

УДК 004.056

DOI 10.37468/2307-1400-2024-2-13-24

## ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ РАСПОЗНАВАНИЯ ФИШИНГОВЫХ РЕСУРСОВ

**Котиков Никита Михайлович**<sup>1</sup>  
**Максимова Елена Александровна**<sup>1</sup>  
**Русаков Алексей Михайлович**<sup>1</sup>

<sup>1</sup> МИРЭА - Российский технологический университет, г. Москва, Россия

### АННОТАЦИЯ

Целью работы является исследование популярных методов машинного обучения, применяемых для обеспечения безопасности информационных систем и их пользователей от фишинга. В настоящей статье рассматриваются актуальные технологии злоумышленников для проведения атак с использованием методов социальной инженерии, меры защиты, позволяющие обеспечить безопасность корпоративных пользователей, а также классификация методов обнаружения нелегитимных интернет-ресурсов с использованием технологий машинного обучения. В качестве существующих алгоритмов машинного обучения, позволяющих производить идентификацию опасных ресурсов в статье представлены: теорема Байеса, принцип классификатора, алгоритм k-ближайших соседей и логистическая регрессия, а также приведена статистическая информация в отношении частоты обнаружения популярных признаков фишинговых и зловредных ресурсов. По результатам исследования в статье обоснована необходимость использования комплексного подхода к обеспечению защиты инфраструктуры с учетом многовекторного анализа как достаточно востребованного как в теоретическом, так и в практическом плане.

**Ключевые слова:** классификация, фишинг, информационная безопасность, машинное обучение.

## USING MACHINE LEARNING ALGORITHMS TO RECOGNIZE PHISHING RESOURCES

**Kotikov Nikita M.**<sup>1</sup>  
**Maksimova Elena A.**<sup>1</sup>  
**Rusakov Alexey M.**<sup>1</sup>

<sup>1</sup> MIREA - Russian Technological University, Moscow, Russia

### ABSTRACT

The purpose of the work is to study popular machine learning methods used to ensure the security of information systems and their users from phishing. This article discusses the current technologies of intruders to carry out attacks using social engineering methods, security measures to ensure the security of corporate users, as well as the classification of methods for detecting illegitimate Internet resources using machine learning technologies. As existing machine learning algorithms that allow the identification of dangerous resources, the article presents: Bayes' theorem, the classifier principle, the k-nearest neighbor algorithm and logistic regression, as well as statistical information on the frequency of detection of popular signs of phishing and malicious resources. The article concludes that an integrated approach to ensuring infrastructure protection, taking into account a multi-vector analysis.

**Keywords:** classification, phishing, information security, machine learning.

## Введение

В условиях существенного роста активности злоумышленников в отношении сегментов промышленности, торговли, здравоохранения и науки Российской Федерации, а также мирового поощрения хактивизма эффективное обеспечение информационной безопасности становится одной из приоритетных задач [1].

Одной из основных тактик воздействия в области кибербезопасности является проведение атак с использованием методов социальной инженерии для рассылки вредоносного программного обеспечения с целью шифрования информации. Жертвами одних из наиболее крупных атак с применением шифровальщиков в 2024 году являются компании СДЭК и сеть магазинов «Верный» [2].

Учитывая тот факт, что человек всегда был и будет наиболее уязвимым звеном любой корпоративной системы, обеспечение эффективного и результативного комплексного подхода к обеспечению информационной безопасности является актуальной и важной задачей [3].

## Технологии социальной инженерии

Злоумышленниками используется обширный перечень технологий компрометации и фальсификации реально существующих ресурсов с целью введения в заблуждение пользователей. Сами фишинговые ресурсы становятся все сложнее в обнаружении, в том числе и по причине исполь-

зования искусственного интеллекта в создании различного рода контента.

Основные технологии, используемые нарушителями, приведены в таблице 1.

## Противодействие атакам

С точки зрения противодействия атакам с использованием методов социальной инженерии рекомендуется применять совокупность мер защиты (рисунок 1).

Актуальные стратегии, организационно-распорядительные документы и средства защиты, необходимые к реализации в целях защиты информационных систем, приведены в таблице 2.

В рамках регулярного повышения осведомленности сотрудников набирает популярность метод проведения обучения сотрудников техникам обнаружения и противодействия фишинговым атакам с последующим тестированием – проведением социотехнических кампаний. Для этого применяется специализированный фреймворк «GoPhish» [4]. Крупные финансовые компании Московского региона при помощи регулярных мероприятий по повышению осведомленности и тестированию сотрудников добились минимизации угроз со стороны атак с применением методов социальной инженерии – менее 5% переходов по подозрительным ссылкам.

Иным подходом в части обучения является геймификация. Данный подход реализован в экосистеме Сбербанка после масштабной

Таблица 1 – Основные технологии социальной инженерии

Техника	Описание
Подмена адресной строки	Спуфинг адресной строки – техника, направленная на манипуляцию значением адресной строки браузера.
Копирование целевой страницы	Создание как можно более точного визуального совпадения с реально существующими ресурсами, включая логотипы, слоганы, картинки и фотографии.
SEO спам	Повышение рейтинга фальшивого или мошеннического сайта в целях агрессивного продвижения в топ выдачи браузера пользователей.

