Творческий проект по технологии на тему:

**«Программа для защиты от мошеннических сайтов»**

**Выполнил:**

**Бородин Денис Викторович**

2025

# Оглавление

[Оглавление 2](#_Toc188445430)

# Реферат

# Определения, сокращения и обозначения

Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям, персональным данным и т.д.

# Введение

## Проблема и её актуальность

В настоящее время наблюдается стремительное увеличение числа киберпреступлений. Одним из самых распространённых видов киберпреступления является фишинг. В этом случае жертва, поддавшись обману, неосознанно передаёт конфиденциальную информацию, которую мошенники затем используют для нанесения материального вреда.

С каждым годом количество фишинговых атак увеличивается, а их методы модернизируются. Ключевым фактором успеха таких атак остаётся человеческий фактор: мошенники активно используют социальную инженерию, манипулируя эмоциями и доверием жертв."

Анализ актуальности проблемы основан на отчёте “Лаборатории Касперского” по спаму и фишингу за 2023 год. Основной целью фишинговых атак в последние года является почта – 96% от всех атак. Существует много видов фишинга, связанных с почтой, но выделить можно несколько основных:

1. Email/spam – наиболее распространенный вид фишинга. Поддельное письмо с вредоносным файлом/ссылкой отправляется огромному количеству пользователей, в надежде на то, что фишинг атака закончится успехом.
2. Spear phishing – похож на спам, но отличается тем, что атака становится более целенаправленной. Злоумышленники знают кого преследуют, и заранее исследуют цель для подготовки наиболее удачной атаки. Может затрагивать как обычных пользователей, так и организацию.
3. Whaling – метод не сильно отличающийся от spear phishing, но целевая группа становится более специфичной и ограниченной. Этот метод нацелен на руководящие должности.
4. Clone phishing – метод, в котором настоящее и ранее отправленное электронное письмо, содержащее вложение или ссылку, используется для создания идентичного письма, в котором настоящие вложения/ссылки будут заменены на вредоносные.

Как мы видим – большинство методов фишинга связаны с вредоносными файлами/ссылками, так что рассмотреть стоит эти две проблемы.

На Рис. П.1. мы можем видеть диаграмму, на которой показана доля спама в почтовом трафике российского интернета. В среднем на протяжении 2023 года она составляла 46,59%, что является крайне высоким показателем и указывает на то, что почти каждое второе письмо является спамом. Но больше всего нас интересуют Рис. П.2. на котором изображена диаграмма количества срабатываний антивируса на попытки открытия вредоносных файлов во вложениях к письмам и Рис. П.3. на котором изображена диаграмма количества срабатываний антивируса на попытки перехода по вредоносным ссылкам в письмах. Всего попыток открыть вредоносные файлы было 136 миллионов, а попыток перейти по опасным ссылкам – 710 миллионов. По этим данным мы можем судить, что количество попыток открыть вредоносные ссылки преобладает более чем в 5 раз. Соответственно, проблема фишинговых сайтов актуальней и подлежит скорейшему решению.

# 1.2 Цели и задачи проекта

**Цель работы**: Создание программы по защите от вредоносных сайтов/ссылок, удобной для работы массовому пользователю.

**Задачи:**

1. Изучить угрозы, которые несут мошеннические сайты;
2. **Провести анализ целевой аудитории;**
3. Выбрать оптимальные методы и инструменты для разработки решения проблемы;
4. Рассмотреть аналоги решения проблемы и аналоги продукта;
5. Разработать рабочий прототип программы;
6. **Разработать документацию и инструкции для пользователей;**
7. Провести опрос про удобство рабочего прототипа;
8. Составить план дальнейшего развития проекта;

# Подготовительный этап

## 2.1 Анализ угроз, которые несут мошеннические сайты

Для разработки методов борьбы с фишинговыми сайтами необходимо, прежде всего, изучить угрозы, которые они представляют. Поскольку технологии мошенничества постоянно развиваются, важно сосредоточиться на актуальных угрозах, чтобы понять общие принципы работы таких сайтов. Несмотря на разнообразие фишинговых сайтов, их механизмы обмана часто схожи. Для понимания этих механизмов достаточно рассмотреть несколько типичных примеров:

1. **Сайты для геймеров с предложением покупки игр или внутриигровой валюты**. Пользователь, надеясь получить товар по выгодной цене, вводит свои персональные данные и оплачивает покупку, но в результате остаётся без товара, а его данные попадают в руки мошенников.
2. **Сайты с предложениями о выигрышах или компенсациях**. Соблазнившись возможностью легко получить деньги, пользователь вводит свои персональные данные, включая данные банковской карты, что может привести как к краже средств, так и к краже личных данных.

