УДК 004.852

5.2.2. Математические, статистические и инструментальные методы экономики (физико-математические науки, экономические науки)

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ИДЕНТИФИКАЦИИ ФИШИНГОВЫХ РЕСУРСОВ

Гальцев Борис Сергеевич
Аспирант
e-mail: b.galtsev@gmail.com
Московский финансово-промышленный университет «Синергия», Москва, Россия

В данном исследовании рассматриваются основные методы фишинговых атак и существующие меры противодействия данным атакам. Подробно рассмотрено решение задачи идентификации фишинговых ресурсов как решение задачи классификации с помощью технологий искусственного интеллекта и методов машинного обучения, определены и обоснованы наиболее подходящие из них. Составлен алгоритм решения задачи идентификации фишинговых ресурсов с помощью технологий искусственного интеллекта и методов машинного обучения, рассмотрены условия применения и использования данных технологий и методов, а также необходимые настройки и конфигурации. Подробно рассмотрены условия применения метрик оценки работы выбранных технологий и методов. С целью выявления признаков, указывающих на фишинговость ресурсов, проанализированы основные векторы сокрытия злоумышленниками таких признаков, а также стратегии и методы работы современных средств защиты по выявлению таких ресурсов. Проведена практическая работа по применению технологий искусственного интеллекта и методов машинного обучения при решении задачи идентификации фишинговых ресурсов на основе общедоступного датасета с признаками фишиговых и легитимных веб-ресурсов (рассматривались признаки, основанные только на информации URL-адресов, без учета данных контента самих ресурсов) с применением языка программирования Python. Сделаны выводы о применимости технологий искусственного интеллекта и методов машинного обучения при решении задачи идентификации фишинговых ресурсов

Ключевые слова: ФИШИНГ, ФИШИНГОВЫЕ РЕСУРСЫ, ЗАДАЧА ИДЕНТИФИКАЦИИ, ЗАДАЧА КЛАССИФИКАЦИИ, МАШИННОЕ ОБУЧЕНИЕ, МЕТРИКИ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

http://dx.doi.org/10.21515/1990-4665-200-014

UDC 004.852

5.2.2. Mathematical, statistical and instrumental methods of economics (physical and mathematical sciences, economic sciences)

APPLICATION OF MACHINE LEARNING METHODS TO IDENTIFY PHISHING RESOURCES

Galtsev Boris Sergeevich
graduate student
e-mail: b.galtsev@gmail.com
Moscow Financial and Industrial University "Synergy", Moscow, Russia

In this research the author examines the main methods of phishing attacks and existing measures to counter these attacks. Here the author considered in detail the solution of the problem of identifying phishing resources as a solution to the classification problem using artificial intelligence technologies and machine learning methods, identified and justified the most suitable of them. In this research the author compiled an algorithm for solving the problem of identifying phishing resources using artificial intelligence technologies and machine learning methods, considered conditions for the application and using of these technologies and methods, as well as the necessary settings and configurations. The conditions for application of metrics for evaluating the performance of selected technologies and methods are considered in detail. In order to identify features indicating the phishing of resources, the main vectors of hiding such features by attackers and strategies and methods of operation of modern security tools to identify such resources were analyzed. Practical work on using of artificial intelligence technologies and machine learning methods in solving the problem of identifying phishing resources based on a publicly available dataset with features of phishing and legitimate web-resources (based only on URL-address information without the content data of the resources) was done by using the Python programming language. Finally the author made conclusions on the applicability of artificial intelligence technologies and machine learning methods in solving the problem of identifying phishing resources

Keywords: PHISHING, PHISHING RESOURCES, IDENTIFICATION TASK, CLASSIFICATION TASK, MACHINE LEARNING, METRICS OF MACHINE LEARNING METHODS

Введение.

Фишинг – это метод атак социальной инженерии, который наиболее широко используется для получения конфиденциальной информации пользователя, такой как учетные данные для входа в различные системы, информация о кредитных и дебетовых картах, банковских счетах и т.д. [1, с.1]. Так в 2023 году почти половина (43%) всех успешных атак на организации были проведены с использованием социальной инженерии (почти 80% через социальные сети, мессенджеры и электронную почту). Все это свидетельствует об эффективности фишинговых атак, которые могут привести как к репутационным, так и к серьезным финансовым потерям [2].

