

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Вычислительные системы и информационная безопасность»

|  |  |  |
| --- | --- | --- |
| И.о. Зав. кафедрой | | «ВСиИБ» |
| \_\_\_\_\_\_\_\_\_\_\_\_ | | А.Р. Газизов |
| подпись | | И.О. Фамилия |
|  | «число» месяц 2024 г. | |

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

Тема «ДЕТЕКТИРОВАНИЕ ФИШИНГОВЫХ САЙТОВ С ПОМОЩЬЮ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ»

Направление подготовки 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация Защита информации в системах связи и управления

Обозначение ВКР 10.05.02.------.--- группа ВИБТ61

Обучающийся \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.В. Никитин

(подпись, дата) И.О.Ф.

Руководитель ВКР \_\_\_\_\_\_\_\_\_\_\_\_\_\_ доц., к.т.н. А.Ю. Полуян

(подпись, дата) должность, И.О.Ф.

Консультанты по разделам:

Безопасность и экологичность работы \_\_\_\_\_\_\_\_\_\_\_\_\_ проф., д.т.н. ------------------

(подпись, дата) (должность, И.О.Ф.)

Технико-экономическое обоснование \_\_\_\_\_\_\_\_\_\_\_\_\_ профессор, А.Е. Сафронов

(подпись, дата) (должность, И.О.Ф.)

Нормоконтроль \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ст. преп. М.А. Ганжур

(подпись, дата) (должность, И.О.Ф.)

Ростов-на-Дону

2024



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Вычислительные системы и информационная безопасность»

|  |  |  |
| --- | --- | --- |
| И.о. Зав. кафедрой | | «ВСиИБ» |
| \_\_\_\_\_\_\_\_\_\_\_\_ | | А.Р. Газизов |
| подпись | | И.О. Фамилия |
|  | «число» месяц 2024 г. | |

**ЗАДАНИЕ**

на выполнение выпускной квалификационной работы

Тема «ДЕТЕКТИРОВАНИЕ ФИШИНГОВЫХ САЙТОВ С ПОМОЩЬЮ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ СЕТИ»

Обучающийся Никитин Дмитрий Валерьевич

Обозначение ВКР 10.05.02.------.000 группа ВИБТ61

Тема утверждена приказом по ДГТУ от «23» июня 2023 г. № 2831-ЛС-О

Срок представления ВКР к защите «\_\_» \_\_\_\_\_\_\_\_\_ 2024 г.

Исходные данные для выполнения выпускной квалификационной работы:

Содержание выпускной квалификационной работы

Введение: Во введении необходимо изложить актуальность выбранной темы, обозначить объект и предмет исследования, цель и задачи выпускной квалификационной работы, теоретическую и практическую значимость работы, структуру работы.

Наименование и краткое содержание разделов:

1. Обзор проблемы фишинговых атак и методов борьбы с ними. Проблематика фишинговых атак и её актуальность. Анализ методов детектирования фишинговых сайтов. Законодательное регулирование и стандарты в области борьбы с фишингом. Типы и характеристики фишинговых сайтов.

2. Анализ и выбор методов детектирования фишинговых сайтов с использованием нейронных сетей. Основы нейросетевых технологий. Существующие методы детектирования фишинговых сайтов с использованием ИИ. Выбор и обоснование методов детектирования фишинговых сайтов. Определение параметров для анализа сайтов: URL, визуальной составляющей и текст

3. Разработка и обучение нейросети для детектирования фишинговых сайтов. Формирование и предобработка набора данных. Архитектура нейронной сети и её обучение. Тестирование и анализ результатов работы нейросети. Оценка эффективности и точности детектирования фишинговых сайтов.

4. Безопасность и экологичность проекта. Влияние шума на организм человека и защита от них. Расчет уровня шума на рабочем месте. Экологичность работы. Организация и обеспечение пожарной безопасности на предприятии. Выводы.

5. Экономическое обоснование. Спецификация проекта. План–график проектирования и разработки системы. Расчет затрат на разработку проекта.

Заключение: Заключение должно содержать обобщенные результаты проведенной работы в соответствии с поставленной целью и задачами, необходимо указать чем завершается работа – усовершенствованием, модернизацией, дать свои предложения.

Перечень графического и иллюстративного материалов:

1. Первое
2. Второе
3. Третье

Руководитель ВКР \_\_\_\_\_\_\_\_\_\_\_\_\_\_ доц., к.т.н. А.Ю. Полуян

(подпись, дата)

Задание к исполнению принял \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.В. Никитин

**Аннотация**

Выпускная квалификационная работа акцентирует внимание на проблематике фишинговых атак и необходимости эффективного метода их детекции. Основное внимание уделено использованию нейросетевых технологий для автоматического определения подозрительных и потенциально опасных сайтов. Целью данной выпускной квалификационной работы является создание автоматической системы, способной определять подозрительные и потенциально опасные веб-сайты. Актуальность данной работы обусловлена растущим числом фишинговых атак в цифровой среде, которые представляют серьезную угрозу безопасности пользователей. В заключение работы представлены экономическое обоснование предложенного решения и анализ потенциальных рисков, а также экологическая оценка проекта.

