



НАУЧНЫЙ АСПЕКТ

na-journal.ru

2023

№4

TOM 15

УДК 001.8(082)

ББК 1

Н 34

Периодичность – 12 раз в год

Свидетельство ПИ № ФС 77-84349

ISSN 2226-5694

Состав ред. коллегии и сведения об учредителе
приведены на сайте <https://na-journal.ru>

Н 34 НАУЧНЫЙ АСПЕКТ № 4 2023. – Самара: Изд-во ООО «Аспект»,
2023 . – Т15 . – 152 с.

Журнал «Научный аспект» является научным изданием и отражает результаты научной деятельности авторов по различным дисциплинам в области гуманитарных, естественных и технических наук.

УДК 001.8(082)

ББК 1



Почтовый адрес: 420100 г. Казань а/я 9

Официальный сайт: <https://na-journal.ru>

Электронная почта: public@na-journal.ru

Подписано к печати 23.05.2023

Бумага ксероксная. Печать оперативная. Заказ № .

Формат 60×84 /16. Объем 9,12 п.л. Тираж 100 экз.

Отпечатано в типографии «Куранты»

г. Казань, Сибирский тракт, 34к14, оф. 317, тел. +7 (843) 216-12-71

Содержание

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Климов И. С.

Методы машинного обучения для обнаружения дефектов программного обеспечения.....1811

Захаров М. А., Маранин А. Ю.

Особенности распределенной экспертной системы поиска нарушений техники безопасности методом видеоанализа.....1821

Захаров М. А., Маранин А. Ю.

Модель знаний экспертной системы поиска нарушений техники безопасности методом видеоанализа.....1830

Яльгин Д. Ю.

Сравнительный анализ OSINT-инструментов для проверки информации на достоверность.....1838

Григорьева А. А., Муклаев С. М.

Автоматизация отчетности Confluence с помощью Python.....1861

Потехина Е. В., Купцова К. М.

Система электронного документооборота как элемент цифровизации предприятия.....1869

Головизов Д. И.

Важность, факторы, подходы, обобщенная модель оптимизации расписания в высших учебных заведениях.....1876

Головизов Д. И.

Обзор видов ограничений и различных методов планирования и оптимизации расписания в учебных заведениях.....1882

Порошин Д. О.

Инновации и их значимость в современном мире.....1888

Юрасова Е. В.

Оптимизация качества дорожной инфраструктуры через метеорологическое обеспечение и использование аддитивных технологий.....1893

Капустин Н. Д.

Модель нарушителя и система объектовой безопасности на примере компании “АЛРОСА”.....1898

Егорова А. Л.

Оценка рисков информационной безопасности.....1907

Репетий Е. О.

Способы мошенничества в интернете.
Методы распознавания интернет-мошенничества.....1917

Клейменова Н. В., Кесян А. Р.

Методология управления проектами в рамках реализации ИТ-проекта по разработке информационно-аналитической системы на базе VI-решения на примере инжинирингового предприятия в нефтегазовой отрасли.....1923

Ильин И. С.

Анализ влияния особенностей языка текстового контейнера на возможности использования стеганографии.....1932

Галямин Д. С., Анিকেева А. А.

Возможности и перспективы использования технологии GPT-4 в консалтинге.....1939

ГЕОЛОГИЯ

Месба М. Х.

Минералогия медного месторождения Айнак в Афганистане.....1947

Қурманчук Н. С.