В своих сообщениях злоумышленники, в основном, выдают себя за:

- партнеров по бизнесу (26%);
- коллег из технических служб (15%);
- работников различных государственных служб (13%).

Приоритетным у злоумышленников способом доставки таких сообщений является электронная почта (92%). Вредоносная часть доставляется посредством вложенных файлов:

- архивы 7z, ZIP, RAR и т.д. (37%);
- текстовые и табличные документы WORD, EXCEL и т.д. (30%).

Вложенные ссылки в фишинговых сообщениях, почти в половине случаев, ведут на web-страницу, предназначенную для введения конфиденциальных данных [2]. Такие ресурсы, в случае известности ресурса (бренда), представляют собой полную копию легитимного ресурса (web-сайта). Ввод конфиденциальных данных (в том числе идентификационных и аутентификационных данных) на таком ресурсе приводит к их раскрытию перед злоумышленниками.

В случае создания фишинговых ресурсов в виде клонов широко известных легитимных ресурсов (в основном web-сайтов)

злоумышленники стараются создать их контент практически идентичным легитимным, а URL-адреса могут отличаться лишь несколькими знаками, при этом пользователь не всегда может визуально идентифицировать эти отличия. Другой широко распространенный вариант подмены URL-адреса – когда часть адреса ресурса состоит из адреса легитимного ресурса и части фишингового, при этом используются двойные слеши и протоколы более 1 раза. Такие тонкости в URL-адресах даже человеку из сферы информационных технологий (IT) сложно идентифицировать [3, с.61]. Все это указывает на необходимость автоматизации процессов идентификации фишинговых ресурсов.

Основная часть.

Существующие меры защиты делятся на три типа: превентивные, реактивные и проактивные. Под превентивными мерами защиты от фишинговых атак понимаются организационные и технические меры, при которых объект атаки не принимает самостоятельных решений по определению фишинговости доставляемых сообщений, все происходит до того, как он получит сообщение. К таким мерам относят: различные спам-фильтры, в том числе на почтовых серверах, а также специализированные антифишинговые решения. К реактивным техническим мерам защиты относят те, которые основываются на проверке уже доставленных сообщений, в качестве примера технических средств, реализующих такой тип защиты, можно привести специализированные плагины для браузера, проверяющие сайты и предупреждающие пользователей о потенциально опасном контенте, а также программные антифишинговые решения в виде «толстого клиента», функционирующие непосредственно на средстве вычислительной техники (объекте атаки) [4, с.930-931]. К реактивным организационным мерам можно отнести повышение уровня культуры информационной безопасности пользователей путем проведения соответствующих обучающих мероприятий, в том числе, нацеленных на

идентификацию нелегитимных ресурсов. К проактивным мерам относятся меры, применяемые уже после реализации фишинговой атаки, такие как блокировка банковской карты, смена паролей и т.д. [5, с.96-97]. Разница между техническими мерами, относящимися к превентивному и реактивному типам, заключается в том, что превентивные, в основном, устанавливаются на входе в локальную вычислительную сеть организации с целью фильтрации входящего трафика (экономия времени, трудовых и материальных ресурсов, необходимых для установки и эксплуатации средств защиты на всех средствах вычислительной техники), а второе – устанавливается непосредственно на каждый потенциальный объект атаки [5, с.97].

Существующие средства защиты для идентификации нелегитимных ресурсов используют различные стратегии и методы, такие как черный и белый списки, эвристические и визуальные методы и другие [3, с.58-60]. Основная задача такой идентификации состоит в том, чтобы определить, относится ресурс по тем или иным признакам к фишинговым или нет (есть подозрение на фишинговость ресурса или нет). Таким образом, задачу идентификации нелегитимных ресурсов можно свести к задаче классификации. Учитывая наличие достаточного объема информации о классифицирующих признаках фишинговых ресурсов (URL-адреса, контент, и другие источники), а также тип решаемой задачи (задача классификации), рассмотрим алгоритм решения задачи идентификации нелегитимных ресурсов как решение задачи классификации методами машинного обучения.