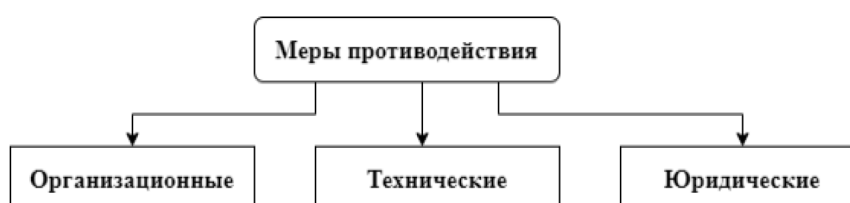


Рисунок 1 – Меры защиты

Таблица 2 – Меры защиты

Меры	Описание
Организационные	Включает в себя различные стратегии, политики безопасности и процессы, которые позволяют обеспечить объективный контроль за состоянием основных процессов в организации. К ним относятся политика противодействия ВПО, парольная политика, а также регулярные мероприятия по проверке знаний и ознакомлению с ответственностью.
Технические	Включает в себя совокупность внедрения, настройки и эффективной эксплуатации разного рода технологий и средств защиты.
Юридические	Включает в себя совокупность нормативно – правовых документов, регламентирующих построение систем защиты и обеспечение информационной безопасности в целом. К ним относятся 152-ФЗ, 187-ФЗ, 149-ФЗ, 126-ФЗ, приказы ФСТЭК № 21, 17, 239 и другие.

фишинговой атаки на сотрудников от имени Германа Грефа [5].

Обзор и анализ существующих алгоритмов машинного обучения

Одним из основных инструментов машинного обучения считается теорема Байеса, основной принцип которой обусловлен оценкой вероятности достоверности того или иного события:

$$P(\theta|D) = \frac{P(\theta)P(D|\theta)}{P(D)} = \frac{P(\theta)P(D|\theta)}{\int_{\theta \in \Theta} P(D|\theta)P(\theta)d\theta} \quad (1)$$

где  $\theta$  – параметры модели,

$D$ – данные объекта исследования,

$P(\theta)$ – априорная вероятность (prior probability),

$P(D|\theta)$ – правдоподобие (likelihood),

$P(\theta | D)$ – апостериорная вероятность (posterior probability),

$P(D)= \int P(D | \theta)P(\theta)d\theta$  – вероятность данных (evidence).

Основной задачей является поиск и/или максимизация распределения апостериорной вероятности  $P(\theta | D)$  для формирования наиболее подходящих к набору данных параметров.

Принцип классификатора заключается в вычислении функции правдоподобия для каждого объекта, по которой, в свою очередь, вычисляются апостериорные вероятности. Для этого определяется плотность распределения каждого из классов [6].

Алгоритм k-ближайших соседей. Метод является метрическим классификатором, обуслов-

ленным оценкой сходства объектов. Алгоритм относит объект к классу, которому принадлежат ближайшие его соседи. Для реализации алгоритма используется расстояние Минковского [7]:

$$\rho(x, y) = (\sum_{i=1}^n |x_i - y_i|^p)^{\frac{1}{p}}, \quad (2)$$

где  $n$  – количество объектов в наборе данных,

$p$  – параметр Минковского.

Логистическая регрессия применяется для моделирования отношений между переменными, а также дальнейшего анализа с целью определения влияния на итоговый результат. Основной задачей является поиск функции, которая наиболее точно описывает текущую зависимость. Одним из алгоритмов обучения для искусственного интеллекта является линейная регрессия [8]:

$$y(x, \omega) = \omega_0 + \sum_{j=1}^p x_j w_j = x^T w. \quad (3)$$

Математическая модель, построенная по принципу нейронных связей живых организмов, где каждый нейрон обладает связью с другими слоями соседей, а их эффективность повышается по мере обучения:

$$y(x, w) = f(\sum_{j=1}^N w_j \phi_j(x)), \quad (4)$$

где  $f$  – нелинейная функция активации,

$w$  – вектор весов,

$\phi$  – нелинейные базисные функции.

#### Критерии классификации интернет – ресурсов

В качестве основного критерия определения подлинности веб – страниц выступают компоненты адресной строки [9–11] (рисунок 2).

<схема> : [ // [ <логин> [ : <пароль> ] @ ] <хост> [ : <порт> ] ] [ / <URL-адрес> ] [ ? <параметры> ] [ # <якорь> ]

Рисунок 2 – Структура URL

На рисунке 2:

<схема> – схема обращения к ресурсу, т.е. сетевой протокол;

<логин> – имя пользователя, используемое для доступа к ресурсу;

<пароль> – пароль пользователя;

<хост> – полное доменное имя хоста в системе DNS или IP-адрес;

<порт> – порт хоста для подключения;

<URL-адрес> – унифицированный указатель ресурса;

<параметры> – строка GET-запроса с передаваемыми параметрами на сервер (символ «?» – начало запроса, символ «&» – разделитель параметров);

<якорь> – идентификатор «якоря» с предшествующим символом #.

Для оценки подлинности используется комплекс критериев оценки фишинговых страниц с использованием методов искусственного интеллекта [12, 13]. Все представленные в таблице 3 критерии были отсортированы по величине [14]:

$$Rank = \frac{\sum_{i=1}^n r_i * a_i}{n}, \quad (5)$$

где  $n$  – кол-во моделей;

$r_i$  – точность классификации модели  $m_i$ , использующей рассматриваемый критерий;

$a_i$  – наличие рассматриваемого критерия.

