Всероссийская олимпиада школьников по Технологии

Профиль: «Информационная безопасность» 9 класс

Пояснительная записка

к проектной работе по теме:

«Категоризация сайтов при использовании маршрутизатора пользователем»

2023

РЕФЕРАТ

Объектом исследования является безопасность использования сети Интернет с помощью маршрутизатора/роутера.

1. Цели работы:

1.1 Изучить процесс работы маршрутизатора/роутера

1.2 Выявить проблемы информационной безопасности при использовании сети Интернет

1.3 Рассмотреть возможные варианты решения проблем

2. Задачи, рассматриваемые в проекте:

2.1 Минимизировать угрозу неправомерной кражи личных данных пользователя

2.2 Сохранить конфиденциальность персональных данных пользователя сети Интернет

2.3 Создание продукта, доступного для любого пользователя

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Интернет - это глобальная сеть для хранения и передачи информации, которая состоит из миллионов компьютерных сетей, связанных между собой по всему миру. Используя интернет, пользователи могут обмениваться электронной почтой, скачивать файлы, искать информацию, просматривать веб-страницы и делать многое другое.

Использование интернета в мире актуально и продолжает расти. В настоящее время большинство людей используют Интернет для поиска информации, общения с друзьями и коллегами, просмотра видео и т.д. Также многие коммерческие компании используют Интернет для продвижения своих товаров и услуг. С каждым днём количество пользователей растёт. Однако увеличивается и количество киберпреступлений. И недостаточная защита при пользовании интернетом может привести к серьезным последствиям, таким как утечка личных данных, потеря финансовых средств, вред компьютеру и другие. Поэтому безопасность использования интернета и информационных и коммуникационных технологий одна из актуальнейших и важнейших тем современности.

1. Понятие маршрутизатора и принцип его работы

По данным Всемирной статистики в мире насчитывается более 8 млрд людей[1]. Согласно статистике Международного союза электросвязи (МСЭ или ITU), специализированного учреждения ООН, состоянию на 2021 года в мире насчитывается почти 5 миллиардов пользователей Интернета[2]. И с каждым годом данное число продолжает расти с огромной скоростью.

По мере роста числа пользователей Интернета каждая отрасль, которая хоть немного связана с Интернетом, даже если отдаленно от неё, растет вместе с ним. Одна из первых вещей, когда речь заходит об Интернете, - это безопасность её использования.

Рассмотрим одно из устройств сетевого оборудования — маршрутизатор. Маршрутизатор – это устройство, которое строит на основе таблицы маршрутизации локальную сеть, принимает внешние пакеты от интернет провайдера и передаёт их получателю по кабелю или беспроводной технологии Wi-Fi (Wireless Fidelity). Маршрутизаторы работают на «сетевом» (третьем) уровне сетевой модели OSI (The Open Systems Interconnection model).

Как домашний роутер передает данные?

1. Пакет данных покидает устройство и проходит через локальную сеть до роутера.
2. Прием данных. Маршрутизатор получает данные от устройств, подключенных к нему. Данные могут быть отправлены в локальную сеть, или же маршрутизатор может получить запрос извне.
3. Определение маршрута. Для этого он использует информацию о сетях, к которым он подключен, и таблицу маршрутизации. Таблица маршрутизации содержит информацию о том, какие устройства находятся

в каких сетях, и какие маршруты нужно использовать для доставки данных до нужного устройства.

4. Передача данных. Маршрутизатор отправляет данные через соответствующий маршрут до нужного устройства или внешней сети через другие маршрутизаторы.
5. Обработка запросов на доступ. Если маршрутизатор получает запрос на доступ к сети извне, то он использует механизм NAT (Network Address Translation), который позволяет перенаправлять запросы на нужное устройство в локальной сети.

Работа домашнего маршрутизатора заключается в том, чтобы пересылать данные между сетями или устройствами на разных сетях. Он использует адреса IP (Internet Protocol) для определения, куда нужно переслать данные. Когда данные поступают на маршрутизатор, он анализирует их и пересылает дальше по правильному пути. Таким образом, маршрутизатор позволяет устройствам на разных сетях обмениваться данными.