Объем текстового материала 82 листа (А4), количество иллюстраций 33, таблиц — 11, использованных источников — 15.

**Abstract**

The graduation qualifying thesis focuses on the issue of phishing attacks and the need for an effective method of detection. The main emphasis is placed on the utilization of neural network technologies for automated identification of suspicious and potentially dangerous websites. The objective of this final qualifying work is to develop an automatic system capable of identifying suspicious and potentially harmful web pages. The relevance of this work is driven by the increasing number of phishing attacks in the digital environment, which pose a significant threat to user security. The thesis concludes with an economic justification of the proposed solution, an analysis of potential risks, and an ecological assessment of the project.

The volume of text material is 82 sheets (A4), the number of illustrations is 33, tables - 11, sources used - 15.

Содержание

[Введение 7](#_Toc150588016)

[1. Обзор проблемы фишинговых атак и методов борьбы с ними 8](#_Toc150588017)

[1.1 Проблематика фишинговых атак и её актуальность 8](#_Toc150588018)

[1.2 Анализ методов детектирования фишинговых сайтов 9](#_Toc150588019)

[1.2.1 Анализ URL-адреса 9](#_Toc150588020)

[1.2.2. Анализ содержания страницы 10](#_Toc150588021)

[1.3 Законодательное регулирование и стандарты в области защиты информации 11](#_Toc150588022)

[1.4 Методы фишинговых атак 12](#_Toc150588023)

[1.4.1 Социальная инженерия 13](#_Toc150588024)

[1.4.2 Смишинг 13](#_Toc150588025)

[1.4.3 Фишинг точек доступа 14](#_Toc150588026)

[1.4.4 Фишинговые наборы 15](#_Toc150588027)

[1.4.5 Drive-By-Download 16](#_Toc150588028)

[1.4.6 Spear-phishing 17](#_Toc150588029)

[1 Анализ и выбор методов детектирования фишинговых сайтов с использованием нейронных сетей 19](#_Toc150588030)

[2.1 Основы нейросетевых технологий 19](#_Toc150588031)

[2.2 Обзор существующих методы детектирования фишинговых сайтов с использованием ИИ 19](#_Toc150588032)

[2.3 Исследование методов детектирования фишинговых сайтов 19](#_Toc150588033)

[2.4 Определение параметров для анализа сайтов: URL, визуальной составляющей и текст 19](#_Toc150588034)

[3. Разработка и обучение нейросети для детектирования фишинговых сайтов 20](#_Toc150588035)

[3.1 Формирование и предобработка набора данных 20](#_Toc150588036)

[3.2 Архитектура нейронной сети и её обучение 20](#_Toc150588037)

[3.4 Оценка эффективности и точности детектирования фишинговых сайтов 20](#_Toc150588038)

[4. Экономическое обоснование 21](#_Toc150588039)

[4.1 Спецификация проекта 21](#_Toc150588040)

[4.2 План–график проектирования и разработки системы 21](#_Toc150588041)

[4.3 Расчет затрат на разработку проекта 21](#_Toc150588042)

[5. Безопасность и экологичность проекта 22](#_Toc150588043)

[5.1 Влияние шума на организм человека и защита от них. Расчет уровня шума на рабочем месте 22](#_Toc150588044)

[5.2 Экологичность работы 22](#_Toc150588045)

[5.3 Организация и обеспечение пожарной безопасности на предприятии 22](#_Toc150588046)

[5.4 Выводы 22](#_Toc150588047)

[Заключение 23](#_Toc150588048)

[Перечень использованных информационных ресурсов 24](#_Toc150588049)

**Введение**

(В проекте)

1. **Обзор проблемы фишинговых атак и методов борьбы с ними**
   1. **Проблематика фишинговых атак и её актуальность**

В современном цифровом мире проблема фишинговых атак становится все более актуальной и серьезной. Киберпреступность продолжает развиваться, и фишинговые атаки входят в число наиболее распространенных и опасных видов мошенничества в онлайн-среде.

Фишинговые атаки – это мошеннические действия, которые направлены на получение конфиденциальной информации, такой как логины, пароли, данные банковских карт, с помощью создания поддельных сайтов, электронных писем и сообщений, выдающихся за официальные.

Современный мир технологий и интернета предоставляет широкие возможности для общения, работы, обучения и отдыха. Однако, вместе с этим он также представляет серьезные угрозы для пользователей, такие как фишинговые атаки. Фишинговые атаки являются одной из наиболее распространенных угроз в сфере кибербезопасности. Они представляют собой попытки мошеннического получения конфиденциальной информации, такой как логины, пароли, номера кредитных карт и другие данные, путем подделки легитимных веб-сайтов или электронных сообщений. Фишинговые атаки могут привести к серьезным последствиям для пользователей, включая финансовые потери, утечку конфиденциальной информации и нарушение частной жизни.