Таблица 3 – Признаки фишинговых сайтов

Критерий	W12	W1	W9	W2	W6	W7	W5	W3	W4	W8	W11	W10	Σ	%	Rank
	99,9	98,7	98,0	98,0	97,6	97,4	95,3	94,3	93,4	92,7	91,5	83,0			
1. Длина URL	+	+		+	+	+	+	+	+	+	+		10	95,9	79,9
2. Наличие IP-адресов в URL	+	+			+	+	+		+	+	+		8	95,8	63,9
3. Наличие @ в URL	+		+		+	+	+	+	+				7	96,6	56,3
4. Рейтинг сайта	+			+	+	+	+		+	+			7	96,3	56,2
5. Возраст домена	+				+	+	+		+	+	+		7	95,4	55,7
6. HTTPS в основном URL		+			+	+	+	+	+				6	96,1	48,1
7. Соотношение внешних ссылок		+			+	+	+		+		+		6	95,7	47,8
8. Кол-во записей домена в DNS	+				+	+	+		+				5	96,7	40,3
9. Срок регистрации домена	+				+	+	+		+				5	96,7	40,3
10. Соотношение общих страниц (распространённых якорных ссылок)		+			+	+	+		+				5	96,5	40,2
11. Наличие перенаправлений с использованием '//' в URL			+		+	+	+		+				5	96,4	40,1
12. Число поддоменов в URL				+	+	+	+		+				5	96,3	40,1
13. Кол-во якорных ссылок					+	+	+		+		+		5	95,1	39,6
14. Наличие всплывающих окон с полями для ввода текста					+	+	+		+		+		5	95,1	39,6
15. Кол-во повторов запроса URL					+	+	+		+		+		5	95,1	39,6
16. Веб-трафик					+	+	+		+		+		5	95,1	39,6
17. Число слешей в URL	+	+	+					+					4	97,7	32,6
18. Использование службы сокращения URL			+		+	+	+						4	97,1	32,4
19. Нестандартный порт					+	+	+		+				4	95,9	32,0
20. Отключение события щелчка правой кнопкой мыши					+	+	+		+				4	95,9	32,0
21. Использование Iframe					+	+	+		+				4	95,9	32,0
22. Кол-во перенаправлений					+	+	+		+				4	95,9	32,0
23. Число точек в URL		+	+					+		+			4	95,9	32,0
24. Обработчик серверных форм (SFM)					+	+	+				+		4	95,5	31,8
25. Нулевые ссылки	+	+							+				3	97,4	24,3

Таблица 3 (продолжение)

Критерий	W12	W1	W9	W2	W6	W7	W5	W3	W4	W8	W11	W10	Σ	%	Rank
	99,9	98,7	98,0	98,0	97,6	97,4	95,3	94,3	93,4	92,7	91,5	83,0			
26. Валидация TLD		+		+				+					3	97,0	24,2
27. Длина домена		+		+				+					3	97,0	24,2
28. Число имен брендов в URL		+		+				+					3	97,0	24,2
29. Средняя длина слова в URL		+		+				+					3	97,0	24,2
30. Число токенов в URL		+		+				+					3	97,0	24,2
31. Длина домена		+		+				+					3	97,0	24,2
32. Число имен брендов в URL		+		+				+					3	97,0	24,2
33. Средняя длина слова в URL		+		+				+					3	97,0	24,2
34. Число токенов в URL		+		+				+					3	97,0	24,2
35. Наличие префикса или суффикса, разделенного «-» в домене					+	+	+						3	96,8	24,2
36. Загрузка Favicon с внешнего домена					+	+	+						3	96,8	24,2
37. Кол-во ссылок в тегах <Meta>, <Script>, <Link>					+	+	+						3	96,8	24,2
38. Наличие индекса в Google					+	+	+						3	96,8	24,2
39. Составление статистических отчетов					+	+	+						3	96,8	24,2
40. Конечное состояние SSL					+	+					+		3	95,5	23,9
41. Ненормальный URL					+		+			+			3	95,2	23,8
42. Наличие имен доменов в титульнике	+	+											2	99,4	16,6
43. Наличие имен доменов в авторских правах	+	+											2	99,4	16,6
44. Наличие имен доменов в тексте заголовков	+	+											2	99,4	16,6
45. Кол-во цифр в URL			+	+									2	98,0	16,3
46. проверка имени хоста по IP-адресу	+							+					2	97,1	16,2
47. Наличие фишинговых слов		+						+					2	96,5	16,1
48. Наличие имен брендов в поддомене		+						+					2	96,5	16,1
49. Число цифр в доменном имени		+						+					2	96,5	16,1
50. Длина имени хоста		+						+					2	96,5	16,1
51. Число дефисов в именах хостов		+						+					2	96,5	16,1
52. Цифры в именах хостов		+						+					2	96,5	16,1
53. Наличие фишинговых слов в URL		+						+					2	96,5	16,1
54. Число цифр в URL		+						+					2	96,5	16,1
55. Длина самого большого слова в URL		+						+					2	96,5	16,1
56. Наличие дефисов в URL			+					+					2	96,1	16,0
57. Количество нижних подчеркиваний в имени хоста			+					+					2	96,1	16,0
58. Наличие вопросительного знака в URL			+					+					2	96,1	16,0
59. Наличие «;» в основном URL			+					+					2	96,1	16,0
60. Наличие вопросительного знака в URL			+					+					2	96,1	16,0
61. Количество нижних подчеркиваний в имени хоста			+					+					2	96,1	16,0
62. Наличие «;» в основном URL			+					+					2	96,1	16,0
63. Изменение статус бара при наведении мыши					+				+				2	95,5	15,9
64. Время между текущим и момента уничтожения домена	+												1	100,0	8,3
65. Наличие заголовка и атрибута ключевого слова	+												1	100,0	8,3

