

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

Кафедра «Прикладная математика
и информатика»

ОТЧЕТ
о выполнении индивидуального задания № 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

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

ЦЕЛЬ РАБОТЫ: создать тексты разделов гида, применяя техники промпт-инжиниринга. Научиться формулировать сложные промпты для анализа реального кейса цифровой угрозы, создавать структурированный и понятный текст для цифрового гида по медиабезопасности для различных ролей пользователей, а также проверять ответы ИИ на логическую связность и практическую применимость.

ЗАДАЧА: создать промпты для интеллектуального ассистента (DeepSeek, YandexGPT, Grok, GigaChat), которые позволят проанализировать реальные кейсы по выбранной согласно варианту цифровой угрозе выделить ключевые факторы и создать текст для раздела гида, объясняющий, как избежать подобных угроз, для различных ролей пользователей.

ХОД ВЫПОЛНЕНИЯ РАБОТЫ

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 промта 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 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.

```
</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 промтата 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:

	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 годы? 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	<p>Алгоритм «Банк тебе не пишет просто так»:</p> <ol style="list-style-type: none"> Запомни: настоящий банк никогда не будет в 	<p>Алгоритм «Банк звонит? Перезвони сам!»:</p> <ol style="list-style-type: none"> Ничего не говори. Если тебе звонят, 	<p>Алгоритм «Компрометация рабочих учетных данных»:</p>

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

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.