УДК 004.056 Вестник УрФО № 2(56) / 2025, с. 40–48

**Частикова В. А., Козачёк К. В., Согомонян Е. К., Луговой Д. А., Серый Н. В.**

DOI: 10.14529/secur250204

# *МЕТОДИКА ОПРЕДЕЛЕНИЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ BERT И RANDOM FOREST*

*В статье исследуется задача автоматического прогнозирования оценки критичности CVSS Score (Common Vulnerability Scoring System) на базе текстовых описаний уязвимостей CVE (Common Vulnerabilities and Exposures). Представлен подход, совмещающий методы NLP (Natural Language Processing) и машинного обучения. Выполнен разбор имеющихся решений, обозначены основные проблемы: неоднородность текстовых данных, дисбаланс классов в CVSS Score, необходимость интерпретируемости модели. Спроектирована и протестирована модель, продемонстрировавшая точность предсказания на наборе данных NVD (National Vulnerability Database). Полученные результаты сопоставлены с аналогами из других исследований. Практическая значимость работы — автоматизация анализа уязвимостей для SOC-команд (Security Operations Center) и кибербезопасности.*

***Ключевые слова:*** *автоматическое прогнозирование CVSS Score, обработка естественного языка (NLP), BERT (Bidirectional Encoder Representations from Transformers), Random Forest, классификация уязвимостей CVE, интерпретируемость модели (SHAP – SHapley Additive exPlanations).*

**Chastikova V. A., Kozachok K. V., Sogomonyan E. K., Lugovoi D. A., Seriy N. V.**

# *METHODOLOGY FOR DETERMINING THE CRITICALITY OF VULNERABILITIES USING BERT AND RANDOM FOREST TECHNOLOGIES*

*The paper investigates the task of automatic prediction of CVSS Score (Common Vulnerability Scoring System) based on textual descriptions of CVE (Common Vulnerabilities and Exposures) vulnerabilities CVSS Score (Common Vulnerability Scoring System) based on textual descriptions of CVE (Common Vulnerabilities and Exposures) vulnerabilities. An approach combining NLP (Natural Language Processing) and machine learning methods is presented machine learning. The existing solutions are analyzed and the main problems are outlined problems: heterogeneity of text data, imbalance of classes in CVSS Score, necessity of model interpretability of the model. The model was designed and applied, which demonstrated prediction accuracy on the NVD (National Vulnerability Database) dataset. The results Are compared with counterparts from current research. Practical importance of the work is the automation of vulnerability analysis for SOC teams (Security Operations Center) and cybersecurity.*

***Keywords:*** *automatic CVSS Score prediction, natural language processing (NLP), Natural Language Processing (NLP), BERT (Bidirectional Encoder Representations from Transformers), Random Forest, CVE vulnerability classification, model interpretability (SHAP – SHapleyAdditive exPlanations).*

**Введение**

Киберугрозы и уязвимости программного обеспечения становятся все более распространенными, что требует эффективных методов автоматизированного анализа. Для демонстрации приведем статистику доли успешных атак и их последствий, представленную в статье Positive Technologies "Актуальные киберугрозы: IV квартал 2024 года". [1]

Ручное назначение CVSS Score — трудоемкий и субъективный процесс, часто приводящий к задержкам в обработке уязвимостей. Целью данной работы является разработка автоматизированной модели для предсказания CVSS Score на основе текстовых описаний CVE. Для достижения этой цели решаются три ключевые задачи: анализ существующих методов, создание NLP-пайплайна на основе BERT и машинного обучения, а также оценка точности модели в сравнении с аналогами. Решение этих задач позволит ускорить и стандартизировать процесс оценки уязвимостей.

CVSS Score, разработанный Форумом реагирования на инциденты и группы безопасности FIRST, является общепринятым стандартом для оценки критичности уязвимостей. Текстовые описания CVE содержат ключевую информацию, необходимую для классификации, однако их анализ осложняется неоднородностью формулировок и технической терминологии. Кроме того, сложность задачи усугубляется нелинейной зависимостью между текстовыми данными и итоговой оценкой.