Таблица 3 (продолжение)

Критерий	W12	W1	W9	W2	W6	W7	W5	W3	W4	W8	W11	W10	Σ	%	Rank
	99,9	98,7	98,0	98,0	97,6	97,4	95,3	94,3	93,4	92,7	91,5	83,0			
66. Наличие ссылки на текущий домен	+												1	100,0	8,3
67. Средняя длина слова		+											1	98,7	8,2
68. Длина самого большого слова		+											1	98,7	8,2
69. Наличие имен доменов в наименьших терминах TF-IDF		+											1	98,7	8,2
70. Коэффициент сходства объектов (их хэшей) с расстоянием Хэмминга		+											1	98,7	8,2
71. Наличие «=» в основном URL			+										1	98,0	8,2
72. Наличие «+» в основном URL			+										1	98,0	8,2
73. Наличие «:» в основном URL			+										1	98,0	8,2
74. Наличие «~» в основном URL			+										1	98,0	8,2
75. Наличие «#» в основном URL			+										1	98,0	8,2
76. Наличие «!» в основном URL			+										1	98,0	8,2
77. Наличие «&» в основном URL			+										1	98,0	8,2
78. Наличие «%» в основном URL			+										1	98,0	8,2
79. Длина самого короткого слова в URL				+									1	98,0	8,2
80. Стандартное отклонение длин слов в необработанном списке слов [15]				+									1	98,0	8,2
81. Количество рассматриваемых слов, обработанных в модуле декомпозиции слова				+									1	98,0	8,2
82. Средняя длина рассматриваемых слов, обработанных в модуле декомпозиции слова [15]				+									1	98,0	8,2
83. Число декомпозированных слов				+									1	98,0	8,2
84. Число ключевых слов в URL				+									1	98,0	8,2
85. Число схожих с ключевыми словами слов				+									1	98,0	8,2
86. Число схожих с ключевыми словами брендов				+									1	98,0	8,2
87. Число случайно сгенерированных слов				+									1	98,0	8,2
88. Число целевых имен брендов в URL				+									1	98,0	8,2
89. Число схожих с ключевыми словами слов				+									1	98,0	8,2
90. Число схожих с ключевыми словами брендов				+									1	98,0	8,2
91. Число целевых ключевых слов в URL				+									1	98,0	8,2
92. Число случайно сгенерированных слов				+									1	98,0	8,2
93. Число целевых ключевых слов в URL				+									1	98,0	8,2
94. Число целевых имен брендов в URL				+									1	98,0	8,2
95. Число других слов				+									1	98,0	8,2
96. Имя домена состоит из случайного набора символов				+									1	98,0	8,2
97. Длина поддомена				+									1	98,0	8,2
98. Наличие www. com в доменах или поддоменах				+									1	98,0	8,2
99. Punycode				+									1	98,0	8,2
100. Наличие специальных символов в URL				+									1	98,0	8,2
101. Последовательное повторение символа				+									1	98,0	8,2

**Алгоритм классификации**

На основании приведенной выше статистики можно сделать вывод, что наиболее эффективным и результативным методом является комплексный компонентно – сигнатурный анализ, использующий совокупность наиболее результативных алгоритмов для идентификации, по окончании работы которого будет получен положительный или отрицательный результат валидации.

Алгоритм классификации (рисунок 3) в ходе исследования реализован на языке JavaScript (Node.js) для различных сред.

**Экспериментальное исследование**

Разработанный алгоритм классификации протестирован в различных сценариях с точки зре-

ния оценки эффективности и результативности. Эксперимент затронул следующий функционал в комплексе:

- защита на основе публичных списков (black-list);
- защита на основе анализа адресной строки на предмет специальных символов (включая Punicode домены);
- защита на основе анализа одноразовых вредоносных ссылок с идентификаторов (?rid = 123...).

В качестве экспериментального ресурса был использован домен reportegrupal12.000webhostapp.com (рисунок 4), не попадающий под ограничения штатных средств защиты браузеров или провайдера, что говорит о том, что данный ресурс