Методика планирования газодинамических исследований скважин на газоконденсатных месторождениях.....1953

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.052

Методы машинного обучения для обнаружения дефектов программного обеспечения

Климов Илья Сергеевич

студент Московского государственного технического университета

***Аннотация:** В данной статье рассмотрены и проанализированы основные методы машинного обучения с целью обнаружения дефектов программного обеспечения (далее — ПО), описаны метрики и проведено сравнение методов машинного обучения для обнаружения дефектов ПО. Также проведена формализация задачи обнаружения дефектов ПО в виде диаграммы в нотации IDEF0. В результате к наиболее эффективным методам машинного обучения отнесены алгоритм случайного леса и бустинг, как его модификация. Однако, в определенных условиях целесообразно применение таких методов машинного обучения, как наивный байесовский классификатор и метод опорных векторов.*

***Abstract:** This paper reviews and analyzes the main machine learning methods for software defect detection, describes the metrics and compares machine learning methods for software defect detection. The paper also formalizes the problem of software defect detection as a diagram in IDEF0 notation. As a result, the most effective methods of machine learning include the random forest algorithm and boosting as its modification. However, under certain conditions it is appropriate to use such machine learning methods as naive Bayesian classifier and support vector method.*

***Ключевые слова:** дефект, искусственный интеллект, машинное обучение, обнаружение, методы.*

***Keywords:** defect, artificial intelligence, machine learning, detection, methods.*

К одному из эффективных методов обнаружения дефектов ПО относится машинное обучение, которое можно отнести к категории искусственного интеллекта, позволяющего имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма)

и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Важность машинного обучения возрастает не только в исследованиях, имеющих отношение к компьютерным наукам, но и в нашей *повседневной жизни*. Оно позволяет пользоваться фильтрами почтового спама, удобным ПО распознавания текста и речи, распознаванием лиц, поисковыми механизмами.

Прогнозирование дефектов ПО является важной частью цикла разработки программного продукта. Ведь наличие дефектов сильно влияет на надежность, качество и стоимость обслуживания. Прогнозирование модулей с ошибками до развертывания повышает общую производительность [1]. Знание о компонентах, содержащих наибольшее число дефектов, позволяет распределить ресурсы тестирования так, чтобы в первую очередь проверялись компоненты с высокой вероятностью наличия дефектов. Сложно составить правила при поиске дефектов, так как могут встретиться совершенно разные ошибки, поэтому довольно известными являются методы машинного обучения, которые решают данную проблему, обучаясь на примерах. Исследователи применяли различные алгоритмы для решения данной задачи. На рисунке 1 представлена общая схема процесса обучения модели обнаружения дефектов ПО.

Первым шагом построения модели является создание и идентификация положительных и отрицательных образцов из набора данных. Каждый образец может представлять собой программный компонент, файл исходного кода, класс или функцию в зависимости от выбранной степени детализации.



Рисунок 1. Процесс обучения модели обнаружения дефектов ПО

Экземпляр имеет метрики и метки, которые указывают, склонен он к дефектам или нет. Затем они передаются в модель машинного обучения для обучения. Наконец, обученная модель может классифицировать различные фрагменты кода как ошибочные или безопасные на основе закодированных знаний [1].

Для обучения моделей во многих статьях [2–7] используются классические алгоритмы машинного обучения такие, как дерево решений, алгоритм случайного леса, градиентный бустинг, метод опорных векторов, наивный байесовский классификатор [1], решающие задачу классификации. Приведем описание каждого из них.

Наивный байесовский классификатор

Наивный байесовский классификатор — простой классификатор, основанный на применении теоремы Байеса с наивным предположением о независимости. Для каждого класса рассчитывается вероятность по теореме Байеса — формула (1), и объект d считается принадлежащим классу c_j ($c_j \in C$), если при этом классе достигается наибольшая апостериорная вероятность: $\max_c P(c_j|d)$. Для рассматриваемой задачи имеются два класса в зависимости от того, есть дефект в программе или нет.

$$P(c_j|d) = \frac{P(d|c_j)P(c_j)}{P(d)} \approx P(d|c_j)P(c_j), \quad (1)$$

где $P(d|c_j)$ — вероятность того, что объект d принадлежит классу c_j ; $P(c_j)$ и $P(d)$ — априорные вероятности класса c_j и объекта d (последняя не влияет на выбор класса и может быть опущена).

