Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.056:004.773.3

Бычек
Маргарита Николаевна

Система фильтрации фишинговых писем для корпоративной почты

АВТОРЕФЕРАТ
диссертации на соискание степени магистра

по специальности 1-98 80 01 – Информационная безопасность

Научный руководитель
Борботько Т. В.
д.т.н., профессор

Минск 2023

Работа выполнена на кафедре защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель:	**Борботько Тимофей Валентинович,** доктор технических наук, профессор, заведующий кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
Рецензент:	**Уткина Елена Апполинарьевна,** кандидат технических наук, доцент кафедры микро- и наноэлектроники учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Защита диссертации состоится «02» мая 2023 г. года в 10^{00} часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П. Бровки, 10, корп. 3, ауд. 111-3, тел. 293-85-91, e-mail: inform@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

КРАТКОЕ ВВЕДЕНИЕ

Подавляющее большинство работы в самых разных отраслях в настоящее время выполняется отдельными лицами или корпорациями, использующими Интернет для выполнения своих задач. Постоянно увеличивается доля электронного документооборота с использованием электронной почты в организациях. Однако, электронная почта является достаточно уязвимым средством общения, так как существует тенденция постоянного увеличения числа хакерских атак на организации с использованием фишинга электронной почты. Одной из проблем, с которой сталкиваются пользователи электронной почты, являются фишинговые сообщения, содержащие вредоносные вложения или ссылки, ведущие на опасные веб-сайты. В результате, фишинг позволяет злоумышленникам нанести ущерб организации с минимальными техническими затратами.

Следовательно, предприятия нуждаются в системах, позволяющих снизить урон от фишинговых атак. Существующие системы защиты корпоративной электронной почты делятся на два вида: технические средства, направленные на предотвращение доставки пользователю писем с признаками фишинга, как правило, располагающиеся на межсетевых экранах организации, или средства, направленные на повышение осведомленности пользователей о фишинге. Однако только технические средства защиты не дают максимальной гарантии, так как выявлено, что после начала атаки проходит минимум 7 часов, прежде чем её замечают технические средства защиты.

Таким образом, наилучшим решением является система, сочетающая в себе как технические, так и организационные меры. Такая система способна не только определить фишинговое письмо, но и предоставить пользователю визуализированные результаты анализа с указанием признаков фишинга в письме, как в заголовке, так и в теле письма, что позволит в дальнейшем повысить уровень осведомленности пользователя о фишинге.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научной, научно-технической и инновационной деятельности

Тема диссертационной работы соответствует разделу 6 «Обеспечение безопасности человека, общества и государства» приоритетных направлений научной, научно-технической и инновационной деятельности в Республики Беларусь на 2021–2025 гг., утверждённых Указом Президента Республики Беларусь 7 мая 2020 г., № 156. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке системы фильтрации фишинговых писем для корпоративной почты.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Проанализировать структуру сообщения, передаваемого по электронной почте, его заголовок, тело и вложения для выявления признаков фишинга в каждой из частей электронного письма;
2. Исследовать существующие методы обнаружения фишинговых писем, как в ручном режиме, так и с применением средств автоматизации;
3. Разработать архитектуру и алгоритмы работы системы фильтрации фишинговых писем для корпоративной почты, а также систему организационно-технических мер, направленных на обучение пользователей информационных систем.

Объектом исследования являются сообщения, передаваемые по электронной почте.

Предметом исследования являются инструментальные средства создания расширений для почтового клиента Microsoft Outlook с возможностью анализа входящих писем, манипулирования ими и предоставления визуализации результатов анализа.