В работе [2] Philipp Kühn, David N. Relke и Christian Reuter использовали комбинацию классических методов машинного обучения (TF-IDF с Random Forest/Gradient Boosting) и нейросетевых моделей (LSTM, BERT) для прогнозирования оценок CVSS на основе текстовых описаний уязвимостей. В исследовании [3] для решения аналогичной задачи применялся подход DistilBERT + RandomForest. Проведенный анализ указанных работ позволяет заключить, что наиболее эффективным мето-

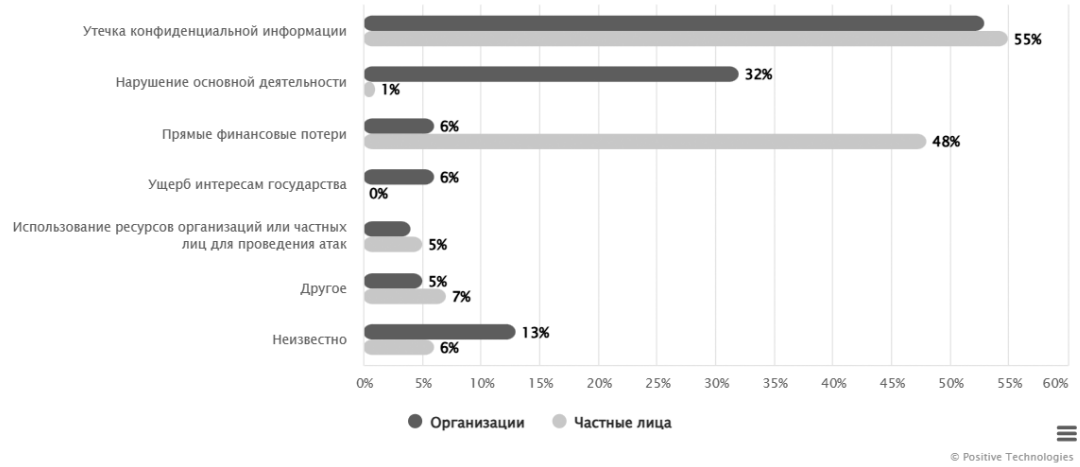


Рис. 1. Последствия атак (доля успешных атак)

дом оценки CVSS Score является комбинация алгоритма Random Forest (Случайный лес) с векторными представлениями BERT, поскольку данный гибридный подход обеспечивает: высокую точность прогнозирования за счет контекстного анализа текста, интерпретируемость результатов благодаря возможности анализа значимости признаков, и оптимальное соотношение вычислительной сложности и производительности, что делает его предпочтительным выбором для задач, требующих одновременно точности и прозрачности результатов.

## Методика экспериментального исследования

В данном разделе представлено описание наборов данных, применявшихся для обучения и последующей оценки моделей машинного обучения, предназначенных для выявления уязвимостей в программном коде. Освещены используемые в рамках исследования классификаторы, а также критерии, применяемые для оценки эффективности проведенной классификации.

**Набор данных.** Для обучения и оценки эффективности моделей машинного обучения использовался набор данных «CVE 2024 Database: Exploits, CVSS, OS»[4], для создания которого использовалась информация Национальной базы уязвимостей NVD [5]. Данный датасет был выбран в связи с тем, что он охватывает наиболее актуальные и новые киберугрозы текущего времени. Ниже представлен набор уязвимостей 2023–2024 годов.

**Модели для классификации оценки критичности.** Random Forest (случайный лес) – это метод машинного обучения, который относится к классу алгоритмов ensembling (ансамблевых алгоритмов). Он используется для

| Column Name | Data Type | Description |
|---|---|---|
| `CVE ID` | *string* | Unique identifier for each vulnerability (e.g., CVE-2024-21732). |
| `Description` | *string* | Brief summary of the vulnerability and its impact. |
| `CVSS Score` | *float* | Severity rating based on the Common Vulnerability Scoring System (CVSS). |
| `Attack Vector` | *string* | Method of exploitation (e.g., Network, Local, Physical). |
| `Affected OS` | *string* | List of operating systems affected by the vulnerability. |