Фишинговые атаки являются актуальной проблемой в мире. Согласно отчету компании «Positive Technologies» от 16 июня 2023, в первом квартале 2023 года количество событий увеличилось на 7% по сравнению с предыдущим периодом и превысило показатель начала 2022 года на 10%. Самыми распространенными последствиями успешных кибератак на компании стали утечки конфиденциальных данных (51%) и нарушения основной бизнес-деятельности (44%).

Фишинговые атаки имеют серьезные последствия как для отдельных пользователей, так и для организаций. Когда пользователь становится жертвой фишинга, его конфиденциальная информация попадает в руки злоумышленников. Это может привести к утрате доступа к банковским счетам, краже личных данных, а также использованию этой информации для совершения других видов мошенничества.

Организации, в свою очередь, могут столкнуться с финансовыми убытками, утратой доверия клиентов и повреждением репутации. Фишинговые атаки могут привести к утечке коммерческой информации, потере конкурентных преимуществ и ухудшению отношений с партнерами. Все это наносит серьезный ущерб бизнесу и экономике в целом.

* 1. **Анализ методов детектирования фишинговых сайтов**

Существует множество методов детектирования фишинговых сайтов, которые используются для борьбы с этой угрозой. Некоторые из них включают анализ содержимого веб-страницы, проверку URL-адреса, использование черных списков и т.д. Каждый метод имеет свои преимущества и недостатки, и выбор конкретного метода зависит от конкретных условий.

Анализ URL-адреса

Один из наиболее распространенных подходов к детектированию фишинговых сайтов основывается на анализе URL-адреса. Этот метод заключается в том, чтобы проверять доменное имя сайта и его поддомены на наличие признаков, таких как:

1. Орфографические ошибки
2. Использование цифр и символов вместо букв
3. Ограниченный срок регистрации домена

Если какой-либо из этих признаков обнаружен, сайт может быть отмечен как потенциальный фишинговый ресурс.

Анализ содержания страницы

Другой распространенный метод анализа фишинговых сайтов заключается в исследовании содержания страницы. Этот подход использует анализ содержимого страницы, чтобы проверить, отличается ли содержание на фишинговом сайте от того, что можно найти на официальном сайте. Этот метод может быть довольно эффективным, если рассматривать фишинговые сайты, которые имитируют определенных поставщиков услуг, таких как банки или платежные системы.

Визуальный метод

Визуальный метод детектирования фишинговых сайтов основан на анализе внешнего вида веб-страницы. Он сфокусирован на обнаружении признаков, которые могут указывать на то, что сайт является поддельным. Некоторые из таких признаков могут быть:

1. Дизайн и макет: Фишинговые сайты часто имеют недостаточно качественный дизайн и макет страницы по сравнению с официальными сайтами. Они могут выглядеть грубо или иметь некорректное расположение элементов.
2. Логотипы и изображения: Фишинговые сайты могут использовать измененные логотипы или изображения, которые могут отличаться от официальных. Также они могут содержать неправильные или нереалистичные изображения.
3. Системные баннеры: Фишинговые сайты могут содержать различные системные предупреждения или баннеры, которые создают ситуацию срочности, чтобы склонить пользователей к предоставлению своих личных данных.

Визуальный метод детектирования может быть полезным для определения фишинговых сайтов, особенно для тех пользователей, у которых не хватает технических знаний для проведения более сложного анализа.

**1.3 Законодательное регулирование и стандарты в защите инфорамции**

Законодательное регулирование и стандарты в области борьбы с фишингом в России направлены на решение проблемы кибермошенничества в цифровой среде страны. Фишинг представляет собой распространенную практику, при которой мошеннические сайты подражают легитимным для обмана пользователей и получения их конфиденциальной информации.

Российское законодательство содержит набор мер и стандартов для эффективной борьбы с фишинговыми атаками и связанными с ними преступлениями. Важным правовым актом является Постановление Пленума Верховного Суда Российской Федерации № 51 от 27 декабря 2007 года, которое определяет ответственность за фишинг. В соответствии с этим документом, незаконный доступ к компьютерной информации или создание и распространение вредоносных программ могут быть квалифицированы по статьям 159 «Мошенничество», 272 «Неправомерный доступ к компьютерной информации» или 273 «Создание, использование и распространение вредоносных компьютерных программ» Уголовного кодекса Российской Федерации.

Одним из распространенных методов фишинга является использование вредоносного программного обеспечения. Злоумышленники разрабатывают и распространяют специальные программы, которые автоматически перенаправляют пользователей на фишинговые сайты при выполнении определенных действий. Такие действия подпадают под статью 273 Уголовного кодекса.

Создание фишинговых сайтов также подпадает под уголовную ответственность по российскому законодательству. Незаконное использование товарных знаков при создании фишинговых сайтов может быть квалифицировано как нарушение статьи 180 Уголовного кодекса Российской Федерации, которая регулирует «Незаконное использование товарного знака». Злоумышленники злоупотребляют чужими товарными знаками и другими средствами идентификации для обмана жертв и осуществления фишинговых атак.