Задача классификации представляет собой задачу отнесения рассматриваемого объекта, в зависимости от его характеристик (признаков), к одному из заранее определенных классов. Решение задачи классификации методами машинного обучения включает в себя следующие основные этапы:

1. Определение количества классов. Задачи классификации разделяют по количеству классов, основные из них: задачи бинарной, множественной, одноклассовой (унарной) и мультиклассовой классификации. Для решения задачи идентификации фишинговых ресурсов наиболее подходящей является задача бинарной классификации (1 – есть подозрение на фишинговость, 0 – нет).

2. Выбор обучающего признакового пространства для машинного обучения. Это один из основных этапов, составляющих базу для качественной и точной работы методов машинного обучения. Чем большего объема является признаковое пространство с качественными различными признаками, тем более точно и качественнее будет работать выбранный метод решения задачи. Зачастую требуется проводить предобработку обучающего признакового пространства, в зависимости от выбранного метода машинного обучения для решения задачи, так как существует множество факторов, которые могут критически влиять на работу одних методов и совершенно быть незначительными для других. Так, например, наличие у объектов признакового пространства нелинейных связей между собой приводит к снижению качества работы «линейных» методов, в частности – метода логистической регрессии (logistic regression), что не особо влияет на качество работы «лесных» методов (random forest, decision tree и др.). Слишком большие объемы признаковых пространств, в свою очередь, привели к появлению методов градиентного бустинга. При решении задачи идентификации фишинговых ресурсов, в основном, выбирают признаковые пространства, основанные на параметрах URL-адресов и контенте самих ресурсов, таких как [3, с.60-61][6, с.503-504][7, с.122]:

- кодировка домена на уровне страны хостинг-провайдера;
- определенные слова в URL-адресе и контексте ресурса;
- схожесть URL-адресов с общеизвестными;

- наличие логически не связанных символов в доменном имени;
- наличие грамматических ошибок в контексте ресурса;
- запрещенный контент;
- информация о SSL/TLS-сертификатах;
- доступность URL-адреса;
- параметры URL-адреса:
    - длина (количество символов, в том числе URL-адреса, субдомена, доменного имени, имени хоста и т.д.);
    - количество субдоменов/подкаталогов;
    - наличие определенных спецсимволов, таких, как @, # и т.д.;
    - наличие сетевого адреса;
    - количество спецсимволов;
    - количество точек;
    - количество цифр;
    - количество дефисов;
    - количество двойных слешей;
    - количество протоколов;
    - количество и номера портов.

Некоторые подходы по формированию и выбору признаковых пространств основываются на иных параметрах ресурсов, таких как: количество предыдущих посещений ресурса [7, с.122], концептуальная и буквальная согласованность между URL-адресом и контентом ресурса [8, с. 1].

Инструментальные средства идентификации фишинговых ресурсов, основанные на применении технологий искусственного интеллекта и методов машинного обучения, в основном относят к реактивному типу мер защиты. Представленный выше перечень признаков является перечнем

наиболее значимых признаков для web-ресурса, не является конечным и зависит от направления векторов фишинговых атак.

3. Сопоставление каждому объекту обучающего признакового пространства определенного класса. Необходимо, чтобы каждому объекту обучающего признакового пространства соответствовал определенный класс (целевой признак), на основе данного соответствия выбранный метод машинного обучения будет осуществлять дальнейшую работу по классификации объектов. Ошибочное соответствие приведет к неточности работы метода классификации.