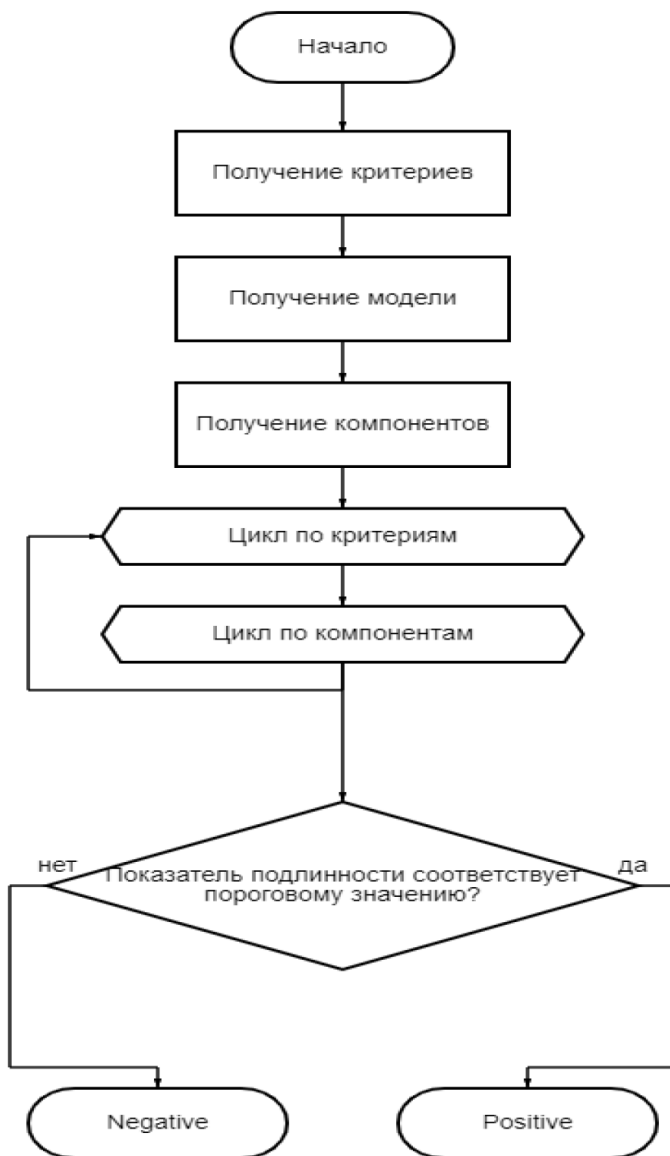


Рисунок 3 – Алгоритм классификации

еще не прошел валидацию алгоритмами доменного патруля и не был добавлен в черные списки провайдера и сервисов Yandex.


 Dog eating cassette tape



Рисунок 4 – Потенциально вредоносный ресурс

Разработанный алгоритм позволил проанализировать вредоносный ресурс и дать достаточно точную оценку его легитимности – 9 из 90 средств защиты от различных вендоров отметили домен как вредоносный или фишинговый, что однозначно сигнализирует о его небезопасности. Результат работы алгоритма представлен на рисунке 5.

В рамках экспериментального исследования был проведен анализ разработанного алгоритма на большом количестве данных. Результаты представлены в таблице 4.

В рамках эксперимента было установлено, что разработанный алгоритм выявляет потенци-

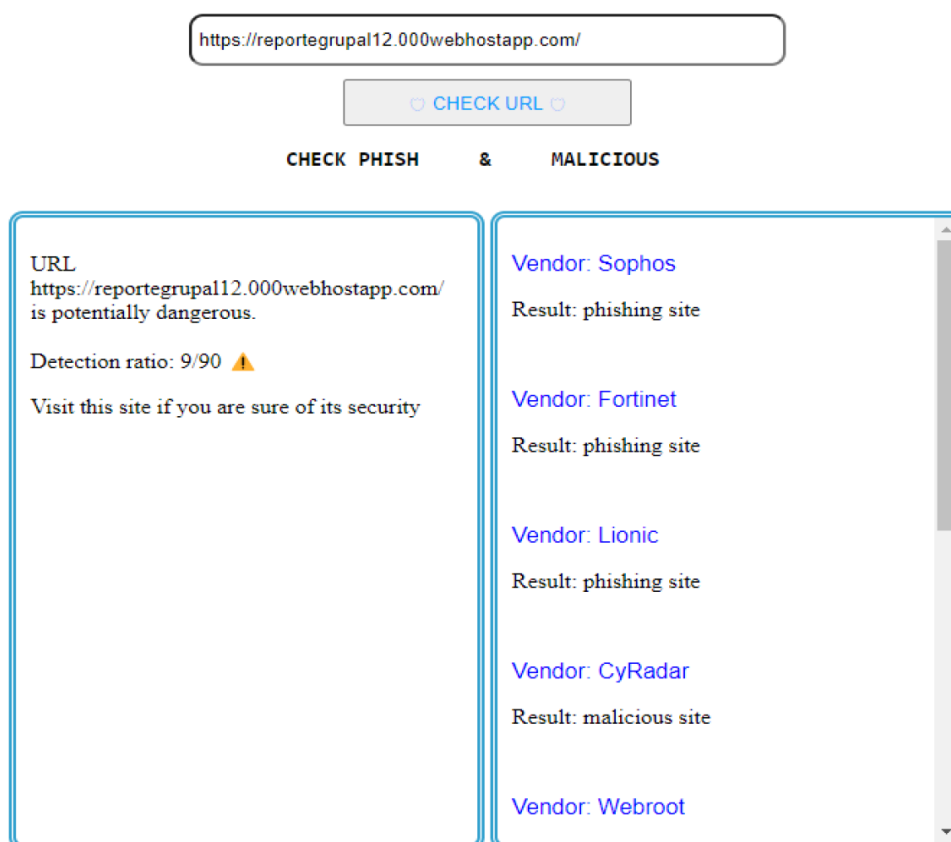


Рисунок 5 – Результат работы алгоритма

Таблица 4 – Сравнительная характеристика

№	Количество ресурсов	Выявлено	Процентная характеристика
1	100	90	90
2	500	435	87
3	1000	819	81,9
4	3000	2141	71,3
5	5000	3985	79,7
6	10000	7337	73,4



ально вредоносные ресурсы с высоким уровнем точности, при этом было обнаружено порядка 5% ресурсов на каждом этапе, прошедших валидацию с низким уровнем критичности – до 5 актуальных меток из 90, что может говорить о том, что исследуемые домены с высокой долей вероятности можно отнести к опасным, но только по косвенным признакам, выявленным алгоритмом. Аналитическую оценку эффективности работы алгоритма позволяют произвести графики (рисунки 6, 7), отображающие соотношение выявленных угроз к общему количеству, а также

динамику процентного соотношения к объемам выборки. На всех этапах анализа разработанный алгоритм показал эффективность свыше 70%, что является достаточным для достижения целей результатом.