Как видно, основная опасность фишинговых сайтов заключается не в их технической вредоносности, а в обмане пользователя, который добровольно передаёт свои данные или совершает платежи. Соответственно, мы можем предотвратить атаку даже после того, как пользователь перешёл по ссылке.

## Анализ соответствия нормативно-правовой базе

Для составления плана дальнейшего развития проекта нужно будет понимать, какие группы лиц больше всего пользуются нашей программой. Так как она будет предполагать обработку персональных в виде опроса пользователей при первом заходе в программу – нам нужно будет соблюсти требования Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ.

Так как данные будут собираться для статистики, условия для сбора персональных данных должны соответствовать п. 8 ст. 6 Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ, а именно сбор должен проходить с согласия пользователя, а данные должны быть обезличены. Также собранные данные не будут пересекаться со списком специальных данных указанных в п. 8 ст. 6 Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ.

## Выбор инструментов и методов

Этот этап можно считать по настоящему важным, так как от выбранных инструментов зависят многие характеристики конечного продукта. Мы разрабатываем десктопное приложение, с вектором на дальнейшую кроссплатформенность, вследствие чего основным инструментом на протяжении всей разработки будет фреймворк. Для удобного просмотра основных параметров фреймворка была сделана таблица.

Табл. 1. Сравнение аналогов



Самыми главными параметрами при выборе можно по праву считать поддерживаемые платформы и лицензию. Для начала следует разобрать вопрос лицензий. Все виды лицензий (кроме GPL) в таблице почти не накладывают ограничений на использование в коммерческих продуктах. Также, как можно видеть в таблице, Electron js и GTK не имеют поддержки мобильных устройств, что сразу делает их намного менее привлекательными для нашей программы. В итоге нам стоит рассмотреть только 2 фреймворка – Flutter и Qt. По своим параметрам они очень похожи, но отличия возникают при их ближайшем рассмотрении: Flutter поддерживает только язык программирования Dart, в то время как на Qt можно писать почти на всех наиболее распространённых языках. После выбора фреймворка было решено писать на Python, так как по сравнению с c++ с ним будет проще и быстрее работать.

После выбора языка перед нами появляется проблема в виде того, что библиотека PyQt для работы с Qt распространяется по лицензии GPL, что не позволит использовать её в коммерческих проектах. Но также существует и библиотека PySide, которая почти полностью идентична PyQt, но при этом распространяется по лицензии LGPL, соответственно использовать мы будем её.

Среди методов, изначально рассматриваемых для реализации в прототипе программы, можно выделить 3 основных:

1. Анализ сайта с помощью машинного обучения по совокупности его характеристик. При таком методе рассматриваются абсолютно разные характеристики – от регистрационных данных сайта до характеристик его URL адреса. Проблема этого метода состоит в том, что он очень сложно алгоритмически реализуется, а также не поддается стандартизации, вследствие чего данный вариант был отложен на будущее.
2. Ручная проверка ссылки с использованием базы со списком адресов фишинг-сайтов.
3. Использование автоматической проверки сайтов, на которые заходит пользователь с помощью DNS.

## Оригинальность и сравнение с аналогами

Непрямыми аналогами программы можно считать сайты и приложения с функцией проверки ссылок. Не было найдено ни одного десктопного приложения с возможностью проверить ссылки ли подключить DNS для защиты от них, из-за чего было решено сравнить функционал нашей программы с сайтами и мобильными приложениями. Для наглядности сравнения была также приведена таблица.

# Список использованной литературы

1. Отчёт “Лаборатории Касперского” по спаму и фишингу за 2023 год [Электронный ресурс]. URL: <https://securelist.ru/spam-phishing-report-2023/109104/>
2. APWG | Phishing Activity Trends Reports [Электронный ресурс]. URL: https://apwg.org/trendsreports/
3. Анализ угроз информационной безопасности при использовании фишинговых сайтов [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/analiz-ugroz-informatsionnoy-bezopasnosti-pri-ispolzovanii-fishingovyh-saytov/viewer>
4. Исследование техник фишинга и методов защиты от него [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/issledovanie-tehnik-fishinga-i-metodov-zaschity-ot-nego/viewer>
5. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ // СПС КонсультантПлюс

# Приложение №1. Графики

Рис. П1.1. Доля спама в почтовом трафике российского интернета

Рис. П1.2. Количество срабатываний почтового антивируса на попытки открыть вредоносный файл

Рис. П1.3. Количество срабатываний системы “Антифишинг” на попытки перехода по мошеннической ссылке