Основной гипотезой, положенной в основу диссертационной работы, является повышение уровня безопасности организации за счет разработки системы, способной определить признаки фишинга в письме, переместить письмо в нежелательную почту и вывести обнаруженные признаки пользователю. Визуализация позволит повысить уровень внимательности пользователя к входящим сообщениям.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XX Белорусско-российской научно-технической конференции (Минск, 2022) и 58-й научной конференции аспирантов, магистрантов и студентов БГУИР (Минск, 2022).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 2 работы, в том числе 2 статьи в сборниках материалов конференций.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, трех глав, заключения и списка использованных источников. В первой главе представлен анализ предметной области, разобрана структура сообщения, передаваемого по электронной почте, в каждой структурной части письма выявлены признаки, доступные для анализа при определении фишинга. Вторая глава посвящена краткому обзору существующих методов фильтрации фишинговых писем. В рамках третьей главы разработана архитектура системы фильтрации, алгоритмы ее работы и интерфейс

Общий объем работы составляет 69 страниц, из которых основного текста – 46 страниц, 34 рисунка на 19 страницах, 1 таблиц на 1 странице и список использованных источников из 37 наименований на 3 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе представлен анализ предметной области, проанализирована структура сообщений, передаваемых по электронной почте. Выявлены структурные части письма.

1. Конверт (envelope), содержащий адреса отправителя и получателей сообщения, эта информация используется только при пересылке сообщения по протоколу SMTP, получателю она недоступна.

2. Заголовок (header), содержащий служебную информацию, формируемую программами, участвующими в передаче сообщения. Это адреса отправителя и получателей, которые могут отличаться от используемых в конверте, тема сообщения, время отправки, сведения о пересылке, информация об использованных для создания сообщения программах и т.д. Заголовок завершается пустой строкой.

3. Тело (body), содержащее само сообщение, созданное отправителем и подлежащее доставке получателю. Сообщение может быть в виде текста или в HTML формате, содержать изображения. Также тело письма включает в себя вложения.

Для анализа доступны две части письма: заголовок и тело. На рисунке 1 представлена структура сообщения, передаваемого по электронной почте.

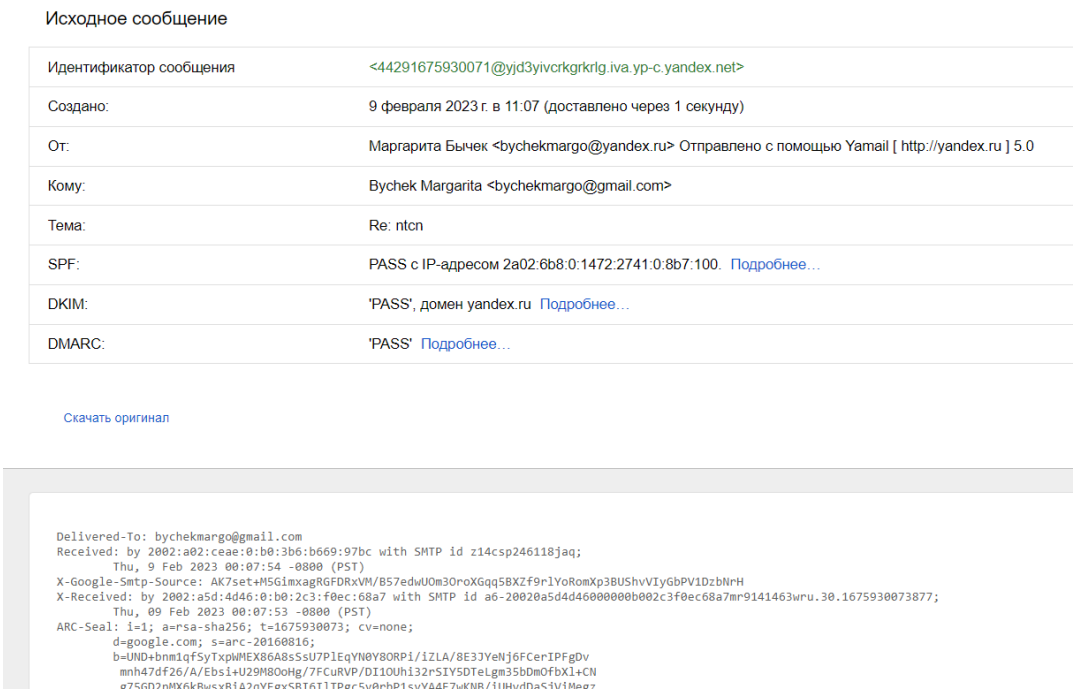

Рисунок 1 – Структура сообщения, передаваемого по электронной почте.