## 1.4 Методы фишинговых атак

Фишинг представляет собой механизм обмана, при котором злоумышленник пытается получить доступ к конфиденциальной информации, представляясь доверенным и надежным источником. Это может включать выдачу себя за банк, онлайн-сервис или другую организацию, с целью убедить жертву предоставить свои личные данные. Фишинг может быть основан как на технических, так и на социальных методах.

Технические методы фишинга включают создание поддельных веб-сайтов, которые могут выглядеть практически идентично оригиналу. Злоумышленники могут использовать поддельные электронные письма, сообщения в социальных сетях или рекламные баннеры, чтобы перенаправить пользователей на эти поддельные сайты. Цель состоит в том, чтобы заставить жертву ввести свои личные данные, такие как логин и пароль, которые затем могут быть использованы для несанкционированного доступа к аккаунту или кражи личной информации.

Социальные методы фишинга основаны на манипуляции психологическими уязвимостями жертвы. Злоумышленники могут использовать такие тактики, как создание срочности или страха, чтобы побудить жертву действовать быстро и без размышления. Это может включать предупреждения о безопасности, угрозы блокировки аккаунта или предложения о крупных выигрышах. Целью является вызвать у жертвы эмоциональные реакции, которые могут привести к необдуманному предоставлению личных данных.

Понимание технических и социальных методов фишинга является важным для защиты от таких атак. Это позволяет пользователям быть более бдительными и осторожными в отношении подозрительных запросов на предоставление личной информации. Кроме того, осведомленность об этих методах помогает разработчикам и специалистам по кибербезопасности создавать более эффективные меры защиты и системы обнаружения фишинга.

Социальная инженерия

Социальная инженерия представляет собой один из наиболее разрушительных и эффективных методов фишинговых атак, в котором фишеры используют психологические механизмы, чтобы манипулировать эмоциями и чувствами жертв. Они искусно воспроизводят чувства, такие как сострадание, тревога, желание помочь, и неосведомленность о том, как достичь своей цели, чтобы развести жертву на неразумные и рискованные действия.

Основная цель социальной инженерии заключается в отвлечении жертвы от логического и рационального мышления, подавляя ее способность принимать разумные решения. Злоумышленники активно используют эмоциональные состояния, такие как страх, зависть, интрига, ярость, дружба, верность, честолюбие, самоотверженность, чувство долга и превосходства. Проникая в эмоциональную сферу жертвы, они вынуждают ее раскрыть свои личные данные и конфиденциальную информацию.

Примером фишинговой атаки, основанной на социальной инженерии, является предоставление жертвам вредоносных ссылок на веб-сайты через электронную почту. Злоумышленники создают иллюзию легитимности и внушают доверие, чтобы убедить жертву вводить свои конфиденциальные данные на поддельных веб-страницах.

Важно быть бдительным и осознавать такие манипуляции, чтобы избежать попадания в ловушку социальной инженерии. Обучение и повышение осведомленности пользователей являются эффективными мерами для защиты от фишинговых атак, основанных на манипуляции эмоциями.

Смишинг

Смишинговые атаки являются формой мошенничества, где злоумышленники используют сервисы коротких сообщений (SMS) для доставки поддельных и мошеннических сообщений. Этот вид атаки становится все более распространенным, так как люди часто доверяют сообщениям, полученным 11 через мобильные приложения для обмена сообщениями на своих телефонах, больше, чем сообщениям, полученным по электронной почте.

Смишинговые атаки оказываются успешными, поскольку злоумышленникам легче найти номера телефонов потенциальных жертв, чем их адреса электронной почты. В отличие от электронной почты, где адреса могут быть произвольной комбинацией цифр, букв и символов, телефонные номера имеют ограниченное количество вариантов. Например, в США номера телефонов состоят из десяти цифр. Это означает, что злоумышленникам достаточно сгенерировать десять случайных цифр, чтобы достичь своей цели, в то время как связаться с человеком через адрес электронной почты может быть гораздо сложнее и требовать больше усилий

Эта уязвимость воспринимается злоумышленниками как привлекательная возможность для проведения мошеннических действий, так как многие люди не ожидают получить поддельные сообщения через SMS и более склонны доверять таким сообщениям, особенно если они выглядят легитимно. Поэтому осведомленность и бдительность пользователей являются важными факторами для предотвращения смишинговых атак.

### Фишинг точек доступа

Wi-Fi фишинг, также известный как "Evil Twin", это метод фишинга, который использует беспроводные сети. В этой атаке злоумышленник создает ложную точку доступа, которая выглядит так же, как легитимная точка доступа, и находится между клиентом и настоящей точкой доступа. Злоумышленник стремится обмануть пользователя, заставляя его подключиться к ложной точке доступа вместо настоящей. Часто злоумышленник копирует конфигурацию реальной точки доступа, чтобы создать идентичный идентификатор сети (SSID) и использовать более мощный сигнал передачи.

DE-аутентификация — это атака, при которой злоумышленник пытается прервать соединение между клиентом и точкой доступа, посылая специальные кадры DE-аутентификации. Это заставляет клиента повторно пройти процесс 12 аутентификации, и злоумышленник может прослушивать и анализировать трафик во время этого процесса. После чего атакующий может расшифровать секретный ключ и обойти шифрование безопасности. Второй этап атаки DEаутентификации заключается в том, чтобы заставить клиента подключиться к ложной точке доступа, чтобы злоумышленник мог прослушивать всю коммуникацию.