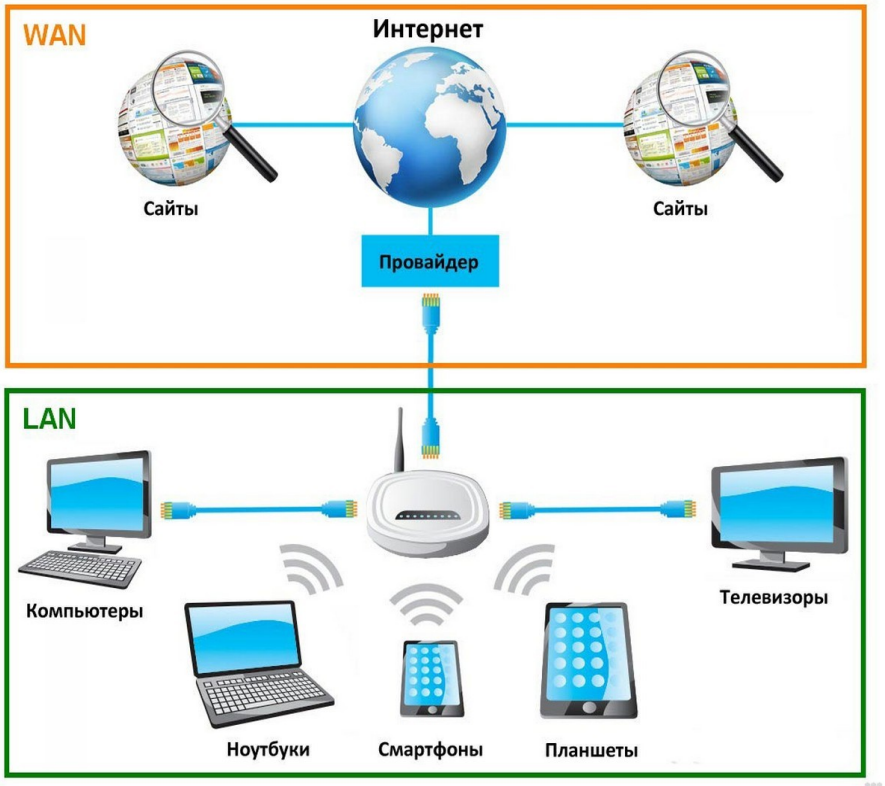

Рисунок 1. Схема подключения маршрутизатора

2. Безопасность использования интернета и возможные угрозы

Поддельные сайты - это веб-сайты, созданные злоумышленниками, которые имитируют настоящие сайты компаний, организаций, правительственных учреждений или банков, чтобы получить доступ к личной информации и финансовым средствам пользователей. Многие поддельные сайты достаточно опасны, так как могут привести к краже личных данных, финансового мошенничества, а также содержать вредоносные программы, которые могут навредить вашему компьютеру или украсть вашу личную информацию. Некоторые из наиболее распространенных видов угроз, которые могут быть скрыты на поддельных сайтах, включают следующее:

1. Кража личных данных: злоумышленники могут создать поддельный сайт, который выглядит как оригинальный(например, государственные сайты), и попросить пользователя ввести свои личные данные, например, имя, номера паспорта, номера кредитных карт и другие. Эти данные могут быть использованы для кражи личности, мошенничества и других киберпреступлений.

2. Финансовое мошенничество: злоумышленники могут создать поддельный сайт похожий на банковский или платежную систему, и попросить пользователя ввести свои номера карт, CVV-коды и другие. Эти данные могут быть использованы для кражи денег с банковских счетов или кредитных карт.

3. Установка вредоносного ПО: злоумышленники могут создать поддельный сайт, который может содержать вредоносные программы (Malware(мальвар) - это любой вид вредоносной программы, разработанный для нанесения вреда устройству), такие, как вирусы, троянские программы или шпионское ПО. При посещении такого сайта вредоносное ПО может быть загружено на компьютер пользователя без его ведома.