4. Выбор метрики оценки работы метода машинного обучения и его порогового значения. Оценка работы методов машинного обучения осуществляется на основе значений метрик. Выбор порогового значения метрики, в основном, применяется для фиксации нижней границы оценки качетсва работы выбранного метода для поставленной задачи. С целью рассмотрения основных метрик введем понятие матрицы ошибок (confusion matrix) в терминах ошибок классификации (ошибки 1 и 2 рода), представленной в Таблице №1 [10]:

Таблица №1 – матрица ошибок

	$y = 1$	$y = 0$
$\hat{y} = 1$	True Positive (TP)	False Positive (FP)
$\hat{y} = 0$	False Negative (FN)	True Negative (TN)

Здесь $\hat{y}$ – это значение результата работы метода на единице данных, а y – истинное значение для этих данных. Таким образом, ошибки классификации бывают двух видов: False Positive (FP) и False Negative (FN). Рассмотрим основные метрики, используемые для оценки работы методов машинного обучения: Accuracy (1), Precision (2), Recall (3), F-мера (4), FPR (5), где:

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \quad (1)$$

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

$$F - мера = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (4)$$

$$FPR = \frac{FP}{FP + TN} \quad (5)$$

Accuracy (точность) – простая для понимания метрика, представляющая собой долю правильно полученных результатов по итогу работы метода. Основной минус данной метрики – для обучения метода необходимы сбалансированные данные.

Precision – доля правильно предсказанных объектов положительного класса среди всех объектов, предсказанных как объекты положительного класса.

Recall – доля предсказанных объектов положительного класса из всего объема объектов положительного класса.

F-мера представляет собой среднее гармоническое Precision и Recall.

FPR (False Positive Rate) показывает, какую долю отрицательных объектов классификатор предсказал неверно. Вариант, при котором FPR = 0 и Recall = 1 – когда классификатор не ошибается.

Как видим, можно использовать значения всех представленных метрик [1, с.62], однако в большинстве исследовательских отчетов представлено значение метрики Accuracy [1, с.12][4, с.931][6, с.505][9, с.9], связано это с тем, что данная метрика логически понятна и прямо коррелирует с поставленной задачей. С целью получения качественных значений метрики Accuracy необходимо проверять обучающее признаковое

пространство на наличие дисбаланса классов и при выявлении – его устранять. Устранить дисбаланс можно следующими методами [11]:

- Class Weighting – присваивание разных весов разным классам данных;
- Oversampling – увеличение количества данных в менее представленных классах;
- Undersampling – уменьшение количества данных в более представленных классах;
- SMOTE – генерация синтетических данных класса меньшинства на основе близлежайших соседей.

Выбор правильного метода устранения дисбаланса (или их комбинаций) зависит от конкретной задачи, выбранного метода машинного обучения и обучающего признакового пространства. Обычно выбор метода (или их комбинаций) достигается экспериментальным путем. Так, например, лучшие результаты метрики точности при решении задачи классификации на основе признакового пространства, состоящего из фичей, характеризующих выражения лиц, были достигнуты после применения таких методов борьбы с дисбалансом классов, как SMOTE и Class Weighting [12, с.688].

5. Выбор метода машинного обучения. Методы машинного обучения, в зависимости от типа решаемых задач, разделяют на 2 вида: регрессионные и классификационные, решающие задачи регрессии и классификации соответственно. Для решения задачи классификации, на практике, в основном, применяются следующие методы (модели):

- Логистическая регрессия (Logistic Regression);
- Дерево решений (Decision Tree);
- Случайный лес (Random Forest);
- Наивный байесовский классификатор (Naive Bayes Classifier);
- K-Ближайших соседей (K-Nearest Neighbors);

- Градиентный бустинг (Gradient Boosting):
  - AdaBoost;
  - XGBoost;
  - *CatBoost* (разработана Яндексом);
- Метод опорных векторов (Support Vector Machines);
- Искусственные нейронные сети (Neural Networks).

При выборе метода машинного обучения необходимо учитывать следующие факторы:

- Признаки могут быть как числовыми, так и категориальными. Для одних типов методов критически важно при предобработке данных выполнить масштабирование числовых и кодирование категориальных данных (Линейные методы, в частности – Логистическая регрессия), для других - «лесных» методов (Random Forest, Decision Tree и др.) важно только кодирование, а для CatBoost не требуется применять методы масштабирования и кодирования данных.
- Признаки могут быть созависимыми, что может критично сказываться на результатах работы Линейных методов.
- Объем данных. Не все методы способны качественно, а главное в разумное время решить поставленную задачу при огромном объеме обучающего признакового пространства, в этом случае стараются применять методы градиентного спуска (Градиентного бустинга) и Искусственные нейронные сети.