При анализе заголовков можно выявить некоторые признаки фишинга:

1. Сходство имени отправителя и его почты. Чаще всего обычные пользователи при регистрации нового почтового ящика придумывают логин максимально близкий к своим имени или фамилии, в то время как фишеры часто используют простые цифробуквенные сочетания без какого-либо сходства с именами.

2. В заголовках отображаются результаты аутентификации отправителя по следующим протоколам проверки подлинности электронной почты:

– Sender Policy Framework (SPF) позволяет принимающему почтовому серверу проверять во время доставки почты, что почта, якобы отправленная из определенного домена, отправлена с IP-адреса, авторизованного администратором этого домена.

– Domain Keys Identified Mail (DKIM) – метод аутентификации электронной почты, который позволяет получателю проверить, действительно ли электронное письмо было отправлено и авторизовано владельцем этого домена. Это делается путем добавления к электронному письму цифровой подписи

– Domain-based Message Authentication, Reporting and Conformance (DMARC) — это протокол, который использует SPF и DKIM для определения подлинности сообщения электронной почты.

Тело письма при анализе можно условно разделить на анализ текста и анализ вложений.

При обработке текста проверяются следующие признаки:

1. Наличие неперсонифицированного обращения, свидетельствующего об отсутствии ранее существующей переписки.

2. Грамматическая и орфографическая корректность письма. Большинство электронных писем, приходящих из ненадежных источников, написаны непрофессионалами. Это означает, что на их серверах нет функций проверки орфографии, а также отсутствует надлежащий процесс корректуры или редактирования. В отличие от них, профессиональные компании тщательно следят за орфографией в своих исходящих сообщениях электронной почты. Кроме того, они нанимают профессиональных копирайтеров для составления своих маркетинговых сообщений по электронной почте.

3. Использование приемов социальной инженерии. Как правило, фишеры в своих письмах влияют на одну из эмоций жертвы, побуждая ее к немедленному действию. Основными векторами психологических атак являются такие чувства, как страх, невнимательность, раздражение, любопытство, жадность и желание помочь. Также используются усилители реакции: чувство срочности и использование авторитета. Атаки направлены на отключение критического мышления жертвы и выполнения действий, необходимых злоумышленнику.

4. Наличие в письме гиперссылок и наличие в тексте акцента на ссылках, по которым должна перейти жертва. Эти ссылки ведут на поддельные сайты с похожим на реальный доменом, и именно там пользователь вводит персональные/платежные данные, которые достаются мошенникам.

Наличие вложений в письме само по себе является опасным признаком. Вложения могут быть любого формата. Наиболее опасными являются файлы с такими расширениями, как *.bat, *.exe, *.zip, наиболее распространенными – *.xls, *.docx, *.pdf. Также в настоящее время существуют программы, позволяющие визуально изменить расширение файла. При фишинге вложения чаще всего могут запускать кейлоггер, который крадет личную информацию, такую как имена пользователей и пароли.

Во второй главе приведен обзор существующих методов противодействия фишинговым атакам. Выделяют два разных вида методов противодействия фишинговым мероприятиям: традиционные и нетрадиционные. Традиционные методы в первую очередь включают обучение и повышение осведомленности пользователей о фишинге, фильтрация писем по черному или белому спискам, исследование контента на визуальное сходство и метод поисковых систем. В то время как нетрадиционные методы в основном включают: различные подходы машинного обучения, глубокое обучение, гибридное обучение, и другие методы искусственного интеллекта. Схема методов противодействия фишингу изображена на рисунке 2.