4. Распространение спама: злоумышленники могут использовать поддельные сайты для сбора адресов электронной почты и других контактных данных пользователей. Эти данные могут быть использованы для отправки спама или фишинговых писем.

5. Кража паролей: злоумышленники могут создать поддельный сайт, который выглядит как сайт социальной сети или другой онлайн-сервис, и попросить пользователя ввести свой логин и пароль. Эти данные могут быть использованы для кражи учетных записей пользователей.

К сожалению, точной статистики по количеству создаваемых фальшивых сайтов каждый день нет. Однако, согласно отчету компании Anti-Phishing Working Group[6] за первый квартал 2021 года, было обнаружено и заблокировано более 160 000 уникальных фишинговых сайтов. Количество людей, попадающих на поддельные сайты, достаточно высоко, так как злоумышленники постоянно усовершенствуют свои методы и делают фальшивку все более убедительными.

По статистике из отчёта[7] «Лаборатории Касперского» о спаме и фишинге в 2022 году количество атак с помощью поддельных сайтов заметно выросло. Больше всего попыток перехода по вредоносным ссылкам было связано со страницами, имитирующими службы доставки (27%), онлайн-магазины (16%), платежные системы (10%) и банки (10%)

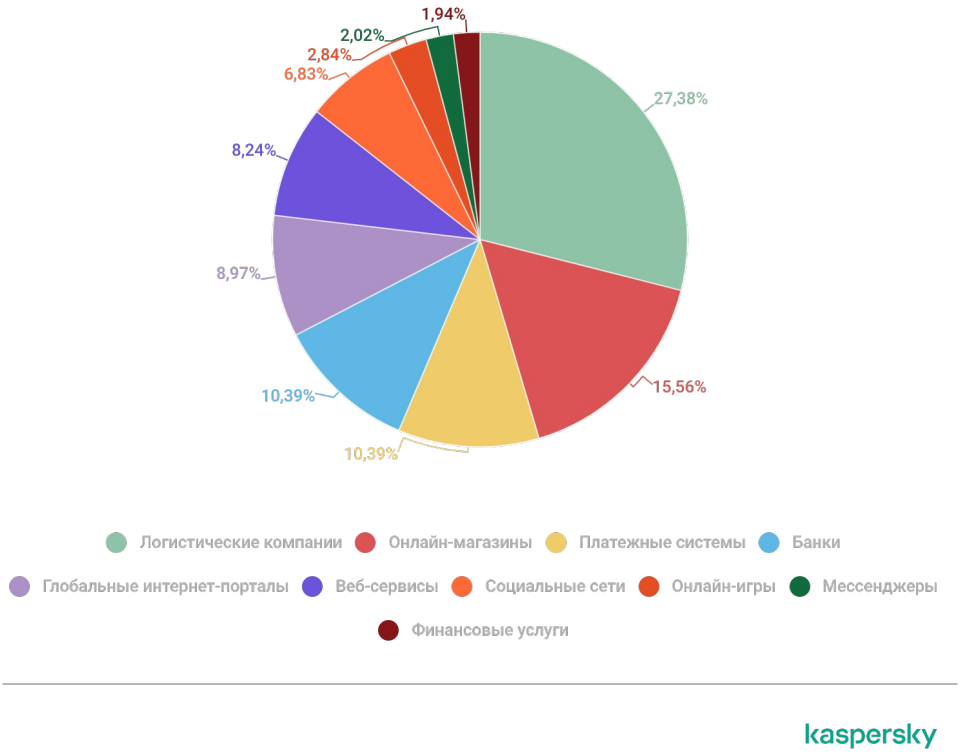

Рисунок 2. Отчёт «Лаборатории Касперского» о спаме и фишинге

Как злоумышленникам удаётся показать фальшивку за оригинал?