Результаты множественных исследований по решению задачи идентификации фишинговых ресурсов определяют лучший показатель метрики Accuracy (99.98%) по результатам работы метода Сверточных нейронных сетей (Convolutional Neural Networks) – класс метода Искусственных нейронных сетей [4, 931]. При этом результаты оценок метрики Accuracy для одних и тех же методов принимают следующие различные значения: для метода Случайного леса – от 93% до 99.57%;

Логистической регрессии - от 96.58% до 99.2%; Дерева решений - от 93% до 98.4%; K-Ближайших соседей - от 97.3% до 99.2%; Градиентного бустинга - от 98.4% до 99.2%; Метода опорных векторов - от 89.75% до 99.2% [9, с.9].

Тем самым анализ множественных исследований показал, что результаты оценки точности работы одних и тех же методов могут различаться, так как множество факторов влияют на итоговый результат, в том числе: правильно выбранное обучающее признаковое пространство, правильно проведенная предобработка его данных, а также – правильно подобранные параметры используемых методов машинного обучения (гиперпараменты).

6. Выбор подходящих параметров работы методов машинного обучения. Для успешной работы выбранных методов машинного обучения необходимо, прежде всего – правильно подобрать их параметры (гиперпараметры). Выбор гиперпараметров методов в общем можно автоматизировать – имеются специально разработанные стратегии и инструменты, такие как:

- Решетчатый поиск (Grid Search) – представляет собой перебор заданных пользователем значений (перебор по сетке) с целью нахождения лучшей комбинации. Хорошо работает, когда небольшое количество гиперпараметров. Является одним из самых простых методов для понимания и реализации. При этом, данный метод не использует результаты других проведенных итераций, ограничен в выборе рассматриваемых параметров заданной заранее сеткой значений. Долгое время работы.
- Случайный поиск (Random Search) – представляет собой случайный выбор значений для каждого гиперпараметра, зачастую срабатывает быстрее, чем решетчатый метод поиска, так как непрерывные параметры можно задать в виде распределения, а не перечислять значения заранее.

При этом, данный метод не использует результаты других проведенных итераций, как и решетчатый метод, ограничен в выборе рассматриваемых параметров заданной заранее сеткой значений.

- Байесовская оптимизация (Bayesian Optimization) – представляет собой сочетание вероятностных методов с методами оптимизации. Данный метод использует результаты предыдущих итераций, умеет выявлять зависимости гиперпараметров, умеет изменять границы поиска гиперпараметров, зачастую достигает более высокого качества, чем метод Случайного поиска. При этом наблюдается долгое время работы и трудности в работе с категориальными гиперпараметрами.

Гиперпараметры очень важны при создании методов машинного обучения. Их неправильный подбор может привести к неудовлетворительным результатам работы методов, низким скоростям обучения или их переобучению [13]. На практике используются все три метода.

7. Проведение обучения выбранного метода на основе обучающего признакового пространства. Данный этап выполняется путем применения определенных методов в зависимости от среды исполнения.

8. Оценка работы обученного метода на основе выбранной метрики. Данный этап выполняется путем применения определенных методов в зависимости от среды исполнения.

9. Решение задачи классификации объекта на основе признакового пространства объекта и обученного метода машинного обучения. Непосредственно применение обученного метода машинного обучения к пространству параметров, объекты которого необходимо классифицировать.

Таким способом решаются задачи классификации машинного обучения, в том числе, задачи идентификации фишинговых ресурсов.

Практическая часть.

Работа выполнялась на языке Python в среде разработки JupiterLab на основе набора URL-адресов, состоящего из 835697 записей [14] (обучающее признаковое пространство), размеченных как URL-адреса фишинговых и легитимных ресурсов (“1” и “0” соответственно). Изначально обучающий набор содержал 390764 фишинговых и 444933 легитимных URL-адресов. Предварительный анализ данного набора выявил 14295 дублирующих значений, после удаления дубликатов соотношение количества фишинговых к количеству легитимных URL-адресов стало: 386189 к 435213.

Рисунок №1 − Соотношение количества фишинговых к количеству легитимных URL-адресов в изначальном наборе

Дисбаланс данных присутствует, но не критичен. Первый круг экспериментов провели без сведения дисбаланса.

