс, сообщая о фишинге через систему анализа. Система анализа принимает отчет, изменяет статус письма на "Анализируется" и начинает автоматическую проверку содержимого по существующим правилам фильтрации. После анализа система создает новый отчет об инциденте с уровнем угрозы и устанавливает его статус "Новый". Администратор получает уведомление о новом инциденте и переводит отчет в статус "В обработке" для дальнейшего расследования. Администратор проверяет детали письма и отчета, при необходимости обновляет правила фильтрации для блокировки подобных угроз. По завершению обработки администратор закрывает инцидент, меняя статус отчета на "Закрыт". Система фиксирует изменения и обновляет статус связанного письма. Весь процесс отслеживается в системе, обеспечивая прозрачность и документирование действий.

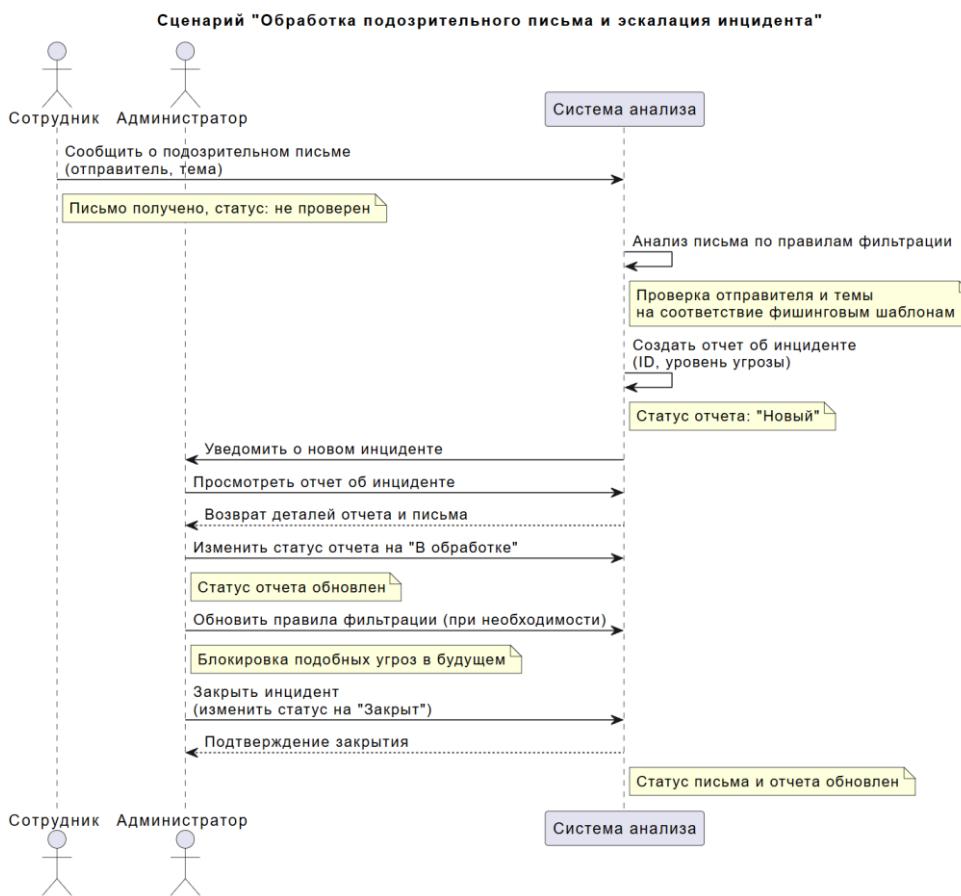


Рисунок 4.4 – Диаграмма Sequence для угрозы «Фишинг-письма»

В результате реализации вышеприведённого кода PlantUML была получена следующая диаграмма, представленная на Рисунке 4.1

Выводы по работе

В ходе работы был разработан комплекс промптов для генеративных ИИ, позволяющих на основе текстового описания системы получать код на языке PlantUML для четырёх типов UML-диаграмм. Последовательное создание промптов для диаграмм прецедентов, последовательности, классов и деятельности подтвердило возможность эффективного применения техник промт-инжиниринга для автоматизации процесса моделирования. Это позволило достичь цели работы — продемонстрировать возможность создания UML-диаграмм без необходимости глубоких предварительных знаний в области моделирования систем.

Таким образом, применение структурированных промптов показало свою эффективность для автоматизированной генерации графических моделей. Результаты работы свидетельствуют о том, что данный подход существенно снижает порог входа для создания UML-диаграмм, предоставляя специалистам из различных предметных областей инструмент для визуализации архитектуры систем. В ходе работы были получены практические навыки составления и оптимизации промптов для решения конкретной задачи генерации кода для построения диаграмм PlantUML.

Заключение

Противодействие фишингу — это не разовое мероприятие, а непрерывный процесс развития цифровой грамотности и формирования устойчивых привычек безопасности. Как демонстрирует данный гид, эффективная защита строится на комбинации теоретического понимания тактик злоумышленников и практического применения простых, но действенных правил верификации.

Ключевым выводом является необходимость постоянной бдительности и критической оценки любого запроса на конфиденциальные данные или совершение необходимых действий, независимо от канала связи или кажущейся надёжности источника. Технические средства защиты (антивирусы, фильтры) играют важную, но вспомогательную роль; основным барьером на пути фишинга остаётся осведомлённый пользователь.

Внедрение культуры кибербезопасности, где проверка ссылки, анализ адреса отправителя и использование двухфакторной аутентификации становится естественной практикой, значительно снижает риски. Важно помнить, что в цифровой среде ответственность за свою безопасность начинается с умения задать правильный вопрос и не поддаваться на искусно созданную иллюзию доверия. Регулярное обновление знаний и обмен опытом по распознаванию новых фишинговых схем — лучшая инвестиция в собственную цифровую безопасность.

Список источников

1. Энциклопедия Лаборатории «Касперского» : сайт : URL: <https://encyclopedia.kaspersky.ru/> (дата обращения: 05.10.2025)
2. Языковая модель DeepSeek 3.0 : сайт : URL: <https://chat.deepseek.com/> (дата обращения: 05.10.2025)
3. Языковая модель Алиса AI : сайт : URL: <https://alice.yandex.ru/> (дата обращения: 05.10.2025)
4. Блог компании Halborn : сайт : URL: <https://www.halborn.com/> (дата обращения: 02.11.2025)
5. Блог компании Cofense : сайт : URL: <https://cofense.com/> (дата обращения: 02.11.2025)
6. Подразделение ФБР «Центр рассмотрения жалоб на интернет-преступления» : сайт : URL: <https://www.ic3.gov/> (дата обращения: 02.11.2025)
7. Генеративная модель Yandex ART 2.7 : сайт : URL: <https://shedevrum.ai/> (дата обращения: 16.11.2025)
8. Генеративная модель Kandinsky 3.0 : сайт : URL: <https://giga.chat/> (дата обращения: 16.11.2025)
9. Редактор UML-диаграмм «PlantUML» : сайт : URL: <https://plantuml-editor.vercel.app/> (дата обращения: 29.11.2025)