Если же сделать «наивное» предположение, что все признаки, описывающие классифицируемые объекты, не связаны друг с другом, то $P(d|c_j)$ можно вычислить как произведение вероятностей встретить признак x_i ($x_i \in X$) среди объектов класса c_j :

$$P(d|c_j) = \prod_{i=1}^{|X|} P(x_i|c_j). \quad (2)$$

На практике при умножении малых вероятностей может наблюдаться потеря значащих разрядов. В связи с этим применяют логарифмы вероят-

ностей. Так как логарифм — монотонно возрастающая функция, то класс c_j с наибольшим значением логарифма вероятности останется наиболее вероятным. Тогда решающее правило принимает следующий вид:

$$c^* = \operatorname{argmax}_c \left[\log P(c_j) + \sum_{i=1}^x P(x_i | c_j) \right]. \quad (3)$$

Несмотря на простоту, наивные байесовские классификаторы могут иметь достаточно высокую точность и производительность по сравнению с другими алгоритмами. К достоинствам также можно отнести малое количество данных, необходимых для обучения [8].

Метод опорных векторов

В случае решения задачи методом опорных векторов рассматривается задача классификации на два непересекающихся класса, в котором объекты описываются мерными вещественными векторами. Необходимо найти и построить гиперплоскость вида: $w^T x + b = 0$, разделяющую объекты на два подмножества с максимальной граничной областью. В случае линейной разделимости — построение сводится к решению задачи условной оптимизации, которая с помощью методов Лагранжа может быть сведена к задаче квадратичного программирования. Однако в реальных задачах такое встречается крайне редко. Для решения линейно неразделимых задач обычно применяют два подхода:

1. Ослабить жесткие ограничения, что приводит к так называемой «мягкой» граничной области — позволяет некоторым точкам нарушать ограничения стандартного метода. В частности, вводятся дополнительные переменные для учета количества ошибок классификации.
2. Применить ядерные функции для линеаризации нелинейных задач — идея заключается в определении ядерной функции, основанной на скалярном произведении данных как нелинейного перехода от пространства входных данных к пространству с большим количеством измерений с целью сделать задачу линейно разделимой. В результате использование ядерных функций делает алгоритм нечувствительным к размерности пространства [9].

Дерево решений

Деревья решений зачастую применяются в задачах классификации — принимается решение о принадлежности объекта к одному из непересекающихся классов. Деревья состоят из вершин, в которых записываются проверяемые условия (признаки), и листьев, в которых записаны ответы дерева (один из классов). Обучение состоит в настройке условий в узлах дерева и ответов в его листьях с целью достижения максимального качества классификации.

Пусть заданы конечное множество объектов $X = \{x_1, \dots, x_L\}$ и алгоритмов $A = \{a_1, \dots, a_D\}$ и бинарная функция потерь $I: A \times X \rightarrow \{0,1\}$. $I(a, x) = 1$ тогда и только тогда, когда алгоритм допускает ошибку на объекте x . Число ошибок алгоритма a на выборке X определяется как $n(a, x) = \sum_{x \in X} I(a, x)$.

Частота ошибок алгоритма на выборке определяется как $\nu = \frac{n(a, x)}{|x|}$. Под

качеством классификации понимается частота ошибок алгоритма на контрольной выборке.

Преимущества:

- интерпретируемость — позволяют строить правила в форме, понятной эксперту;
- автоматический отбор признаков — признаки в вершины дерева выбираются автоматически из набора признаков;
- управляемость — если некоторые примеры классифицируются неправильно, можно заново обучить только те вершины дерева, из-за которых это происходит. Кроме того, при тренировке разных поддеревьев могут оказаться более эффективными разные алгоритмы обучения.

Недостатки:

- зависимость от сбалансированности обучающих примеров — при неправильных пропорциях классов в обучающей выборке дерево обучится некорректно;
- требуются методы предотвращения переобучения — явление переобучения возникает из-за излишней сложности модели, когда обучаю-

щих данных недостаточно. При их нехватке высока вероятность выбрать закономерность, которая выполняется только на этих данных, но не будет верна для других объектов;

- экспоненциальное уменьшение обучающей выборки — так как после обучения каждой вершины дерева происходит разделение на два подмножества, то на каждом следующем уровне дерева обучающее множество вершины содержит все меньше и меньше примеров [10].