После этого каждый URL-адрес разбили на слова, очистили от стоп-слов (несут мало смысловой нагрузки, например, артикли, предлоги, союзы и т.д.) с помощью свободно распространяемой Python-библиотеки NLTK, оставили только слова и буквенные наборы, в том числе, обозначающие протоколы (http, https, www и т.д.). К такому набору данных применили токенизацию (процесс разбиения текста на более мелкие части, такие как

слова) и лемматизацию (сводит слова к их лемме) с помощью широко известного инструмента WordNetLemmatizer, входящего в состав библиотеки NLTK. В итоге получили наборы лемм слов, входящих в URL-адреса:

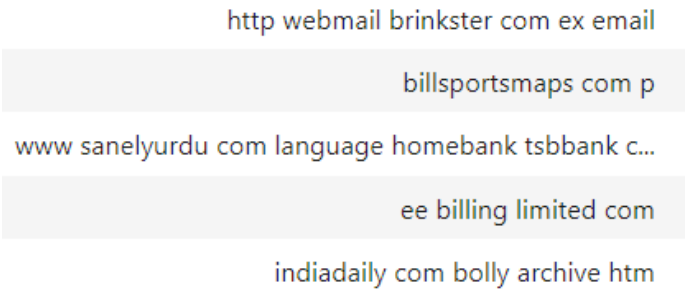

Рисунок №2 − Наборы лемм слов, входящие в URL-адреса

Целевым признаком выбрали разметку URL-адресов (фишинговые или легитимные). Из наборов лемм с помощью метода Term Frequency-Inverse Document Frequency (TF-IDF) выделили слова с большим весом для каждого URL-адреса в контексте всех URL-адресов набора. Данный метод вычисляет важность каждой леммы в URL-адресе относительно количества ее употреблений в данном URL-адресе и во всем наборе URL-адресов.

В качестве метрики оценки работы методов машинного обучения выбрали Accuracy (точность) – показывающую долю правильных значений в результате работы метода. Метрика была выбрана в соответствии выборами метрик других исследователей, результаты работ которых приведены выше [4, 931][9, с.9] для возможного сравнения полученных результатов. Как было отмечено, основной минус данной метрики – необходимы сбалансированные данные для обучения метода.

Определившись с набором обучающих признаков и типом метрики, приступили к обучению разных методов (моделей): LogisticRegression, DecisionTreeClassifier, RandomForestClassifier, CatBoostClassifier и SGDClassifier.

Для каждого метода поиск гиперпараметров выполнялся с помощью решетчатого поиска Grid Search.

По итогу обучения указанных методов (моделей) получили следующие значения метрики Accuracy:

- Accuracy LogisticRegression = 0.93;
- Accuracy DecisionTreeClassifier = 0.85;
- Accuracy RandomForestClassifier = 0.72;
- Accuracy CatBoostClassifier = 0.92;
- Accuracy SGDClassifier = 0.91.

Второй круг экспериментов провели с предварительно сведенным дисбалансом посредством Undersampling (уменьшение количества данных в более представленном классе). Результаты работы методов практически не изменились, что говорит о небольшом дисбалансе в представленных классах и его незначительном влиянии на итоговый результат работы, даже для линейных моделей.

Полученные результаты коррелируют с результатами других исследователей, приведенными выше [4, 931][9, с.9]. При этом стоит отметить, что рассмотренные нами методу обучались только на очищенных леммах слов, не содержащих цифр и каких-либо символов, отличных от буквенных, это указывает на то, что при ином подходе к предобработке обучающего набора признаков (различные подходы рассмотрены в данной статье выше) можно добиться увеличения значения метрики Accuracy.

Выводы.

Задача идентификации фишинговых ресурсов не является тривиальной, успешность решения которой напрямую зависит от правильно определенных признаков, указывающих на фишинговость, и от применяемых методов к ее решению. Задача идентификации нелегитимных ресурсов сводится к задаче классификации, которая успешно решается с

помощью технологий искусственного интеллекта и методов машинного обучения.