1. Создаются доменные имена, которые очень похожи на оригинальные. Например, может заменить одну букву в доменном имени на похожую или же удалить какой-то символ. Например, они могут заменить латинскую букву "o" на цифру "0" в доменном имени.

2. Копируются дизайн и контент. Злоумышленник может создать сайт, который выглядит и работает точно так же, как оригинальный, поэтому сложно распознать подделку.

3. Используют социальную инженерии. Злоумышленники могут использовать различные методы, чтобы убедить пользователей перейти на поддельный сайт и ввести свои личные данные. Чаще всего наблюдается отправка электронных писем, сообщений в социальных сетях или телефонных звонков.

4. Некачественные поисковые запросы: злоумышленники могут создавать веб-страницы, которые будут появляться в результатах поиска, когда пользователи вводят определенные запросы. Например, когда пользователи ищут бесплатные загрузки программного обеспечения или торренты.

Но не все знают, как отличить оригинальный сайт от поддельного, так как они очень похожи, и злоумышленники стараются показать фальшивку все более убедительными. Например, по данным из отчёта “Лаборатории Касперского” в 2022г. мошенники в качестве приманки использовали одно из самых ожидаемых для людей: новые фильмы и сериалы. На сайтах предлагалось оформить подписку, посмотреть новинки до выхода в кинотеатры. После ввода номера карты и других данных пользователь рисковал не только оплатить несуществующую покупку, но и передать данные злоумышленнику. Примерно также работали мошеннические сайты, обещавшие бесплатные трансляции футбольных матчей в Катаре.

У провайдеров есть функция фильтрации трафика. Но он блокирует только сайты, которые прописаны в Едином реестре запрещённых сайтов. Если адрес сайта находится в этом списке, то провайдер блокирует к нему доступ.

По последним данным Росстата, аудитория интернета в России составляет более 100 млн человек. В 2020 году большинство пользователей интернета (более 60%) относятся к возрастной группе от 18 до 44 лет. Кроме того, значительное количество пользователей интернета приходится на возрастную группу от 45 до 54 лет (15%), а возрастная группа от 55 до 64 лет составляет около 10%. Также некоторое количество пользователей интернета приходится на возрастные группы до 18 лет и более 65 лет (соответственно 8% и 7%).

Большинство людей зрелого и пожилого возраста, а также часть остальных людей не берут во внимание, что стоит быть осторожным при переходе по ссылке на незнакомый сайт. Получается, есть риск угрозы неправомерного доступа к личной информации и финансовым средствам пользователей.

3. Решение проблемы неправомерного доступа к личной информации пользователей

На основании проведённых выше исследований были сделаны выводы и предложено решение по снижению и минимизации возможности неправомерного доступа к личной информации пользователей. Наиболее эффективной возможной реализацией этой проблемы - создание модификации для маршрутизатора, которое поможет пользователю улучшить защиту своего роутера путём категоризации оригинальных и вредоносных сайтов.

Основная концепция данной программа будет заключаться в выполнении следующих функций:

- На сервере лежит список нежелательных и вредоносных сайтов, который будет обновляться. Для этого можно использовать любой удобный формат, например, текстовый файл или базу данных.
- Пользователь заходит на сайт. Пакет данных покидает устройство и проходит через локальную сеть до маршрутизатора.
- Роутер принимает данные и отслеживание трафика пользователей, то есть анализирует URL-адрес, на который пользователь пытается зайти.
- Если URL-адрес, на который пытается зайти пользователь, находится в списке запрещенных сайтов, то программа блокирует доступ к нему. В таком случае будет выведено уведомление пользователю, что данный сайт считается вредоносным, поэтому он заблокирован.
- Программа будет работать в фоновом режиме, автоматически обновлять список запрещенных сайтов один раз в день ночью, чтобы у пользователя не возникли проблемы с доступом к сети Интернет.

