МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования
09.03.01 «Информатика и вычислительная техника»

ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №4

Практическая работа по дисциплине
«Основы информационной безопасности»
студента 3 курса группы ИВТ-б-о-222(2)
Чудопалова Богдана Андреевича

Симферополь, 2024

ЦЕЛЬ: Цель данной работы заключается в анализе актуальности такой проблемы, как социальная инженерия. Также было необходимо создать опросник на данную тему и на основе ответов сформировать картину того, какая степень осведомленности присуща людям.

ХОД РАБОТЫ:

Социальная инженерия — это практика манипулирования людьми, чтобы получить конфиденциальную информацию или заставить их совершить определенные действия. Она базируется на использовании психологических уловок, чтобы обойти технические меры безопасности.

Чтобы корректно сформулировать актуальность данной проблемы я обратился к книге Кевина Митника «Искусство обмана» в которой он обстоятельно рассмотрел данное явление. В главе 1 он привел пример, притворяясь сотрудником компании он смог получить пароли и кусочки секретной информации компании, тем самым он хотел продемонстрировать, что компания может приобрести лучшие технологии по защите информации, новсегда останется человеческий фактор, а это именно то, из-за чего они до сих пор уязвимы.[1]

Также в своей книге Митник рассматривает феномен, суть которого заключается в том, что информация, которая находится во владении компании и кажется безвредной, на самом деле может быть очень существенной в руках социального инженера и сотрудник без особых на то препятствий может ее разгласить, если социальный инженер сможет завоевать доверие своей потенциальной жертвы, о чем, кстати тоже пишет Митник.

Таким образом, исходя из того, что пишет автор можно сказать, что проблема социальной инженерии будет актуальна до тех пор пока будет существовать информация и с этой информацией будут работать люди.

Далее с помощью сервиса YandexForms[2] я создал опросник, содержащий следующие вопросы:

Что такое социальная инженерия?

- ○ Механизм, используемый для анализа социальных тенденций.
- ◉ Психологическое манипулирование людьми для получения конфиденциальной информации.
- ○ Методология проектирования социальных программ и услуг.

Какие виды атак социальной инженерии вам известны? (Выберите все подходящие варианты)

- ☑ Фишинг
- ☑ Вишинг
- ☑ Скимминг
- ☑ Претекстинг

Как можно защитить себя от социальной инженерии на работе?

- ○ Использовать пароли, состоящие из простых слов для легкого запоминания
- ◉ Обучаться распознаванию подозрительных электронных писем и сообщений, соблюдать меры информационной безопасности
- ○ Открывать все ссылки и вложения для проверки их содержания

Рис. 1. Часть вопросов.

Какие признаки могут указывать на попытку социальной инженерии?

- Полностью формализованные запросы, поступающие через официальные каналы
- **Настойчивые требования предоставить личные или финансовые данные, использование давления и манипуляций**
- Предложение провести легальную транзакцию с использованием защищенных каналов

Какую роль играет доверие в социальной инженерии?

- Отсутствие значимого влияния на эффективность атаки
- **Ключевой фактор, на котором базируются большинство социальных инженерных атак, используется для создания ложного чувства безопасности**
- Элемент, который применяется только в высокотехнологичных атаках, не имеющих отношение к персональным манипуляциям

Как современные технологии (например, искусственный интеллект) могут использоваться в социальных инженерных атаках?

- Исключительно для улучшения безопасности данных и защиты от хакеров
- **Автоматизация фишинговых кампаний, персонализация атак, анализ поведения пользователей для выбора целей**
- Никак не применяются, так как социальная инженерия полностью базируется на человеческом факторе

Рис. 2. Вторая часть вопросов.