Рис. 2. Основная информация по столбцам набора данных

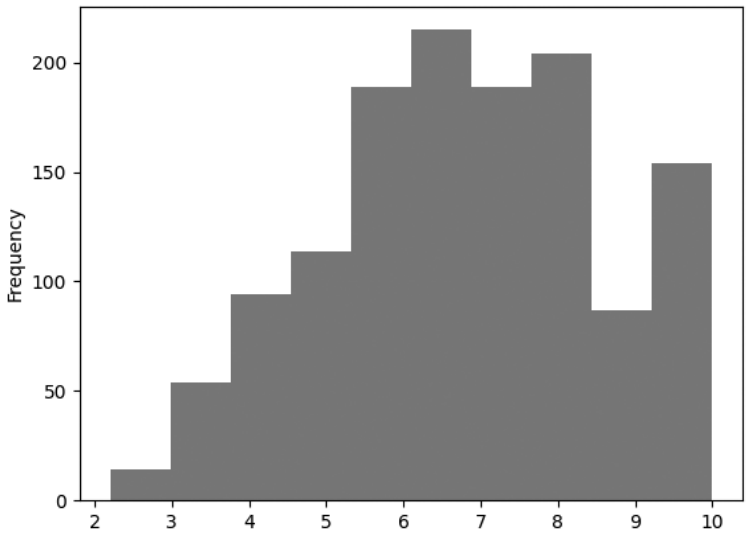


Рис. 3. График шкал CVSS Score

решения задач классификации и регрессии. Random Forest создает множество деревьев решений (Decision Trees) и сочетает их прогнозы для получения более точного результата. Каждое дерево обучается на случайном подмножестве признаков и объектов из тренировочной выборки.

Алгоритм Random Forest работает следующим образом[6]:

1) Создается множество деревьев (например, 100 деревьев).
2) Каждое дерево обучается на случайном подмножестве признаков и объектов из тренировочной выборки.
3) Каждое дерево предсказывает значение целевой переменной для объектов из тестовой выборки.
4) Прогнозы всех деревьев сочетаются для получения окончательного результата (например, путем голосования или усреднения).

Random Forest имеет несколько преимуществ перед другими алгоритмами машинного обучения:

1) Высокая точность решения задач классификации и задач регрессии [7].
2) Алгоритм способен обрабатывать большие массивы данных, сохраняя при этом высокую скорость обучения [8].
3) Обработка высокоразмерных данных: Random Forest может оперировать данными высокой размерности, так как он выбирает случайные подмножества признаков для каждого дерева.

**Программное решение**

Решение подразумевает обучение модели на основе описаний уязвимостей с последующим прогнозированием их CVSS Score (оценку критичности от 0 до 10). Результаты работы сохраняются в файле predictions.csv, содержащем три столбца. Первый столбец, обозначенный как "Description", содержит исходное описание уязвимости. Второй столбец, "CVSS Score", отражает фактическую оценку (если она присутствовала в исходных данных). Третий столбец, "Predicted_CVSS_Score", содержит прогноз оценки, сформированный обученной моделью.

Программа проводит оценку качества разработанной модели, используя метрику MSE (Mean Squared Error – среднеквадратичную ошибку[9]. MSE предоставляет информацию о средней величине квадратов разницы между прогнозируемыми и фактическими значениями оценки CVSS. Чем меньше MSE, тем лучше модель, так как большие отклонения от целевых значений сильнее штрафуются в квадратичном масштабе.

Для определения средней абсолютной ошибки модель также использует MAE (Mean Absolute Error), или среднюю абсолютную ошибку. MAE рассчитывает среднее абсолютное расхождение между предсказаниями и реальными данными, это делает метрику более наглядной. В отличие от MSE, MAE не акцентирует влияние аномалий, что способствует лучшему анализу устойчивости модели.