В ходе исследования мною были обнаружено следующие аналоги программы, описанной выше:

1. Norton Safe Web - программа, проверяющая сайты на наличие вредоносного контента и блокирует доступ к ним.

2. Avast Online Security - расширение для браузера, предупреждает о фишинговых сайтах и блокирует доступ к ним.

3. McAfee WebAdvisor - программа, которая предупреждает пользователей о фишинговых сайтах и блокирует доступ к ним.

4. Malwarebytes Browser Guard - расширение для браузера, блокирующее доступ к фишинговым сайтам и предупреждает пользователей о потенциальных угрозах.

5. Bitdefender TrafficLight - расширение для браузера, которое блокирует доступ к фишинговым сайтам и предупреждает пользователей о потенциальных угрозах.

Но программа (предложенная мною), встроенная в маршрутизатор и блокирующая подозрительные сайты, имеет ряд преимуществ по сравнению с сервисами и расширениями для браузеров, выполняющих ту же функцию:

1. Программа блокирует доступ к подозрительным сайтам на уровне маршрутизатора. Это означает, что все устройства, подключенные к нему, будут защищены от этих сайтов. Сервисы и расширения для браузеров блокируют только те сайты, которые открыты в этом конкретном браузере.

2. Защита от всех угроз: программа блокирует не только фишинговые сайты, но и другие подозрительные сайты, которые могут содержать вредоносный код, вирусы, трояны и другие угрозы.

3. Не требует установки на каждом устройстве: сервисы и расширения для браузеров требуют установки на каждом устройстве, которое нужно защитить. А

программа, которая встроена в маршрутизатор, защищает все устройства, подключенные к нему, без необходимости установки на каждом из них.

Стоит отметить, что данная программа не собирает конфиденциальную информацию и статистику, а ограничивается именно блокировкой ресурсов. Заметим, что этот продукт не нарушает Статью 272 «Неправомерный доступ к компьютерной информации» Главы 28 Уголовного кодекса Российской Федерации. и Федеральный Закон «О персональных данных»[5]. Но можно нарушить заводскую гарантию на маршрутизатор из-за изменения исходных кодов.

ЗАКЛЮЧЕНИЕ

Исходя из всего вышеперечисленного, делаем вывод, что разработка данной программы поможет решить проблему информационной безопасности обычного пользователя сети интернет при использовании маршрутизатора.

Можно с уверенностью утверждать, что эта программа внесёт свой вклад в научный потенциал России и, возможно, всего мира, поскольку это поможет обеспечить более лучшую защиту от несанкционированного доступа к личной информации пользователей

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Worldometer - всемирная статистика в реальном времени — URL: https://www.worldometers.info/ru/

2. ITU Facts and Figures 2021 by International Telecommunication Union — URL: https://public.tableau.com/app/profile/ituint/viz/ITUFactsandFigures2021/InternetUse01

3. Маршрутизатор: что это такое, и чем он отличается от роутера? — URL:

https://wifigid.ru/poleznoe-i-interesnoe/marshrutizator

4. Информационное общество в Российской Федерации 2020. Статистический сборник — URL: https://rosstat.gov.ru/storage/mediabank/lqv3T0Rk/info-ob2020.pdf

5. Уголовный Кодекс Российской Федерации Статья 272. Неправомерный доступ к компьютерной информации (—URL: https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/) и Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (—URL: https://www.consultant.ru/document/cons_doc_LAW_61801/)

6. Phishing Activity Trends Report — URL: https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

7. Отчет «Лаборатории Касперского» о спаме и фишинге в 2022 году | Securelist — URL: https://securelist.ru/spam-phishing-scam-report-2022/

8. Быстро, дёшево и опасно: «Лаборатория Касперского» рассказывает, как фишеры создают множество фейковых страниц с помощью готовых инструментов | Лаборатория Касперского — URL: https://www.kaspersky.ru/about/press-releases/2022_bystro-dyoshevo-i-opasno-laboratoriya-kasperskogo-rasskazyvaet-kak-fishery-sozdayut-mnozhestvo-fejkovyh-stranic-s-pomoshyu-gotovyh-instrumentov