Алгоритм случайного леса

Проблема переобучения, возникающая при использовании дерева решений, может быть решена лесом решений — несколько деревьев, при этом результат определяется путем голосования.

Пусть имеется множество деревьев решений, каждое из которых относит объект $x \in X$ к одному из классов $c \in Y$. Считаем, что если $f_c^t(x) = 1$, то дерево t относит объект $x \in X$ к одному из классов c . При использовании алгоритма простого голосования для каждого класса подсчитывается число деревьев, относящих объект к данному классу — формула (4).

$$G_c(x) = \frac{1}{T_c} \sum_{t=1}^{T_c} f_c^t(x), c \in Y. \tag{4}$$

Ответом леса является тот класс, за который подано наибольшее число голосов:

$$\alpha(x) = \operatorname{argmax}_{c \in Y} G_c(x). \tag{5}$$

Если обучать деревья на одном и том же множестве тренировочных примеров одним и тем же методом, получатся одинаковые или очень похожие деревья. Поэтому для достижения независимости ошибок деревьев, составляющих лес решений, применяются специальные методы [10].

Бустинг

Бустинг — модификация алгоритма случайного леса, обучение происходит путем последовательного обучении нескольких моделей для повы-

шения точности всей системы. Выходным данным отдельных деревьев присваиваются веса. Затем неправильным классификациям из первого дерева решений присваивается больший вес, после чего данные передаются в следующее дерево. После многочисленных циклов бустинг объединяет «слабые» классификаторы в один алгоритм [11].

Существуют две основные разновидности бустинга: адаптивный и градиентный.

Адаптивный бустинг (англ. AdaBoost)

Одна из самых ранних реализаций бустинга, которая адаптируется и самостоятельно корректирует классификаторы в каждой итерации бустинга. Тренировочным примерам назначаются веса w_1^1, \dots, w_m^1 . Так как они имеют

вероятностную природу, для них выполняется условие: $\sum_{j=1}^m w_j^1 = 1, w_j^1 \in$.

Начальное распределение весов является равномерным. Происходит обучение первого дерева, с помощью которого производится классификация тренировочных примеров. Веса правильно классифицированных примеров снижаются, неправильно — повышаются. Следующее дерево строится с учетом обновленных весов, и так далее до достижения заданного количества деревьев или требуемой ошибки классификации [10].

Градиентный бустинг (англ. Gradient Boosting)

Похож на адаптивный бустинг, разница состоит в том, что он не присваивает неправильно классифицированным элементам больший вес. Вместо этого модель градиентного бустинга оптимизирует функцию потерь, используя градиентный спуск, в результате чего текущая базовая модель всегда становится эффективнее предыдущей. Градиентный бустинг пытается сразу генерировать точные результаты, а не исправлять ошибки [11].

Как правило, результаты классификации помечаются как положительные (имеются дефекты) и отрицательные (дефекты отсутствуют). Для оценки качества работы полученных моделей используются различ-

ные метрики. Так, в статьях [3–7] при сравнении результатов рассматриваются такие метрики, как *ассигасу*, точность (*precision*), полнота (*recall*) и *F-мера*. Для их определения используется матрица ошибок, которая содержит 4 ячейки:

- верно-положительные объекты (TP) — объекты, которые были верно классифицированы как положительные;
 - верно-отрицательные объекты (TN) — объекты, которые были верно классифицированы как отрицательные;
 - ложно-положительные объекты (FP) — объекты, которые были ложно классифицированы как положительные;
 - ложно-отрицательные объекты (FN) — объекты, которые были ложно классифицированы как отрицательные.
1. *Ассигасу* (точность) — широко используемая метрика, представляет собой отношение всех правильных прогнозов к общему числу предсказанных образцов (формула (6)). В ряде задач (с неравными классами) метрика может являться неинформативной.