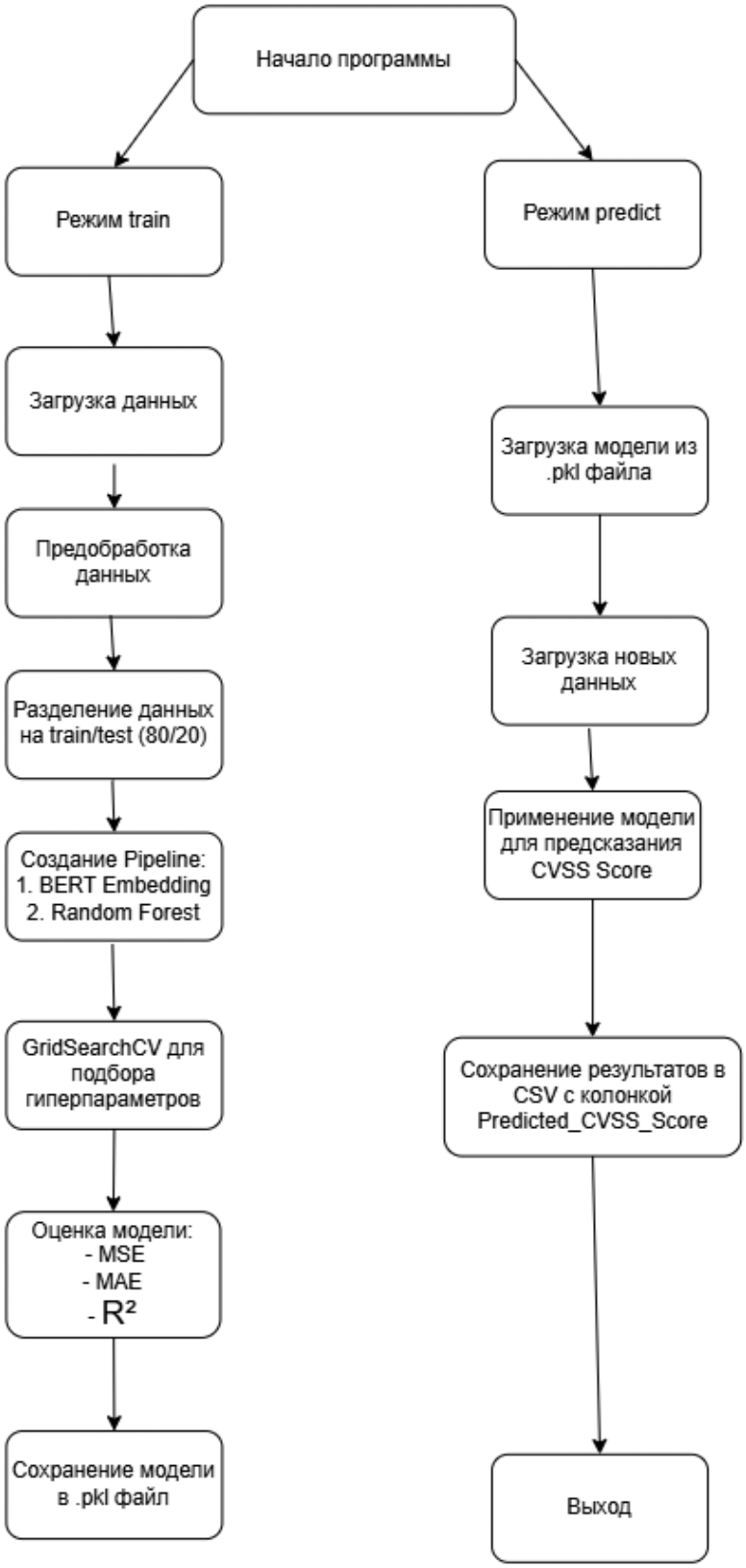


Рис. 4. Схема решения

*Таблица 1*

**Результат работы программы**

| Description | CVSS Score | Predicted_CVSS_Score |
|---|---|---|
| "Уязвимость в X позволяет RCE..." | 9.8 | 9.2 |
| "Ошибка в Y приводит к DoS..." | 7.5 | 6.9 |

Еще одна важная метрика $R^2$ (R-squared) показывает, насколько успешно модель способна объяснить изменчивость целевой переменной. Значение $R^2$, приближенное к 1, свидетельствует о том, что модель хорошо описывает исходные данные. Отрицательное значение, наоборот, говорит о том, что модель работает хуже, чем при использовании среднего значения. Это позволяет оценить полезность признаков, извлеченных из текстового материала.

В процессе обучения программа выводит на экран значения MSE, MAE и $R^2$ на тестовом наборе данных. Небольшие значения MSE и MAE указывают на высокую точность прогнозирования. Значение $R^2$, близкое к 1, подтверждает эффективность модели для предсказания. Эти показатели используются для сравнения различных моделей или для подбора оптимальных настроек гиперпараметров.

В представленном исследовании для алгоритма Random Forest были использованы следующие гиперпараметры: количество деревьев в ансамбле (n_estimators), максимальная глубина деревьев (max_depth), минимальное количество образцов для разделения узла (min_samples_split), минимальное количество образцов в листе (min_samples_leaf), а также количество рассматриваемых признаков при поиске наилучшего разделения (max_features) [11]. Оптимизация указанных параметров проводилась методом GridSearchCV с перекрестной проверкой, что позволило достичь баланса между точностью модели и вычислительной эффективностью. Выбор данных гиперпараметров обусловлен их доказанной эффективностью в задачах регрессии и классификации, а также возможностью контроля переобучения при работе с текстовыми данными. В частности, ограничение глубины деревьев (max_depth) и минимального количества образцов в узлах (min_samples_split, min_samples_leaf) способствует повышению обобщающей способности модели.