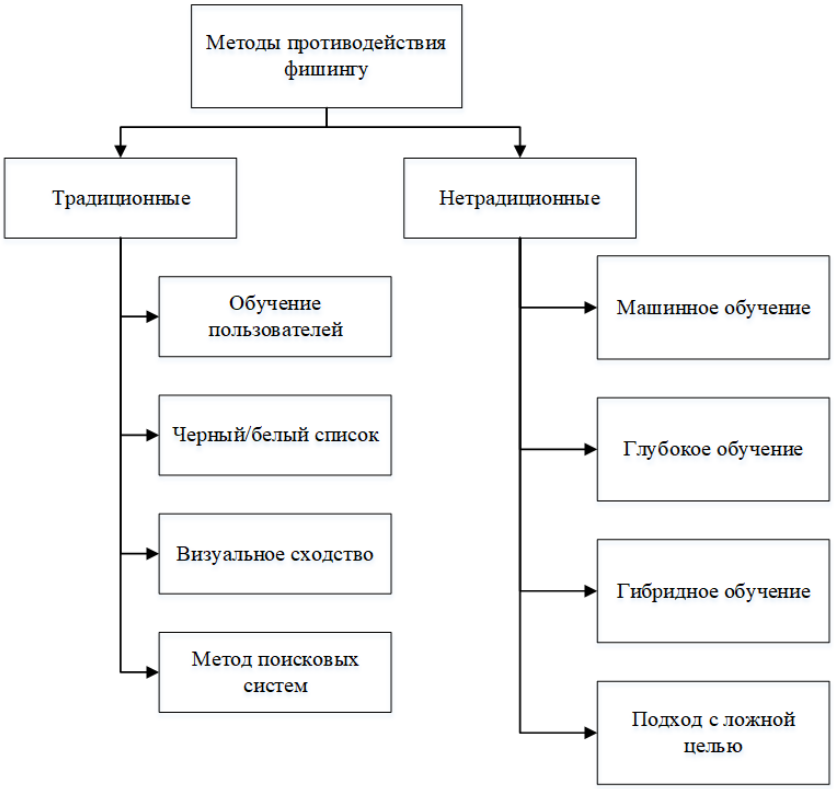

Рисунок 2 – Методы противодействия фишингу

При обучении пользователей распознавание фишинговых писем происходит в ручном режиме. Оно полностью зависит от уровня осведомленности и бдительности пользователя. Существуют курсы по безопасности работы с почтой и обучающие программы, тренирующие пользователей отличать фишинговые письма и замечать любые признаки фишинга, описанные в первой главе.

Для облегчения выявления фишинговых писем, увеличения вероятности их быстрой и точной и снижения рисков утечки данных во всем мире разрабатываются различные средства автоматизации. Обнаружение фишинга на основе технологий предлагает следующие преимущества по сравнению с образовательными или юридическими решениями:

– уменьшение времени реакции на атаку;

– способность обнаружить атаки нулевого дня;

– возможность предотвращения человеческих ошибок.

Одним из базовых технических решений являются решения, основанные на решениях пользователей. Пользователям показываются различные подсказки, и на их основе он сам решает, доверять сайту, письму или нет. Такой подход хорош для пользователей, кто уже разбирается в фишинге.

Одной из самых популярных стратегий для немедленного выявления фишингового или законного веб-сайта является подход на основе списков. Подход на основе черного списка заключается в ведении списка недоверенных URL-адресов. Попытка перехода по такому адресу блокируется. Ведение

белого списка, напротив, заключается в составлении списка доверенных адресов, и разрешается переход только по URL из этого списка.

Способы, основанные на визуальном сходстве, заключаются в анализе шрифтов, изображений и структуре DOM сайтов, благодаря чему возможна блокировка перехода пользователя по ссылке на фишинговый сайт.