Карма-атака основана на активном сканировании беспроводной сети WLAN для сбора запросов от устройств пользователей и генерации поддельных ответов, чтобы устройства думали, что настоящая сеть WLAN находится поблизости. Когда устройства автоматически сканируют доступные сети, они отправляют запросы зонда для проверки наличия сети в зоне действия. Злоумышленник может использовать карма-атаку, чтобы привлечь целевое устройство к своей ложной точке доступа. Эта атака особенно опасна для клиентов, которые используют активное сканирование для аутентификации.

Фишинговые наборы

Фишинговые наборы представляют собой комплекты инструментов, созданные с целью облегчить злоумышленникам проведение фишинговых атак, даже в отсутствие необходимых программных навыков [10]. Эти наборы широко доступны как бесплатно, так и за плату, и предоставляют киберпреступникам возможность создавать и распространять вредоносные веб-сайты, электронные письма и скрипты с минимальными усилиями.

Однако использование бесплатных фишинговых наборов не рекомендуется из-за потенциальных угроз для конечных пользователей. Часто такие наборы включают в себя злоумышленный код, который может быть использован для кражи и передачи личных данных пользователей разработчикам наборов. Такие действия могут привести к серьезным последствиям для жертв, включая финансовые потери и нарушение конфиденциальности.

В свете этих рисков рекомендуется оставаться бдительными и применять меры безопасности при обнаружении подозрительных веб-сайтов, электронных 13 писем или запросов на предоставление личной информации. Это включает в себя проверку подлинности отправителя, осмотр URL-адресов и использование антивирусного программного обеспечения для защиты от вредоносных программ. Поддержание информационной грамотности и обучение о практиках безопасности в сети также являются важными мерами для защиты от фишинговых атак, независимо от того, используются ли фишинговые наборы или другие методы атаки.

Drive-By-Download

Техника Drive-By-Download представляет собой хитроумный метод, при котором злоумышленники эксплуатируют уязвимости веб-сайтов и браузеров, чтобы непреднамеренно загрузить и запустить вредоносные программы на уязвимые системы. Эта атака может произойти при посещении опасного веб-сайта или ответе на мошенническое электронное письмо.

Drive-By-Download может быть осуществлен различными способами. Например, злоумышленники могут внедрить злонамеренный JavaScript-код на сервер веб-сайта или использовать электронную почту для передачи вредоносных программ. При успешной эксплуатации уязвимости в браузере или на сервере, вредоносное ПО загружается и устанавливается на компьютер жертвы.

Затем загруженное вредоносное ПО может превратить компьютер в ботнет, то есть включить его в сеть зараженных устройств, которые злоумышленники могут использовать для проведения дальнейших атак. Это может привести к серьезным последствиям, таким как кража личных данных, финансовые мошенничества или даже нарушение конфиденциальности.

В свете этих угроз рекомендуется принимать меры безопасности при использовании интернета. Это включает в себя регулярное обновление программного обеспечения, включая операционную систему, браузер и антивирусные программы, чтобы устранить известные уязвимости. Кроме того, следует избегать посещения подозрительных или непроверенных веб-сайтов, а 14 также быть осторожными при открытии вложений в электронных письмах, особенно если они приходят от неизвестных отправителей.

Spear-phishing

Spear-phishing - это изощренный вид атаки, при котором злоумышленники создают и распространяют поддельные электронные письма, содержащие вредоносные программы или ссылки на вредоносные веб-сайты. Эта хитрая техника основывается на использовании социальной инженерии и поддельных источников, чтобы убедить жертву в легитимности полученного письма.

В процессе spear-phishing атаки, злоумышленники тщательно исследуют своих потенциальных жертв, собирают информацию о них и создают электронные письма, максимально подобные легитимным сообщениям, чтобы вызвать доверие и убедить получателя открыть вложение или перейти по ссылке.

Вложения или ссылки, предоставленные в этих электронных письмах, обычно содержат скрытые вредоносные программы, такие как троянские кони или шпионское ПО, которые могут быть активированы при неправильном взаимодействии с ними. В некоторых случаях, ссылки могут вести на вредоносные веб-сайты, которые маскируются под легитимные источники, чтобы собрать личные данные жертвы или провести фишинговые атаки.

Spear-phishing атаки являются особенно опасными, поскольку они маскируются под легитимные коммуникации и представляют собой персонифицированный подход к атаке, что делает их более убедительными и успешными. Часто такие атаки направлены на организации или отдельных сотрудников с целью получения конфиденциальной информации или доступа к защищенным системам.

Для защиты от spear-phishing атак рекомендуется быть внимательными при открытии электронных писем, особенно от неизвестных отправителей. При получении подозрительного письма необходимо избегать открытия вложений или перехода по ссылкам без проверки их подлинности. Важно также обучать 15 сотрудников организаций узнавать признаки поддельных электронных писем и предоставлять им средства для проверки подлинности сообщений.