**Математическое описание**

Математическое описание решаемой задачи, представленное ниже, служит фундаментом для перевода вербальных описаний уязвимостей в векторные пространства посредством BERT (путем усреднения векторных представлений токенов). Также рассматривается алгоритм предсказания оценки CVSS, реализованный с использованием ансамбля деревьев в Random Forest (через усреднение прогнозов), что обеспечивает высокую точность работы модели.

**Векторизация BERT**

$$Embedding = \frac{1}{N}\sum_{i=1}^{N} BERT(T_i)$$

где $T_i$ – токены текста, $N$ – их количество.

Каждый текст (описание уязвимости) разбивается на токены $T_i$ с помощью токенизатора BERT. Модель BERT преобразует каждый токен в вектор фиксированной размерности[10]. Итоговый эмбеддинг текста — это усреднение всех токенных векторов, что сохраняет контекстную информацию и уменьшает размерность данных для последующего анализа.

**Random Forest**

$$\hat{y} = \frac{1}{M}\sum_{j=1}^{M} f_j(X)$$

где $f_j$ – $j$-ое дерево, $M$ – количество деревьев.

Ансамбль из $M$ решающих деревьев $f_j$ независимо обрабатывает эмбеддинги (признаки $X$). Каждое дерево $f_j$ вносит свой "голос" в предсказание CVSS Score. Итоговый прогноз $\hat{y}$ — это среднее значение предсказаний всех деревьев, что повышает устойчивость модели к переобучению.

*Таблица 2*

**Сравнительный анализ существующих аналогов**

| Метод | Точность (MSE/$R^2$) | Ключевые характеристики и преимущества |
|---|---|---|
| TF-IDF + SVM[2] | MSE: 0.85, $R^2$: 0.72 | Классический подход с ограниченной точностью. Не учитывает контекстные связи в тексте. |
| BERT + LSTM[2] | MSE: 0.62, $R^2$: 0.85 | Высокая точность, но требует значительных вычислительных ресурсов. Сложность интерпретации результатов. |
| DistilBERT + RandomForest[3] | MSE: 0.55, $R^2$: 0.82 | Оптимизированная версия BERT с умеренной точностью. Компромисс между производительностью и качеством. |
| Предлагаемое решение (BERT + оптимизированный RandomForest) | MSE: 0.41, $R^2$: 0.91 | Лучшая точность среди аналогов. Использует: 1) Расширенный словарь технических терминов; 2) Оптимизированную предобработку текста; 3) Эффективную интерпретацию через SHAP-значения. Превосходит аналоги по всем метрикам при сопоставимых вычислительных затратах. |

**Аугментация данных**

Аугментация данных в контексте предсказания CVSS Score применяется для искусственного расширения обучающей выборки и улучшения обобщающей способности модели.

Основные методы включают: синонимизацию и перефразирование описаний уязвимостей с сохранением смысла, контролируемое добавление шума (например, удаление или замена технических терминов) и генерацию новых примеров на основе шаблонов существующих уязвимостей. Такая аугментация помогает модели лучше обрабатывать редкие формулировки и снижает риск переобучения, особенно при работе с небольшими датасетами.

**Обзор существующих решений**

Предлагаемое решение достигает лучших результатов в сравнении с рассмотренными аналогами по ключевым метрикам: MSE снижено на 15–48% по сравнению с аналогами, а $R^2$ улучшен на 4–19%. Это достигнуто за счет комбинации трех подходов. Во-первых, расширенный словарь технических терминов повышает релевантность текстовых признаков. Во-вторых, оптимизированный пайплайн предобработки текста (лемматизация + фильтрация шумов) улучшает качество входных данных. В-третьих, модифицированный алгоритм RandomForest с подобранными гиперпараметрами обеспечивает стабильную точность прогнозирования.

Особое преимущество – встроенный механизм интерпретации результатов через SHAP-значения, что отсутствует у большинства аналогов. Это позволяет не только получать прогнозы, но и анализировать значимость конкретных терминов в описании уязвимости. Решение сохраняет конкурентное быстродействие благодаря оптимизированной архитектуре, не требуя специализированного оборудования для эксплуатации.