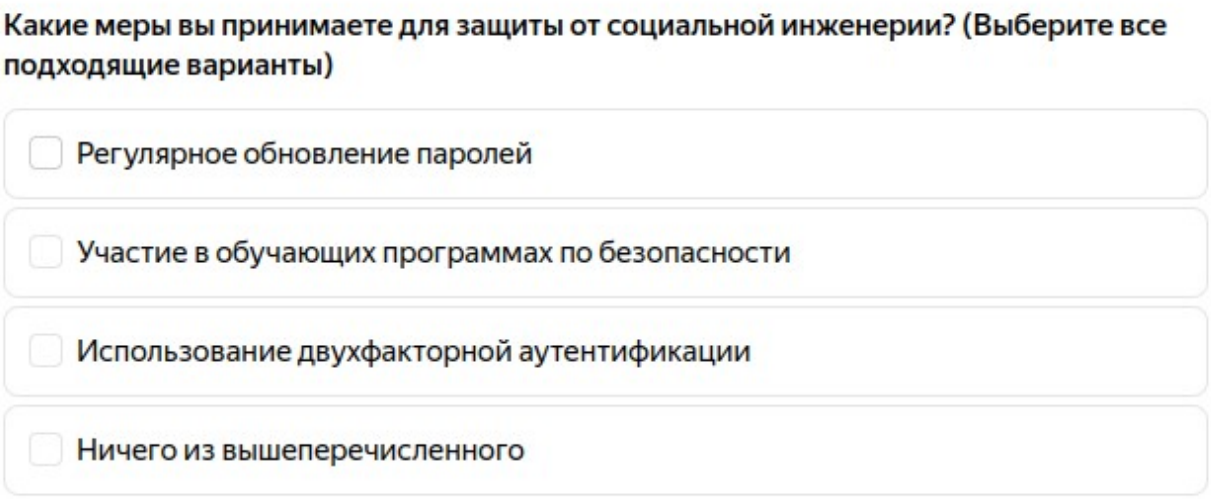

Рис. 3. Последний вопрос.

Мой опросник прошло 10 человек, полученные результаты:

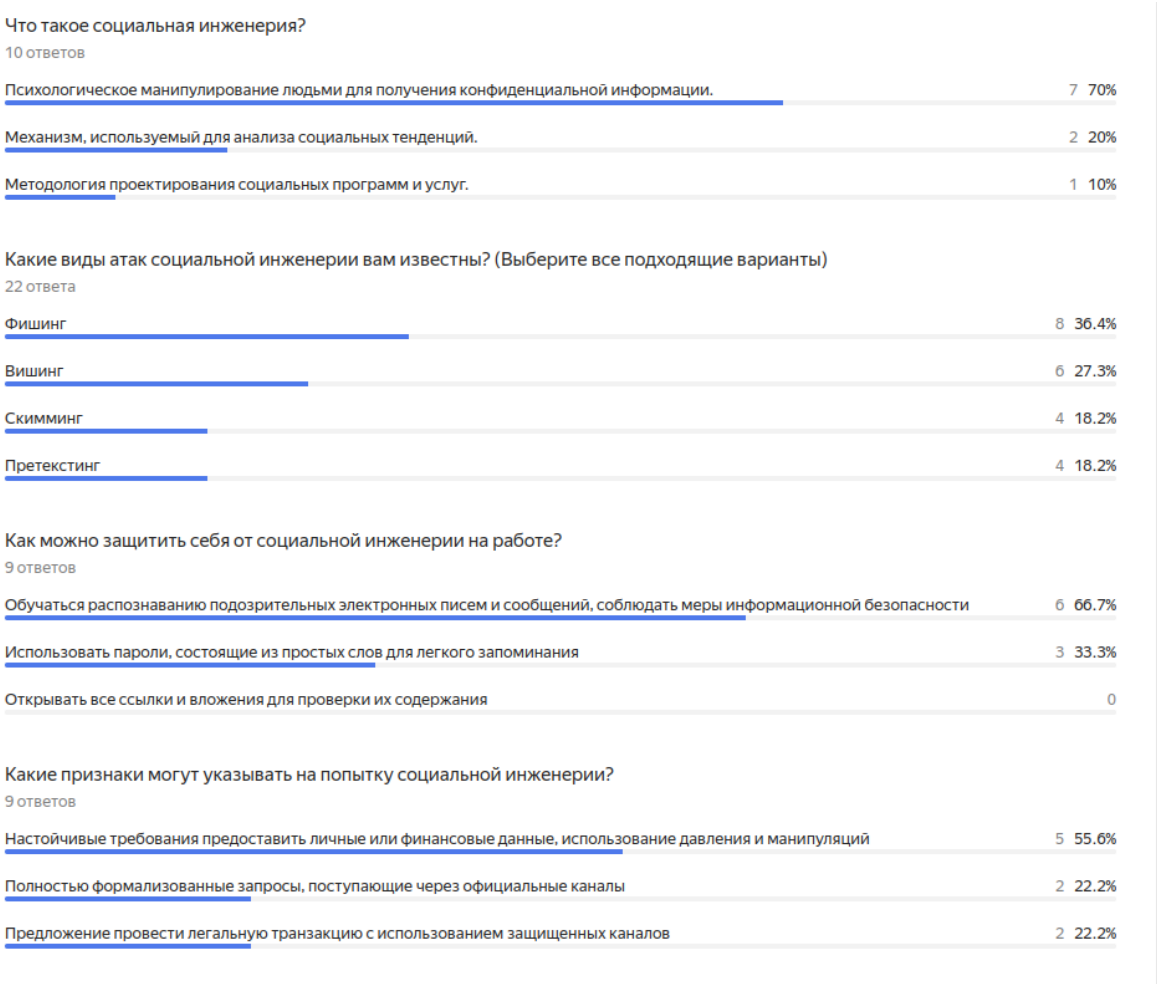

Рис. 4. Ответы на вопросы.