Метод поисковых систем включает проверку рейтинга веб-сайтов в поисковых системах. Популярность фишинговых веб-сайтов ограничена, поскольку они существуют всего несколько дней и не появляются в верхней части результатов поиска.

Все большую популярность приобретают методы машинного обучения. При обнаружении фишинга широко используются два типа алгоритмов машинного обучения: классификация и кластеризация. Для обнаружения фишинга в различных случаях используются функции URL, элементы контента веб-сайта или функции канала связи. Фишинговые электронные письма классифицируются на основе таких характеристик, как ключевые слова, вложения и домен отправителя.

Использование глубокого обучения для обнаружения фишинга в последние годы становится все более популярным из-за его превосходной производительности и способности преодолевать ограничения подходов машинного обучения. Глубокое обучение пытается эмулировать человеческий мозг, используя несколько источников данных с разным весом и предвзятостью. В результате элементы внутри данных могут быть надежно идентифицированы, классифицированы и описаны путем объединения этих частей. Как правило, он использует иерархические нейронные сети для анализа данных.

В гибридном подходе методы комбинируются таким образом, что уравновешиваются их сильные и слабые стороны. Например, существует объединение сверточных нейронных сетей и алгоритмов долгой краткосрочной памяти с использованием изображений, кадров и текстовых данных для создания гибридной техники.

Подход с ложной целью — это стратегия, в которой используются ненастоящие цели захватчика. Использование приманок для сбора фишинговых электронных писем широко применяется поставщиками услуг безопасности и финансовыми учреждениями, чтобы можно было быстрее обнаруживать новые фишинговые сайты и немедленно их закрывать.

В третьей главе выполнена разработка системы фильтрации электронной почты. Первоначально детально изучен процесс фильтрации почты и определения письма как фишингового или легального. Для этого разработана модель по методологии IDEF0. Проведена декомпозиция каждого этапа и выявлены необходимые шаги.

Архитектура системы представляет собой классическое клиент-серверное приложение, однако в качестве клиента выступает почтовый клиент Microsoft Outlook. Почтовый клиент может быть как десктопным приложением, автоматически устанавливаемым в пакете программ Office, так

и открываться в браузерной версии в любом из интернет- браузеров. Система фильтрации представляет собой расширение для Outlook, запускаемое во время его работы. Для корректной работы системы необходимо развертывать файлы веб-страниц на веб-сервере или в службе веб-хостинга с настроенным HTTPS. Взаимодействие системы фильтрации и MS Outlook представлено на рисунке 3.