1. **Анализ и выбор методов детектирования фишинговых сайтов с использованием нейронных сетей**

**2.1 Основы нейросетевых технологий**

(В проекте)

**2.2 Обзор существующих методов детектирования фишинговых сайтов с использованием ИИ**

(В проекте)

**2.3 Выбор и обоснование методов детектирования фишинговых сайтов**

(В проекте)

**2.4 Определение параметров для анализа сайтов: URL, визуальной составляющей и текст**

(В проекте)

**3.** **Разработка и обучение нейросети для детектирования фишинговых сайтов**

**3.1** **Формирование и предобработка набора данных**

(В проекте)

**3.2** **Архитектура нейронной сети и её обучение**

(В проекте)

**3.3** **Тестирование и анализ результатов работы нейросети**

(В проекте)

**3.4** **Оценка эффективности и точности детектирования фишинговых сайтов**

(В проекте)

**4. Экономическое обоснование**

Для обоснования экономической эффективности разработанной системы детектирования фишинговых сайтов с помощью нейросетевых технологий был составлен план-график разработки и внедрения, определены затраты на разработку и внедрение, включая оплату труда, материалы, машинное время и общехозяйственные расходы. Оценка экономических показателей включает учет снижения потерь от фишинговых атак, риск утечки данных, повышение доверия клиентов и привлечение новых клиентов. Анализ конкурентоспособности и оценка рисков помогут определить преимущества системы и разработать стратегии смягчения рисков, а также прогнозирование доходов и окупаемости инвестиций позволит оценить финансовые перспективы проекта.

**4.1 Спецификация проекта**

Техническое описание проекта является составной частью проектной документации, содержащей информацию о материалах, изделиях и оборудовании. Эта информация необходима для определения общих потребностей и комплектации материальными ресурсами для строительного объекта. Техническое описание имеет следующие цели:

— Определение полного списка требуемого оборудования;

— Расчет количества материальных ресурсов.

На основе данных ведомости можно определить потребность в материалах, рассчитать их стоимость и составить график приобретения для обеспечения непрерывности процесса разработки системы. Техническое описание системы оценки защищенности беспроводных устройств представлено в таблице 4.1.

Таблица 4.1 — Спецификация системы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Материалы | Единица измерения | Требуемое количество | Цена за единицу руб. | Сумма, руб. |
| Сервер Dell PowerEdge R740 | шт. | 1 | 250000 | 250000 |
| Маршрутизатор Cisco ISR 4321 | шт. | 1 | 70000 | 70000 |
| Жесткий диск Seagate IronWolf NAS HDD (4 ТБ) | шт. | 1 | 15000 | 15000 |
| Антивирусная программа Kaspersky Endpoint Security | шт. | 1 | 10000 | 10000 |
| Итого |  | | | 345 000 |

**4.2 План–график проектирования и разработки системы**

Выбор комплекса работ по разработке проекта производится в соответствии со стандартом «ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств», устанавливающим стадии разработки программных продуктов, приведен в таблице 4.2.

Таблица 4.2 — Комплекс работ по разработке системы анализа радиоэфира

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Содержание работ | Исполнители | Длитель-ность в календар-ных днях | | Загрузка | | |
| в днях | в % | |
| 1 Разработка технического задания | | | | | | |
| 1.1 Исследование и обоснование разработки | | | | | | |
| 1.1.1 Постановка задачи | Руководитель | 3 | | 3 | 100 | |
| Программист | 3 | 100 | |
| 1.1.2 Сбор исходных данных | Руководитель | 5 | | 3 | 60 | |
| Программист | 5 | 100 | |
| 1.2 Поиск аналогов и прототипов | | | | | | |
| 1.2.1 Анализ существующих методов | Руководитель | 7 | | 7 | 100 | |
| Программист | 7 | 100 | |
| 1.2.2 Обоснование необходимости разработки и внедрения | Руководитель | 5 | | 5 | 100 | |
| Программист | 0 | 0 | |
| 1.3 Анализ требований | | | | | | |
| 1.3.1 Определение и анализ требований к разрабатываемой системе | Руководитель | | 4 | 2 | | 50 |
| Программист | | 4 | | 100 |
| 1.3.2 Определение структуры входных и выходных данных | Руководитель | | 5 | 2 | | 40 |
| Программист | | 5 | | 100 |
| 1.3.3 Согласование и утверждение технического задания | Руководитель | | 4 | 4 | | 100 |
| Программист | | 4 | | 100 |
| Итого по этапу 1 | Руководитель | | 33 | 26 | | 80 |
| Программист | | 28 | | 85 |
| 2 Проектирование | | | | | | |
| 2.1 Проектирование архитектуры системы | Руководитель | | 14 | 14 | | 100 |
| Программист | | 0 | | 0 |
| 2.2 Выбор аппаратных средств цифровой радиосвязи | Руководитель | | 14 | 7 | | 50 |
| Программист | | 14 | | 100 |
| 2.3 Сборка макета системы на основе аппаратных модулей для тестирования и отладки | Руководитель | | 14 | 2 | | 14 |
| Программист | | 14 | | 100 |
| Итого по этапу 2 | Руководитель | | 42 | 23 | | 53 |
| Программист | | 28 | | 67 |
| 3 Разработка и тестирование модулей системы | | | | | | |
| 3.1 Разработка программных модулей системы | Руководитель | | 18 | 9 | | 50 |
| Программист | | 18 | | 100 |
| 3.2 Тестирование программной части | Руководитель | | 7 | 0 | | 0 |
| Программист | | 7 | | 100 |
| 3.3 Сборка и испытание системы | Руководитель | | 14 | 4 | | 29 |
| Программист | | 14 | | 100 |
| 3.4 Анализ результатов экспериментов, формулирование выводов | Руководитель | | 7 | 3 | | 36 |
| Программист | | 7 | | 100 |
| Итого по этапу 3 | Руководитель | | 46 | 16 | | 34 |
| Программист | | 46 | | 100 |
| 4 Оформление рабочей документации | | | | | | |
| 4.1 Проведение расчетов показателей безопасности жизнедеятельности | Руководитель | | 3 | 0 | | 0 |
| Программист | | 3 | | 100 |
| 4.2 Проведение экономических расчетов | Руководитель | | 7 | 0 | | 0 |
| Программист | | 7 | | 100 |
| 4.3 Оформление пояснительной записки | Руководитель | | 31 |  | | 0 |
| Программист | | 21 | | 100 |
| Итого по 4 этапу | Руководитель | | 41 | 0 | | 0 |
| Программист | | 31 | | 100 |
| Итого по проекту | Руководитель | | 162 | 65 | | 40 |
| Программист | | 133 | | 82 |

