

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

Кафедра «Прикладная математика
и информатика»

ОТЧЕТ

о выполнении индивидуального задания № 1

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

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

ЦЕЛЬ РАБОТЫ: сформировать понимание актуальных угроз и собрать материал для гида, используя ИИ как инструмент поиска и анализа.

ЗАДАЧА: создать промты для интеллектуального ассистента (Qween, Grok, DeepSeek, YandexGPT), который позволит собрать данные о выбранной цифровой угрозе (например, фишинг, утечка данных, фейковые новости), проанализировать их и подготовить раздел для гида, ориентированный на первокурсников.

ХОД ВЫПОЛНЕНИЯ РАБОТЫ

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 разделится на массовый и целевой. Массовый фишинг рассылается 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: УТОЧНЕНИЯ 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 общеизвестные факты или стандарты, а также на исследования крупных IT-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 примечательна 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 YndexGPT:

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 IT-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.