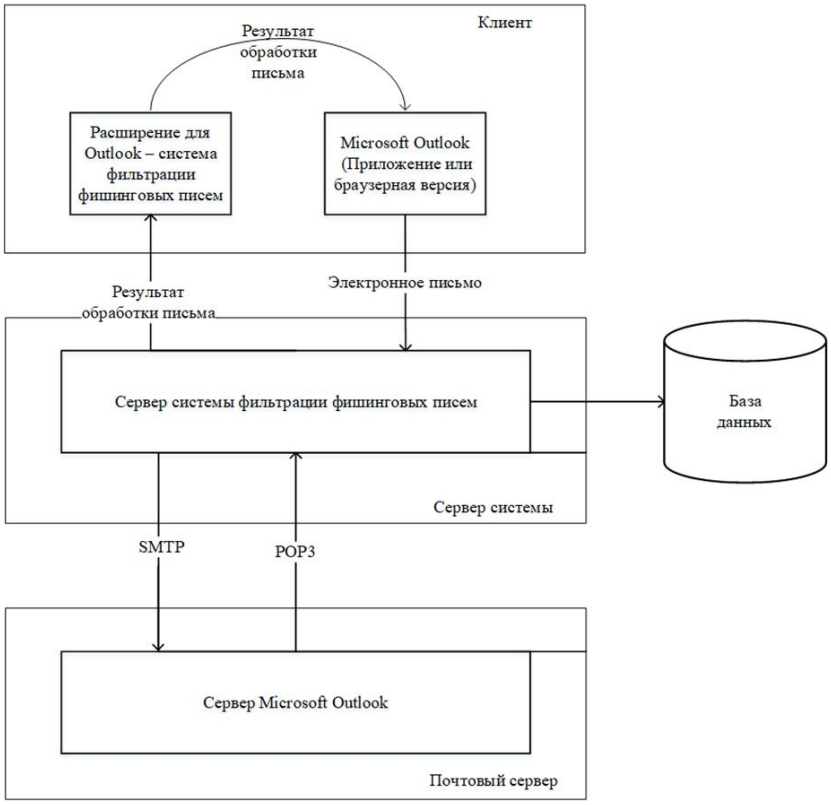

Рисунок 3 – Взаимодействие системы фильтрации и MS Outlook

Входящее письмо анализируется системой, и, если оно определено как фишинговое, может быть помещено в специальную папку «Фишинг».

Во входящем письме анализу подвергаются заголовок письма, его текст, присутствующие ссылки и вложения.

Заголовок анализируется на схожесть имени отправителя и его почтового адреса, а также на прохождение протоколов SPF, DKIM, DMARC.

Анализ тела письма включает два процесса: анализ текста на наличие лексики, характерной для фишинговых писем и анализ ссылок на какие-либо признаки, характерные для схем хакеров.

В частности, ссылки проверяются по множеству признаков, среди которых:

– наличие в ссылке IP-адреса;

– использование в ссылке символа @;

– использование шестнадцатеричных кодов символов;

– наличие перенаправления в ссылке;

– переопределение портов.

Последним при анализе письма происходит проверка вложений в письме. Наличие любого вложения является потенциально опасным, но вложения с расширениями .mp3, .txt, .bmp, .jpg, .png считаются менее опасными, так как не было известно достаточно случаев заражения файлов данного типа.

По результатам выполнения описанных процессов система получает ряд значений, которые впоследствии обрабатывает и выдает суммарный результат об общем уровне безопасности письма. Если письмо получено во время работы сервера системы, то при уровне безопасности входящего письма менее 50 % оно автоматически помещается в папку «Фишинг». Результаты оценки письма программой в десктопном приложении Outlook представлены на рисунке 4.