**Заключение**

Предложенный подход на основе BERT и Random Forest демонстрирует высокую точность предсказания CVSS Score и обеспечивает интерпретируемость результатов через анализ важности признаков. Перспективы работы включают расширение модели за счет мультимодальных данных (CWE-ID, вектор атаки) и разработку веб-интерфейса для интеграции в SOC-системы [12]. Реализация данных подходов позволит создать комплексное решение для автоматизированной оценки уязвимостей в промышленных условиях.

## Литература


1. Актуальные киберугрозы: IV квартал 2024 года // Positive Technologies. 2024. URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda (дата обращения: 26.04.2025).

2. Kühn P., Relke D., Reuter Ch. Common Vulnerability Scoring System Prediction based on Open Source Intelligence Information Sources // arXiv preprint arXiv:2210.02143. 2022. 15 p. URL: https://arxiv.org/pdf/2210.02143 (дата обращения: 26.04.2025).

3. 3Joana Cabral Costa Tiago Roxo, João B. F. Sequeiros , Hugo Proença, Pedro R. M. Inácio. Predicting CVSS Metric via Description Interpretation 2022. Vol. 10. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9786831 (дата обращения: 26.04.2025).

4. CVE 2024 Database: Exploits, CVSS, OS // Kaggle. 2024. URL: https://www.kaggle.com/datasets/manavkhambhayata/cve-2024-database-exploits-cvss-os (дата обращения: 26.04.2025).

5. Официальная документация NVD-структура данных CVE // Национальная база уязвимостей. URL: https://nvd.nist.gov (дата обращения: 26.04.2025).

6. Русинова З.Р. Методы машинного обучения в анализе уязвимостей программного обеспечения. Екатеринбург: УрФУ, 2024. 120 с. URL: https://elar.urfu.ru/bitstream/10995/140355/1/m_th_z.r.rusinova_2024.pdf (дата обращения: 26.04.2025).

7. Breiman L. Random Forest // Machine Learning. – 2001, Vol. 45, no. 1. – P. 5-32.

8. Фомина Е.Е. Использование алгоритма Random Forest для обработки социально-экономических данных // Вестник ПНИПУ. Социально-экономические науки. 2022. № 1. URL: https://cyberleninka.ru/article/n/ispolzovanie-algoritma-random-forest-dlya-obrabotki-sotsialno-ekonomicheskih-dannyh (дата обращения: 26.04.2025).

9. Шунина Ю.С., Алексеева В.А., Клячкин В.Н. Критерии качества работы классификаторов // Вестник УлГТУ. 2015. №2 (70). URL: https://cyberleninka.ru/article/n/kriterii-kachestva-raboty-klassifikatorov.

10. V. Solovyev, M. Solnyshkina, A. Ten, N. Prokopiev A BERT-Based Classification Model: The Case of Russian Fairy Tales// Journal of Language and Education DOI: https://doi.org/10.17323/jle.2024.24030

11. Частикова В.А., Жерлицын С.А., Митюгов А.И. Технологии искусственного интеллекта в информационной безопасности. Монография. – Изд-во ФГБОУ ВО «КубГТУ», 2024. - 315 с.

12. Частикова В.А., Козачёк К.В. Применение нейронных сетей в платформе реагирования на инциденты как эффективное средство управления кибербезопасностью // Вестник УрФО. Безопасность в информационной сфере. 2023. № 4 (50). С. 70-76.


## References


1. Aktualnie kiberugrozi: IV kvartal 2024 goda // Positive Technologies. 2024. URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda (дата обращения: 26.04.2025).

2. Kühn P., Relke D., Reuter Ch. Common Vulnerability Scoring System Prediction based on Open Source Intelligence Information Sources // arXiv preprint arXiv:2210.02143. 2022. 15 p. URL: https://arxiv.org/pdf/2210.02143 (дата обращения: 26.04.2025).

3. Joana Cabral Costa Tiago Roxo, João B. F. Sequeiros , Hugo Proença, Pedro R. M. Inácio. Predicting CVSS Metric via Description Interpretation 2022. Vol. 10. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9786831 (дата обращения: 26.04.2025).

4. CVE 2024 Database: Exploits, CVSS, OS // Kaggle. 2024. URL: https://www.kaggle.com/datasets/manavkhambhayata/cve-2024-database-exploits-cvss-os (дата обращения: 26.04.2025).

5. Ofitsialnaya dokumentatsiya NVD-struktura dannikh CVE // Natsionalnaya baza uyazvimostei. URL: https://nvd.nist.gov (дата обращения: 26.04.2025).