На основании вышеописанных таблиц, был составлен план–график по проектированию и реализации системы детектирования фишинговых сайтов, показывающий последовательность и взаимосвязь выполнения комплекса работ.

Таблица 4.3 — Календарный график выполнения работ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Содержание работ | Исполнители | Длитель-ность в днях | График работ | |
| начало 1 сентября | окончание 31 января |
| Постановка задачи | Руководитель | 3 | 1 авг | 3 авг |
| Программист | 3 | 1 авг | 3 авг |
| Сбор исходных данных | Руководитель | 3 | 3 авг | 5 авг |
| Программист | 5 | 3 авг | 8 авг |
| Анализ существующих методов | Руководитель | 7 | 8 авг | 15 авг |
| Программист | 7 | 8 авг | 15 авг |
| Обоснование необходимости разработки и внедрения | Руководитель | 5 | 15 авг | 20 авг |
| Программист | 0 | 15 авг | 15 авг |
| Определение и анализ требований к системе | Руководитель | 2 | 20 авг | 22 авг |
| Программист | 4 | 20 авг | 24 авг |
| Определение структуры входных и выходных данных | Руководитель | 2 | 24 авг | 26 авг |
| Программист | 5 | 24 авг | 29 авг |
| Согласование и утверждение технического задания | Руководитель | 4 | 29 авг | 2 сен |
| Программист | 4 | 29 авг | 2 сен |
| Проектирование архитектуры системы | Руководитель | 14 | 2 сен | 16 сен |
| Программист | 0 | 2 сен | 2 сен |
| Выбор аппаратных средств для реализации системы | Руководитель | 7 | 16 сен | 22 сен |
| Программист | 14 | 16 сен | 30 сен |
| Сборка макета системы | Руководитель | 2 | 30 сен | 1 окт |
| Программист | 14 | 30 сен | 13 окт |
| Разработка программных модулей системы | Руководитель | 9 | 13 окт | 22 окт |
| Программист | 18 | 13 окт | 31 окт |
| Тестирование программной части | Руководитель | 0 | 31 окт | 31 окт |
| Программист | 7 | 31 окт | 7 ноя |
| Сборка и испытание системы | Руководитель | 4 | 7 ноя | 11 ноя |
| Программист | 14 | 7 ноя | 21 ноя |
| Анализ результатов экспериментов, формулирование выводов | Руководитель | 3 | 21 ноя | 23 ноя |
| Программист | 7 | 21 ноя | 28 ноя |
| Проведение расчетов показателей безопасности жизнедеятельности | Руководитель |  | 28 ноя | 28 ноя |
| Программист | 3 | 28 ноя | 31 ноя |
| Проведение экономических расчетов | Руководитель |  | 31 ноя | 31 ноя |
| Программист | 7 | 31 ноя | 7 дек |
| Оформление пояснительной записки | Руководитель |  | 7 дек | 7 дек |
| Программист | 31 | 7 дек | 10 янв |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **янв** | **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **декабрь** | **31** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **ноябрь** | **31** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Рисунок 4.1 — План-график разработки проекта |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **октябрь** | **30** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **сентябрь** | **31** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **август** | **30** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Содержание работы** | | Постановка задачи | Сбор исходных данных | Анализ существующих методов | Обоснование необходимости разработки и внедрения | Определение и анализ требований к разрабатываемой системе | Определение структуры входных и выходных данных | Согласование и утверждение технического задания | Проектирование архитектуры системы | Выбор аппаратных средств цифровой радиосвязи | Сборка макета системы | Разработка программных модулей системы | Тестирование программной части | Сборка и испытание системы | Анализ результатов экспериментов, формулирование выводов | Проведение расчетов показателей безопасности жизнедеятельности | Проведение экономических расчетов | Оформление пояснительной записки |

**4.3 Расчет затрат на разработку проекта**

Предпроизводственные затраты представляют собой единовременные расходы на разработку обеспечивающих или функциональных систем и элементов на всех этапах проектирования, а также затраты на обработку материалов исследования, разработку технического задания, проверки. Сюда включаются затраты на разработку алгоритмов и программ, разработку технического и рабочего проекта системы и её опытной проверки.