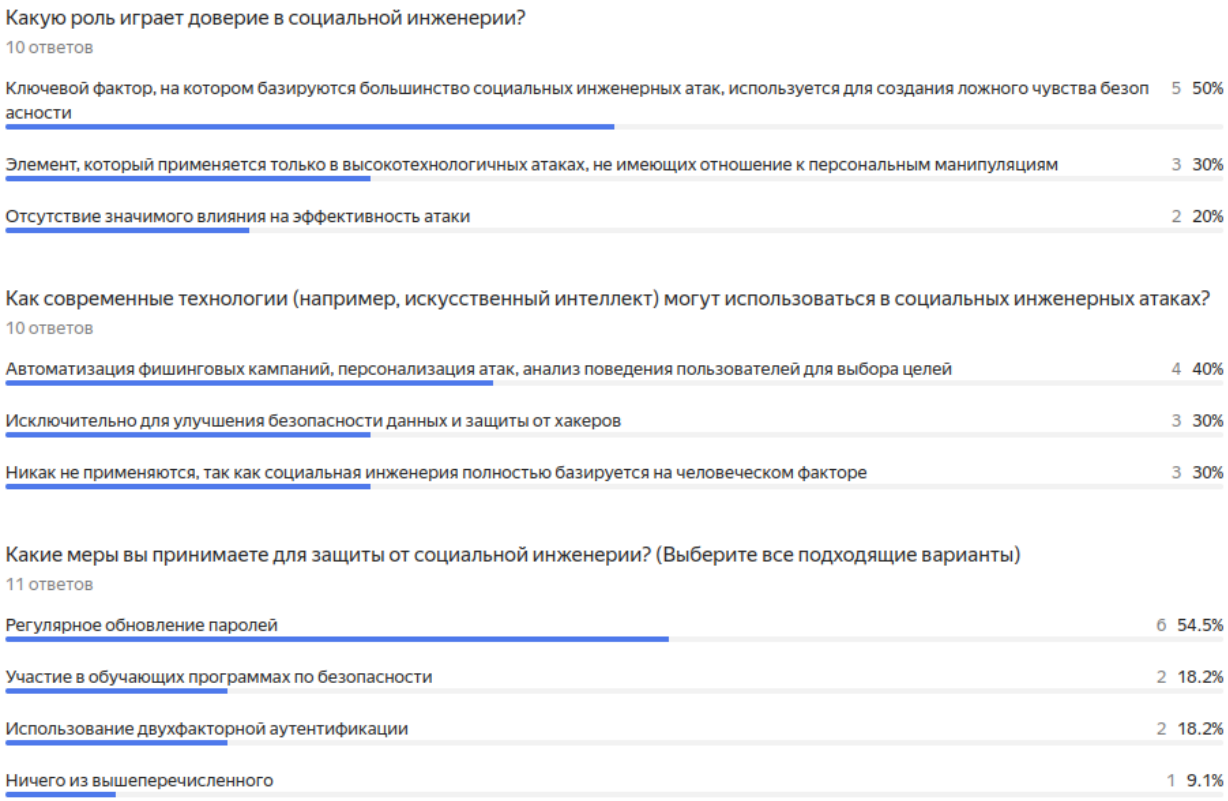

Рис. 5. Ответы на последние вопросы.

Исходя из распределения ответов можно сделать следующие выводы:

1.Общие знания о социальной инженерии:

- Большинство респондентов правильно определяют социальную инженерию как психологическое манипулирование для получения конфиденциальной информации, что демонстрирует базовый уровень осведомленности. Однако некоторые респонденты дают неверные определения, например, связывают социальную инженерию с анализом социальных тенденций или проектированием социальных программ, что свидетельствует о недостаточном понимании термина.

2. Виды атак:

- Наиболее часто упоминаются такие атаки, как фишинг и вишинг, что указывает на хорошее знание этих распространённых видов атак. Однако скимминг и претекстинг упоминаются значительно реже, а некоторые

респонденты не знают о существовании этих видов атак, что говорит о недостаточной осведомленности в более редких формах социальной инженерии.

3. Методы защиты:

- Большинство респондентов признают важность регулярного обновления паролей, что является правильной мерой безопасности. Однако многие не используют другие важные меры, такие как двухфакторная аутентификация и участие в обучающих программах, что указывает на недостаток комплексного подхода к защите от социальной инженерии.

4. Современные технологии:

- Знания о том, как современные технологии могут быть использованы в социальных инженерных атаках, также ограничены. Некоторые респонденты считают, что технологии не играют роли в социальной инженерии, что является заблуждением. Это свидетельствует о том, что понимание интеграции технологий, таких как ИИ, для автоматизации атак и анализа поведения, недостаточно развито у части респондентов.

Общий вывод:

Респонденты обладают базовыми знаниями о социальной инженерии, особенно в отношении наиболее распространённых видов атак (фишинг, вишинг) и некоторых методов защиты (обновление паролей). Однако их осведомленность о менее известных атаках и современных методах, таких как использование ИИ, ограничена. Это говорит о среднем или ниже среднего уровне общей осведомленности.

ВЫВОД: В результате проведённой работы была выполнена задача по исследованию актуальности проблемы социальной инженерии. Сначала была проведена теоретическая часть, в которой раскрыто определение социальной инженерии и рассмотрены её основные аспекты. С опорой на труды Кевина Митника, в частности книгу «Искусство обмана», было выявлено, что социальная инженерия остаётся актуальной проблемой. Практическая часть работы заключалась в создании и проведении опроса, который охватил вопросы, касающиеся знаний респондентов о социальной инженерии, её видах, методах защиты и использовании современных технологий в атаках. Опрос прошли 10 человек, и по итогам анализа их ответов был сделан вывод о среднем уровне осведомлённости среди респондентов.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Митник К. Д., Симон У. Л. Искусство обмана. Москва: Альпина Бизнес Букс, 2004. 320 с.

2. Сервис YandexForms [Электронный ресурс]. URL: https://forms.yandex.ru (Дата обращения 18.10.24)