**Заключение**

1. Была проанализирована качественная информация о популярных технологиях проведения атак с использованием методов социальной инженерии.
2. Проведен обзор комплекса мер защиты, позволяющих обеспечить высокий уровень

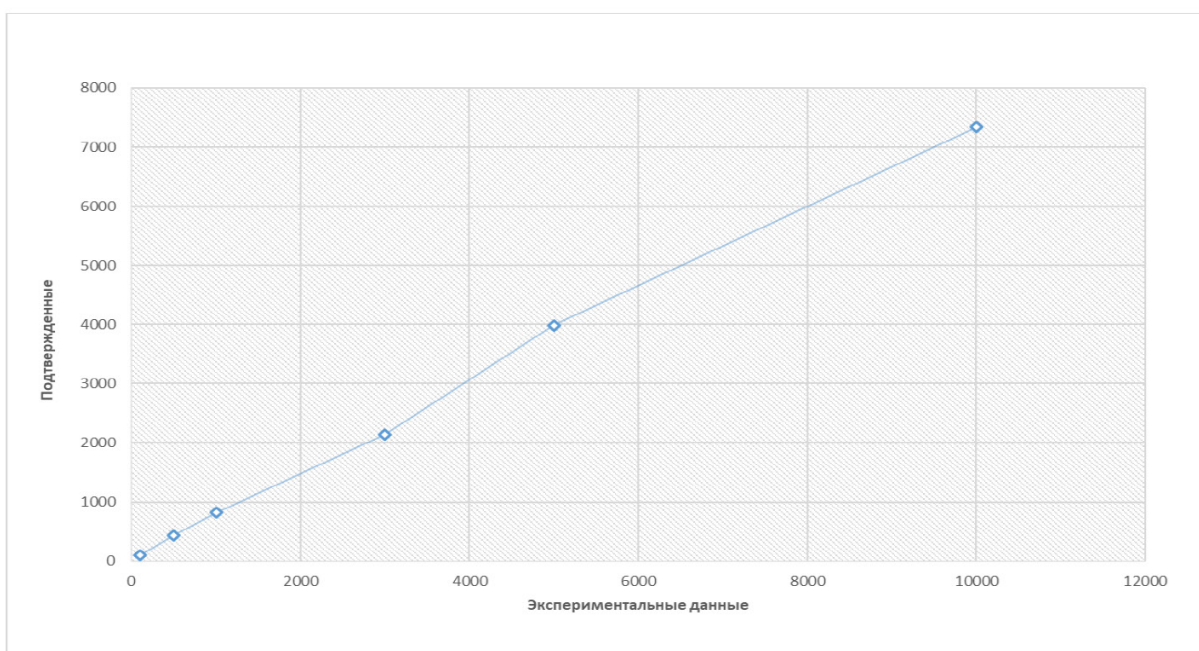


Рисунок 6 – Динамика обнаружения

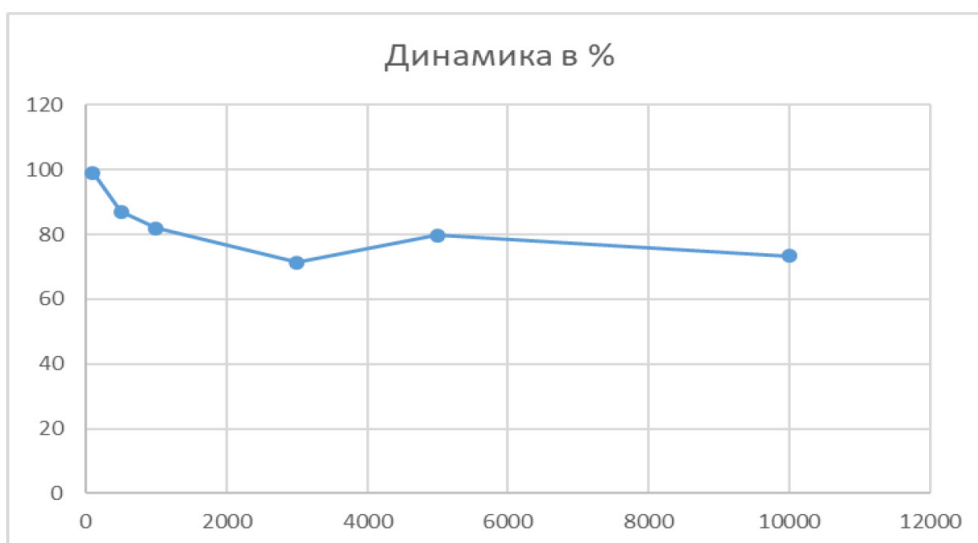


Рисунок 7 – Оценочное процентное соотношение

безопасности в отношении атак класса социальной инженерии.

3. Проведен обзор существующих алгоритмов машинного обучения и перечень подходов к их использованию.

4. Наиболее эффективным методом классификации интернет – ресурсов можно отметить агрегированный, комплексный подход с использованием наиболее популярных и эффективных критериев и методов. Алгоритм классификации реализован на Java Script.

5. Проведена демонстрация разработанного алгоритма, его визуальной составляющей и результатов работы на реальных примерах.

6. Проведено экспериментальное исследование в отношении эффективности и результативности разработанного алгоритма. В качестве выборки были приведены от 100 до 10000 вредоносных ресурсов, подлежащих автоматизированной валидации. Результаты работы алгоритма изложены в таблицах, а на основе полученной информации сделано выводы в отношении эффективности и результативности разработанного решения. Получены аналитические результаты и оценка эффективности работы алгоритма.