Применяя технологии искусственного интеллекта и методы машинного обучения необходимо учитывать их специфику, от которой напрямую зависит результат работы, а именно: правильное проведение предобработки данных признакового пространства, выбор методов решения задачи и метрик оценки работы.

Решение задачи идентификации фишинговых ресурсов с помощью технологий искусственного интеллекта и методов машинного обучения является одним из наиболее точных и перспективных.

Проведенная практическая работа показала, что на существующих общедоступных наборах URL-адресов можно построить довольно точные модели машинного обучения, решающие задачи по идентификации фишинговых ресурсов. При этом используемые нами методы конфигурации моделей – только малая часть, доступная исследователям.

Список литературы:

1. Gowda H.R.M., Adithya M.V., Prasad S.G., Vinay S, Development of anti-phishing browser based on random forest and rule of extraction framework // Cybersecurity. 2020. Vol. 3. N. 1. P. 1-14. URL: https://cybersecurity.springeropen.com/counter/pdf/10.1186/s42400-020-00059-1.pdf.

2. https://www.ptsecurity.com/ru-ru/research/analytics/phishing-attacks-on-organizations-in-2022-2023 (дата обращения: 27.04.2024).

3. Митюков, Е.А. Модель обнаружения фишинговых атак на основе гибридного подхода для защиты автоматизированных систем управления производством / Е.А. Митюков, А.В. Затонский // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2020. – Т. 20, № 2. – С. 56–66. DOI: 10.14529/ctcr200206.

4. Mohammed A., Bakar A., Azaliah N., and Fiza R. Anti-Phishing Tools: State of the Art and Detection Efficiencies // Applied Mathematics & Information Sciences. 2022. № 16. P. 929–934. DOI: 10.18576/amis/160609.

5. Архипова А. Б., Нечаев Д. А. Технология формирования интегрированной антифишинговой системы в цифровом обществе // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 93–103. https://doi.org/10.55648/1998-6920-2023-17-2-93-103.

6. Maraximov A., Xudaybergenov K., Choriyev H., Nasiriddinov A. Модифицированный алгоритм повышения производительности машинного обучения для обнаружения и классификации фишинговых атак // Science and innovation. 2022. Т.

1. № A8. С. 499-507. URL: https://cyberleninka.ru/article/n/modifitsirovannyy-algoritm-povysheniya-proizvoditelnosti-mashinnogo-obucheniya-dlya-obnaruzheniya-i-klassifikatsii-fishingovyh-atak.

7. Власенко А. В., Дзьобан П. И., Жук Р. В. Защита персональных данных при авторизации пользователя в распределенных информационных системах, построенных на основе Web-технологий // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2017. № 2 (201). С. 120-128. URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-pri-avtorizatsii-polzovatelya-v-raspredelennyh-informatsionnyh-sistemah-postroennyh-na-osnove-web.

8. Azeez, Nureni Ayofe and Salaudeen, Balikis Bolanle and Misra, Sanjay and Damasevicius, Robertas and Maskeliunas, Rytis Identifying phishing attacks in communication networks using URL consistency features // International Journal of Electronic Security and Digital Forensics. 2020. Vol. 12. N. 2. P. 200. URL: https://www.inderscienceonline.com/doi/epdf/10.1504/IJESDF.2020.106318.

9. Alnemari, S.; Alshammari, M. Detecting Phishing Domains Using Machine Learning. Appl. Sci. 2023, 13, 4649. https://doi.org/ 10.3390/app13084649.

10. https://habr.com/ru/companies/ods/articles/328372/ (дата обращения: 29.04.2024).

11. https://habr.com/ru/companies/otus/articles/769242/ (дата обращения: 29.04.2024).

12. Рюмина Е.В., Карпов А.А. Сравнительный анализ методов устранения дисбаланса классов эмоций в видеоданных выражений лиц // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 5. С. 683–691. doi: 10.17586/2226-1494-2020-20-5-683-691/.

13. https://habr.com/ru/companies/otus/articles/754402/ (дата обращения: 29.04.2024).

14. https://huggingface.co/datasets/ealvaradob/phishing-dataset/blob/main/urls.json (дата обращения: 13.05.2024).