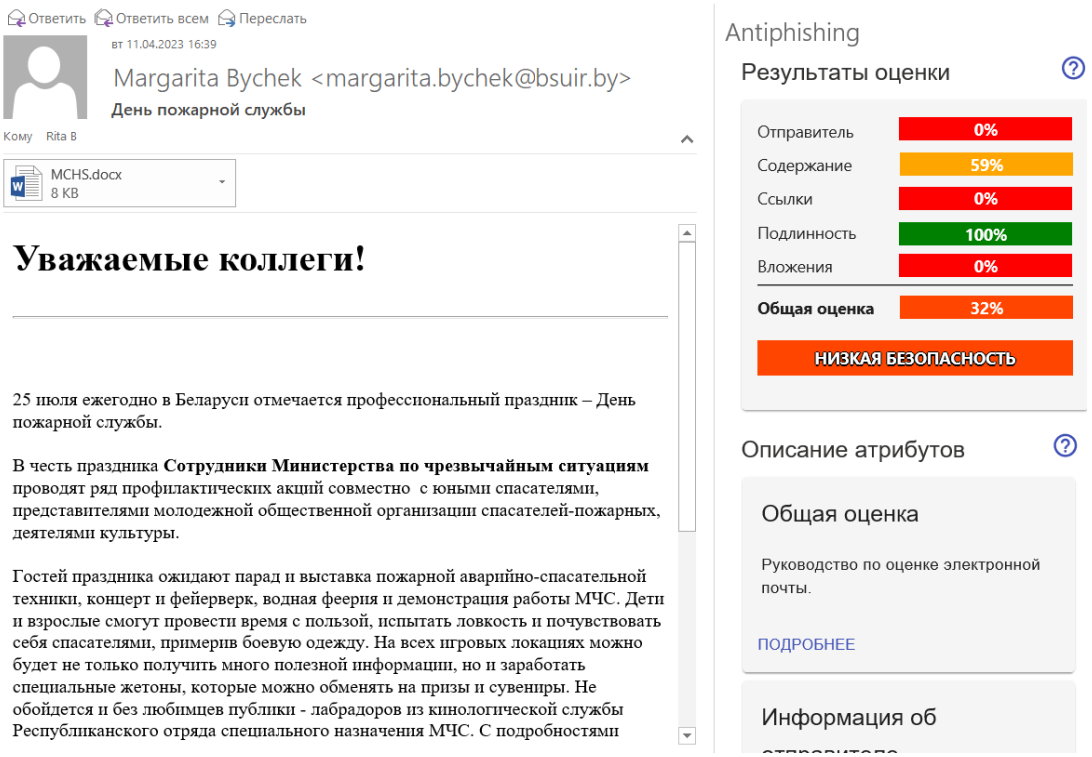

Рисунок 4 – Результаты оценки письма программой

Выполнена проверка работоспособности разработанной системы. Для этого проведена тестовая фишинговая кампания с помощью ресурса GoPhish. На несколько адресов электронной почты было направлено 50 фишинговых писем. Затем разработанная система проанализировала каждое из них, а также 50 реальных писем, полученных ранее. В итоге, 92 письма были идентифицированы верно, 5 фишинговых писем идентифицированы как легальные и 3 легальных письма идентифицированы как фишинг. Результаты обработки результатов представлены на диаграмме на рисунке 5.

Рисунок 5 – Результаты обработки результатов проверки работы системы

Разработанная система способна функционировать как в качестве самостоятельной программы, определяющей фишинговые письма, так и использоваться как обучающий модуль естественной среды в рамках повышения осведомленности сотрудников о фишинге.

ЗАКЛЮЧЕНИЕ

В результате работы над магистерской диссертацией были выполнены следующие задачи.

Проанализирована структура сообщения, передаваемого по электронной почте. Выявлены структурные части электронного письма: конверт, заголовок и тело. Исследована каждая структурная часть сообщения. Выявлены возможные признаки фишинга в заголовке письма, тексте, ссылках и вложениях.

Проведено исследование существующих методов выявления фишинга. Рассмотрены способы анализа писем как в ручном режиме, так и с использованием средств автоматизации.

Разработана архитектура системы фильтрации писем для корпоративной почты. Разработаны алгоритмы анализа каждой структурной части письма для определения уровня безопасности сообщения. Разработан графический интерфейс системы, позволяющий пользователю ознакомиться с результатом анализа письма, где подробно разъяснен процесс оценки сообщения по каждой структурной части и визуализирован результат оценки уровня безопасности. Проведено тестирование точности работы системы, для чего проведена фишинговая кампания с помощью ресурса GoPhish. Точность работы системы составила 92 %. Разработана система организационно-технических мер, направленных на обучение пользователей.

Разработанная система позволяет определить, является полученное письмо фишинговым или легальным и может предотвратить получение нежелательных писем. Также система может быть включена в обучение и тренировку навыков пользователей информационных систем, позволяя пользователям запоминать признаки фишинга в условиях киберучений в естественной среде в организации.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Бычек, М. Н. Email phishing: structure and distinguishing features / М. Н. Бычек, науч. рук. Т. В. Борботько // Электронная техника и технология: Тезисы докладов 58-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 18–22 апреля 2022 г. – Минск: БГУИР, 2022. – С. 915–918.

2. Бычек, М. Н. Система фильтрации фишинговых писем / М.Н. Бычек, Т.В. Борботько // Технические средства защиты информации: тезисы докладов XX Белорусско-российской научно-технической конференции, Республика Беларусь, Минск, 7 июня 2022 г. – Минск: БГУИР, 2022. – С. 27–28.