#### Список литературы

1. Импортзамещение на рынке информационной безопасности [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/articles/676664/>

2. Угрозовая активность: как связаны хакерские атаки на сеть «Верный» и СДЭК [Электронный ресурс]. – Режим доступа: <https://iz.ru/1706284/ivan-chernousov-valerii-kodachigov-evgeniia-pertceva/ugrozovaia-aktivnost-kak-sviazany-khakerskie-ataki-na-set-vernyi-i-sdek>

3. Хакеры открывают сезон распродаж [Электронный ресурс]. – Режим доступа: <https://www.kommersant.ru/doc/4548082>

4. Gophish – фреймворк для фишинга. Как писать фейковые письма и обманывать своих сотрудников [Электронный ресурс]. – Режим доступа: <https://xaker.ru/2016/12/07/gophish->

[phishing-framework-howto/](#)

5. Сбербанк создал flash-игру для сотрудников после фишинговых «писем Грефа» [Электронный ресурс]. – Режим доступа: [https://www.rbc.ru/technology\\_and\\_media/15/02/2017/58a430e69a79472ba6d0aad?from=newsfeed](https://www.rbc.ru/technology_and_media/15/02/2017/58a430e69a79472ba6d0aad?from=newsfeed)

6. Наивный алгоритм Байеса в машинном [Электронный ресурс]. – Режим доступа: <https://www.guru99.com/ru/naive-bayes-classifiers.html>

7. Метод k-ближайших соседей (k-nearest neighbour) [Электронный ресурс]. – Режим доступа: <https://proglib.io/p/metod-k-blizhayshih-sosedey-k-nearest-neighbour-2021-07-19>

8. Logistic Regression in Machine Learning [Электронный ресурс]. – Режим доступа: <https://www.geeksforgeeks.org/understanding-logistic-regression/>

9. Punycode [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki/Punycode/>

10. Phishing with Unicode Domains [Электронный ресурс]. – Режим доступа: <https://www.xudongz.com/blog/2017/idn-phishing/>

11. Rao R.S., Pais A.R. Two level filtering mechanism to detect phishing sites using lightweight visual similarity approach // Journal of Ambient Intelligence and Humanized Computing. – 2020. – V. 11. – No. 9. – P. 3853-3872. DOI: <https://doi.org/10.1007/s12652-019-01637-z>

12. Nagaraj K., Bhattacharjee B., Sridhar A., Sharvani G.S. Detection of phishing websites using a novel twofold ensemble model // Journal of Systems and Information Technology. – 2018. – V. 20. – No 3. – P. 321-357. DOI: <https://doi.org/10.1108/JSIT-09-2017-0074>

13. Sönmez Y., Tuncer T., Gökal H., Avci E. Phishing web sites features classification based on extreme learning machine // 2018 6th International Symposium on Digital Forensic and Security (ISDFS). – 2018. – P. 1-5. DOI: <https://doi.org/10.1109/ISDFS.2018.8355342>

14. Zamir A., Khan H.U., Iqbal T., Yousaf N., Aslam F., Anjum A., Hamdani M. Phishing web site detection using diverse machine learning algorithms // The Electronic Library. – 2020. – V. 38. – No 1. – С. 65-80. DOI: <https://doi.org/10.1108/EL-05-2019-0118>

15. Sonowal G., Kuppusamy K.S. PhiDMA – A Phishing Detection Model with Multi-filter Approach // Journal of King Saud University-Computer and Information Sciences. – 2020. – V. 32. – No. 1. – P. 99-112. DOI: <https://doi.org/10.1016/j.jksuci.2017.07.005>

16. Purwanto R., Paly A., Blair A., Jha S. PhishZip: A New Compression-based Algorithm for Detecting Phishing Websites // 2020 IEEE Conference on Communications and Network Security (CNS). – IEEE, 2020. – P. 1-9. DOI: <https://doi.org/10.1109/CNS48642.2020.9162211>

### References

1. Import substitution in the information security market [Electronic resource]. URL: <https://habr.com/ru/articles/676664/>

2. Criminal activity: how are hacker attacks on the Verny network and SDEK related? [Electronic resource]. URL: <https://iz.ru/1706284/ivan-chernousov-valerii-kodachigov-evgeniia-pertceva/ugrozovaia-aktivnost-kak-sviazany-khakerskie-ataki-na-set-vernyi-i-sdek>

3. Hackers open the sales season [Electronic resource]. URL: <https://www.kommersant.ru/doc/4548082>

4. Gophish is a phishing framework. How to write fake emails and deceive your employees [Electronic resource]. URL: <https://xakep.ru/2016/12/07/gophish-phishing-framework-howto/>

5. Sberbank has created a flash game for employees after phishing “Gref letters” [Electronic resource]. URL: [https://www.rbc.ru/technology\\_and\\_media/15/02/2017/58a430e69a79472ba6d0aad?from=newsfeed/](https://www.rbc.ru/technology_and_media/15/02/2017/58a430e69a79472ba6d0aad?from=newsfeed/)

6. Naive Bayes algorithm in machine learning [Electronic resource]. URL: <https://www.guru99.com/ru/naive-bayes-classifiers.html>

7. The k-nearest neighbor method (k-nearest neighbour) [Electronic resource]. URL: <https://proglib.io/p/metod-k-blizhayshih-sosedey-k-nearest-neighbour-2021-07-19>

8. Logistic Regression in Machine Learning [Electronic resource]. URL: <https://www.geeksforgeeks.org/understanding-logistic-regression/>