References:

1. Gowda H.R.M., Adithya M.V., Prasad S.G., Vinay S, Development of anti-phishing browser based on random forest and rule of extraction framework // Cybersecurity. 2020. Vol. 3. N. 1. P. 1-14. URL: https://cybersecurity.springeropen.com/counter/pdf/10.1186/s42400-020-00059-1.pdf.

2. https://www.ptsecurity.com/ru-ru/research/analytics/phishing-attacks-on-organizations-in-2022-2023 (data obrashhenija: 27.04.2024).

3. Mitjukov, E.A. Model' obnaruzhenija fishingovyh atak na osnove gibridnogo podhoda dlja zashhity avtomatizirovannyh sistem upravlenija proizvodstvom / E.A. Mitjukov, A.V. Zatonskij // Vestnik JuUrGU. Serija «Komp'juternye tehnologii, upravlenie, radiojelektronika». – 2020. – T. 20, № 2. – S. 56–66. DOI: 10.14529/ctcr200206.

4. Mohammed A., Bakar A., Azaliah N., and Fiza R. Anti-Phishing Tools: State of the Art and Detection Efficiencies // Applied Mathematics & Information Sciences. 2022. № 16. P. 929–934. DOI: 10.18576/amis/160609.

5. Arhipova A. B., Nechaev D. A. Tehnologija formirovanija integrirovannoj antifishingovoj sistemy v cifrovom obshhestve // Vestnik SibGUTI. 2023. T. 17, № 2. S. 93–103. https://doi.org/10.55648/1998-6920-2023-17-2-93-103.

6. Maraximov A., Xudaybergenov K., Choriyev N., Nasiriddinov A. Modificirovannyj algoritm povyshenija proizvoditel'nosti mashinnogo obuchenija dlja obnaruzhenija i klassifikacii fishingovyh atak // Science and innovation. 2022. T. 1. № A8. S. 499-507. URL:

https://cyberleninka.ru/article/n/modifitsirovannyy-algoritm-povysheniya-proizvoditelnosti-mashinnogo-obucheniya-dlya-obnaruzheniya-i-klassifikatsii-fishingovyh-atak.

7. Vlasenko A. V., Dz'oban P. I., Zhuk R. V. Zashhita personal'nyh dannyh pri avtorizacii pol'zovatelja v raspredelennyh informacionnyh sistemah, postroennyh na osnove Web-tehnologij // Vestnik Adygejskogo gosudarstvennogo universiteta. Serija 4: Estestvenno-matematicheskie i tehnicheskie nauki. 2017. № 2 (201). S. 120-128. URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-pri-avtorizatsii-polzovatelya-v-raspredelennyh-informatsionnyh-sistemah-postroennyh-na-osnove-web.

8. Azeez, Nureni Ayofe and Salaudeen, Balikis Bolanle and Misra, Sanjay and Damasevicius, Robertas and Maskeliunas, Rytis Identifying phishing attacks in communication networks using URL consistency features // International Journal of Electronic Security and Digital Forensics. 2020. Vol. 12. N. 2. P. 200. URL: https://www.inderscienceonline.com/doi/epdf/10.1504/IJESDF.2020.106318.

9. Alnemari, S.; Alshammari, M. Detecting Phishing Domains Using Machine Learning. Appl. Sci. 2023, 13, 4649. https://doi.org/ 10.3390/app13084649.

10. https://habr.com/ru/companies/ods/articles/328372/ (data obrashhenija: 29.04.2024).

11. https://habr.com/ru/companies/otus/articles/769242/ (data obrashhenija: 29.04.2024).

12. Rjumina E.V., Karpov A.A. Sravnitel'nyj analiz metodov ustranenija disbalansa klassov jemocij v videodannyh vyrazhenij lic // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2020. T. 20. № 5. S. 683–691. doi: 10.17586/2226-1494-2020-20-5-683-691/.

13. https://habr.com/ru/companies/otus/articles/754402/ (data obrashhenija: 29.04.2024).

14. https://huggingface.co/datasets/ealvaradob/phishing-dataset/blob/main/urls.json (data obrashhenija: 13.05.2024).