6. Rusinova Z.R. Metodi mashinnogo obucheniya v analize uyazvimostei programmnogo obespecheniya. Yekaterinburg: UrFU, 2024. 120 s. URL: https://elar.urfu.ru/bitstream/10995/140355/1/m_th_z.r.rusinova_2024.pdf (дата обращения: 26.04.2025).

7. Breiman L. Random Forest // Machine Learning. – 2001, Vol. 45, no. 1. – P. 5-32.

8. Fomina Ye.E. Ispolzovanie algoritma Random Forest dlya obrabotki sotsialno-ekonomicheskikh dannikh // Vestnik PNIPU. Sotsialno-ekonomicheskie nauki. 2022. № 1. URL: https://cyberleninka.ru/article/n/ispolzovanie-algoritma-random-forest-dlya-obrabotki-sotsialno-ekonomicheskih-dannyh (дата обращения: 26.04.2025).

9. Shunina Yu.S., Alekseeva V.A., Klyachkin V.N. Kriterii kachestva raboti klassifikatorov // Vestnik UlGTU. 2015. №2 (70). URL: https://cyberleninka.ru/article/n/kriterii-kachestva-raboty-klassifikatorov

10. Solovyev V., Solnyshkina M., Ten A., Prokopiev N. A BERT-Based Classification Model: The Case of Russian Fairy Tales// Journal of Language and Education DOI: https://doi.org/10.17323/jle.2024.24030

11. Chastikova V.A., Zherlicyn S.A., Mityugov A.I. Tekhnologii iskusstvennogo intellekta v informacionnoj bezopasnosti. Monografiya. – Izd-vo FGBOU VO «KubGTU», 2024. - 315 s.

12. Chastikova V.A., Kozachyok K.V. Primenenie nejronnyh setej v platforme reagirovaniya na incidenty kak effektivnoe sredstvo upravleniya kiberbezopasnost'yu // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2023. № 4 (50). S. 70-76.

**ЧАСТИКОВА Вера Аркадьевна,** кандидат технических наук, доцент, доцент кафедры кибербезопасности и защиты информации ФГБОУ ВО «Кубанский государственный технологический университет». 350000, г. Краснодар, ул. Красная, 135. E-mail: chastikova_va@mail.ru

**КОЗАЧЁК Константин Валерьевич,** аспирант кафедры кибербезопасности и защиты информации ФГБОУ ВО «Кубанский государственный технологический университет». 350000, г. Краснодар, ул. Красная, 135. E-mail: Koza4ek.Konstantin@yandex.ru

**СОГОМОНЯН Ева Кареновна,** студент ФГБОУ ВО «Кубанский государственный технологический университет». 350000, г. Краснодар, ул. Красная, 135. E-mail: evo4ka.673@bk.ru

**ЛУГОВОЙ Дмитрий Алексеевич,** студент ФГБОУ ВО «Кубанский государственный технологический университет». 350000, г. Краснодар, ул. Красная, 135.E-mail: dmitrijlugovoy@gmail.com

**СЕРЫЙ Никита Викторович,** студент ФГБОУ ВО «Кубанский государственный технологический университет». 350000, г. Краснодар, ул. Красная, 135. E-mail: SS21102003@yandex.ru

C**HASTIKOVA Vera Arkadyevna,** Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Cybersecurity and Information Protection of the Kuban State Technological University. 350000, Krasnodar, Krasnaya street, 135. E-mail: chastikova_va@mail.ru

**KOZACHOK Konstantin Valerievich,** post-graduate student of the Department of Cybersecurity and Information Protection of the Kuban State Technological University. 350000, Krasnodar, Krasnaya street, 135. E-mail: Koza4ek.Konstantin@yandex.ru

**SOGOMONYAN Eva Karenovna,** student of the Federal State Budgetary Educational Institution of Higher Education "Kuban State Technological University". 350000, Krasnodar, Krasnaya street, 135. E-mail: evo4ka.673@bk.ru

**LUGOVOY Dmitry Alekseevich,** student of the Federal State Budgetary Educational Institution of Higher Education "Kuban State Technological University". 350000, Krasnodar, Krasnaya street, 135. E-mail: dmitrijlugovoy@gmail.com

**SERIY Nikita Viktorovich,** student of the Federal State Budgetary Educational Institution of Higher Education "Kuban State Technological University". 350000, Krasnodar, Krasnaya street, 135. E-mail: SS21102003@yandex.ru