9. Punycode [Electronic resource]. URL: <https://ru.wikipedia.org/wiki/Punycode/>

10. Phishing with Unicode Domains [Electronic resource]. URL: <https://www.xudongz.com/blog/2017/idn-phishing/>

11. Rao R.S., Pais A.R. Two level filtering mechanism to detect phishing sites using lightweight visual similarity approach // Journal of Ambient Intelligence and Humanized Computing. – 2020. – V. 11. – No. 9. – P. 3853-3872. DOI: <https://doi.org/10.1007/s12652-019-01637-z>

12. Nagaraj K., Bhattacharjee B., Sridhar A., Sharvani G.S. Detection of phishing websites using a novel twofold ensemble model // Journal of Systems and Information Technology. – 2018. – V. 20. – No 3. – P. 321-357. DOI: <https://doi.org/10.1108/JSIT-09-2017-0074>

13. Sönmez Y., Tuncer T., Gökal H., Avci E. Phishing web sites features classification based on extreme learning machine // 2018 6th International Symposium on Digital Forensic and Security (ISDFS). – 2018. – P. 1-5. DOI: <https://doi.org/10.1109/ISDFS.2018.8355342>

14. Zamir A., Khan H.U., Iqbal T., Yousaf N., Aslam F., Anjum A., Hamdani M. Phishing web site detection using diverse machine learning algorithms // The Electronic Library. – 2020. – V. 38. – No 1. – C. 65-80. DOI: <https://doi.org/10.1108/EL-05-2019-0118>

15. Sonowal G., Kuppusamy K.S. PhiDMA - A Phishing Detection Model with Multi-filter Approach // Journal of King Saud University-Computer and Information Sciences. – 2020. – V. 32. – No. 1. – P. 99-112. DOI: <https://doi.org/10.1016/j.jksuci.2017.07.005>

16. Purwanto R., Paly A., Blair A., Jha S. PhishZip: A New Compression-based Algorithm for Detecting Phishing Websites // 2020 IEEE Conference on Communications and Network Security (CNS). – IEEE, 2020. – P. 1-9. DOI: <https://doi.org/10.1109/CNS48642.2020.9162211>

Статья поступила в редакцию 16 марта 2024 г.  
Принята к публикации 23 июня 2024 г.

**Ссылка для цитирования:** Котиков Н.М., Максимова Е.А., Русаков А.М. Использование алгоритмов машинного обучения для распознавания фишинговых ресурсов // Национальная безопасность и стратегическое планирование. 2024. № 2(46). С. 13-24. DOI: <https://doi.org/10.37468/2307-1400-2024-2-13-24>

**For citation:** Kotikov N.M., Maksimova E.A., Rusakov A.M. Using machine learning algorithms to recognize phishing resources // National security and strategic planning. 2024. № 2(46). pp. 13-24. DOI: <https://doi.org/10.37468/2307-1400-2024-2-13-24>

#### **Сведения об авторах:**

**КОТИКОВ НИКИТА МИХАЙЛОВИЧ** – ассистент кафедры «Разработка программных решений и системное программирование» Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА (119454, ЦФО, г. Москва, Проспект Вернадского, д. 78), г. Москва, Россия  
e-mail: [kotikov@mirea.ru](mailto:kotikov@mirea.ru)

**МАКСИМОВА ЕЛЕНА АЛЕКСАНДРОВНА** – доктор технических наук, доцент, профессор кафедры «Информационно-аналитические системы кибербезопасности» Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА (119454, ЦФО, г. Москва, Проспект Вернадского, д. 78), г. Москва, Россия  
ORCID: <https://orcid.org/0000-0001-8788-4256>  
SPIN-код: 6876-5558  
e-mail: [maksimova@mirea.ru](mailto:maksimova@mirea.ru)

**РУСАКОВ АЛЕКСЕЙ МИХАЙЛОВИЧ** – старший преподаватель кафедры «Разработка программных решений и системное программирование» Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА (119454, ЦФО, г. Москва, Проспект Вернадского, д. 78), г. Москва, Россия  
SPIN-код: 1066-8077  
e-mail: [rusakov\\_a@mirea.ru](mailto:rusakov_a@mirea.ru)

#### **Information about the authors:**

**KOTIKOV NIKITA M.** – Assistant at the Department of Software Solutions Development and System Programming at the Institute of Cybersecurity and Digital Technologies of the Russian Technological University MIREA (78 Vernadsky Avenue, Moscow, 119454, Central Federal District), Moscow, Russia  
e-mail: [kotikov@mirea.ru](mailto:kotikov@mirea.ru)

**MAKSIMOVA ELENA A.** – Doctor of Technical Sciences, Associate Professor, Professor of the Department of Information and Analytical Systems of Cybersecurity at the Institute of Cybersecurity and Digital Technologies of the Russian Technological University MIREA (78 Vernadsky Avenue, Moscow, 119454, Central Federal District), Moscow, Russia  
ORCID: <https://orcid.org/0000-0001-8788-4256>  
SPIN: 6876-5558  
e-mail: [maksimova@mirea.ru](mailto:maksimova@mirea.ru)

**RUSAKOV ALEXEY M.** – Senior Lecturer at the Department of Software Solutions Development and System Programming at the Institute of Cybersecurity and Digital Technologies of the Russian Technological University MIREA (78 Vernadsky Avenue, Moscow, 119454, Central Federal District), Moscow, Russia  
SPIN: 1066-8077  
e-mail: [rusakov\\_a@mirea.ru](mailto:rusakov_a@mirea.ru)