Основная заработная плата разработчиков определяется по формуле:

,

где *O* — должностной оклад, руб;

— число рабочих дней в году;

— затраты времени на разработку, рабочие дни.

Число рабочих дней на разработку определяется по формуле:

,

где — календарные дни;

— коэффициент перевода календарных дней в рабочие;

Данный коэффициент равен отношению рабочих дней в году к общему числу календарных дней.

Согласно данным из таблицы 4.1, рассчитаем трудозатраты руководителя:

Рассчитаем трудозатраты программиста:

.

В компании оклад руководителя равен 100 000 руб., а оклад программиста 80 000 руб.

Рассчитаем заработную плату программиста и руководителя по формуле:

Отсюда следует, что основная заработная плата на разработку:

Рассчитаем дополнительную зарплату:

где — коэффициент начисления на дополнительную зарплату.

Премия рассчитывается согласно следующей формуле:

где — коэффициент начисления на премию.

Рассчитаем начисления на единый страховой сбор:

Ввиду того, что проектируемая система должна быть разработана и отлажена с помощью компьютеров, к суммарным затратам на разработку добавляются затраты на их использование.

Доля амортизационных отчислений на компьютерное оборудование, приходящаяся на разработку проекта, определяется по формуле:

где — балансовая стоимость компьютерного оборудования;

— продолжительность использования компьютера программистом, час;

— срок службы компьютерного оборудования. = 6 лет;

число одновременно выполняемых проектов (*z* = 1…3).

 — действительный годовой фонд времени компьютерного оборудования;

Действительный годовой фонд компьютерного оборудования рассчитывается по формуле:

где — номинальный фонд времени работы компьютерного оборудования;

— коэффициент потерь времени; *y* = 3 – 5 %.

Рассчитаем амортизационные отчисления для компьютерного оборудования:

Используемое при конструкторской подготовке системы анализа радиоэфира относится к нематериальным активам предприятия. Амортизационные отчисления на программное обеспечение, приходящиеся на конструкторскую подготовку производства, определяются по формуле:

Где — балансовая стоимость программного обеспечения, руб.;

— срок службы программного обеспечения (при отсутствии фактических данных применяется равным 10 годам).

Рассчитаем затраты электроэнергии, необходимые на проектирование и разработку системы.

где — установленная мощность компьютера, кВт;

— коэффициент загрузки установленной мощности.

— цена электроэнергии, руб/кВт.

Итого затраты на энергию будут следующими:

руб.

Итого затраты на машинное время:

Общехозяйственные расходы:

В таблице 4.4 представлены затраты на разработку и материалы в соответствии со спецификацией, приведённой в п. 5.1.

Таблица 4.4 — Затраты на разработку

|  |  |
| --- | --- |
| Статьи затрат | Затраты |
| Основная заработная плата | 631 578,94 |
| Дополнительная зарплата | 94 736,84 |
| Премия | 252 631,57 |
| Отчисления на социальные нужды | 293 684,20 |
| Затраты на материалы | 345 000 |
| Затраты на машинное время | 30 019,86 |
| Общехозяйственные расходы | 1 705 263,13 |
| ИТОГО | 3 007 914,54 |

В результате проведенных расчетов определено, что себестоимость разработки составляет 3 007 914,54 руб. С учетом нормативной рентабельности R = 15% планируемая прибыль П составит:

*П* = *С* · *R* = 3 007 914,54 · 15% = 451 187,18 руб.

A цена продукта составит:

*Ц* = *С* + *П* = 3 007 914,54 + 451 187,18 = 3 498 559,84 руб.

Цена продукта с учётом НДС составит:

*ЦНДС* = 1,2·*Ц* = 1,2 · 3 498 559,84 = 4 198 271,80 руб.

Потенциальными покупателями разработанной системы являются компании, занимающиеся производством антивирусных программных продуктов.

**5. Безопасность и экологичность проекта**

**5.1 Влияние шума на организм человека и защита от них. Расчет уровня шума на рабочем месте**

(В проекте)

**5.2 Экологичность работы**

(В проекте)

**5.3 Организация и обеспечение пожарной безопасности на предприятии**

(В проекте)

**5.4 Выводы**

(В проекте)

**Заключение**

(В проекте)

**Перечень использованных информационных ресурсов**

1. <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q1/>
2. <https://blog.pravo.ru/blog/5805.html>

Приложение A