$$\text{accuracy} = \frac{TP + TN}{TP + TN + FP + FN}. \quad (6)$$

2. *Precision* (точность) — это доля прогнозируемых положительных результатов, которые действительно относятся к этому классу, от всех положительно предсказанных объектов — формула (7).

$$\text{precision} = \frac{TP}{TP + FP}. \quad (7)$$

3. *Recall* (полнота) — пропорция всех верно-положительных предсказанных объектов к общему количеству действительно положительных (формула (8)). Чем выше значение полноты, тем меньше положительных примеров пропущено в классификации.

$$\text{recall} = \frac{TP}{TP + FN}. \quad (8)$$

4. *F-measure* (*F-мера*) — взвешенное гармоническое среднее полноты и точности (формула (9)). Этот показатель демонстрирует, как много

объектов классифицируется моделью правильно, и сколько истинных экземпляров она не пропустит [12].

$$F - \text{measure} = \frac{\text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}} \quad (9)$$

Для сравнения рассмотренных методов использованы результаты, описанные в статьях [2–7]. Модели обучались на данных, представленных в репозитории NASA [13]. Язык программирования, преобладающий в данных, — C++. В таблице 1 отображены средние арифметические значения для каждой из метрик по всем наборам данных.

Таблица 1. Сравнительная таблица результатов работы алгоритмов

Алгоритмы \ Метрики	Accuracy (точность)	Precision (точность)	Recall (полнота)	F-measure (F-мера)
Наивный байесовский классификатор	0.795	0.845	0.803	0.849
Метод опорных векторов	0.841	0.901	0.879	0.902
Дерево решений	0.823	0.845	0.878	0.889
Алгоритм случайного леса	0.847	0.903	0.883	0.903
Градиентный бустинг	0.845	0.859	0.863	0.890
Адаптивный бустинг	0.835	0.858	0.861	0.889

Таким образом, по каждой из метрик алгоритм случайного леса показал наивысший результат. Можно сделать вывод, что его применение является наиболее выгодным для рассматриваемой задачи. Однако хочется отметить, что результаты моделей бустинга несильно отличаются. Благодаря использованию ансамблю моделей и большому варьированию параметров при обучении, данный алгоритм имеет высокую перспективу использования.

Список литературы

1. Sharma, T. A Survey on Machine Learning Techniques for Source Code Analysis [Текст] / T. Sharma, M. Kechagia, S. Georgiou, R. Tiwari, I. Vats, H. Moazen, F. Sarro. — 2022. — С. 11–13.

2. Assim, A. Software Defects Prediction using Machine Learning Algorithms [Текст] / A. Assim, Q. Obeidat, M. Hammad // 2020 International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI) — 2020. — С. 1–6.
3. Shah, M. Software Defects Prediction Using Machine Learning [Текст] / M. Shah, N. Pujara — 2020. — С. 1–5.
4. Iqbal, A. Performance Analysis of Machine Learning Techniques on Software Defect Prediction using NASA Datasets [Текст] / A. Iqbal, S. Aftab, U. Ali, A. Husen // International Journal of Advanced Computer Science and Applications — 2019. — С. 1–6.
5. Aleem, S. Comparative performance analysis of machine learning techniques for software bug detection / S. Aleem, L. F. Capretz, F. Ahmed — 2015. — С. 1–9.
6. Cetiner, M. A Comparative Analysis for Machine Learning based Software Defect Prediction Systems [Текст] / M. Cetiner, O. K. Sahingoz // 11th International Conference on Computing, Communication and Networking Technologies — 2020. — С. 1–7.
7. Bhandari, G. P. Machine learning based software fault prediction utilizing source code metrics [Текст] / G. P. Bhandari, R. Gupta // IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), Kathmandu (Nepal) — 2018 — С. 1–6.
8. Шитиков, В. К. Классификация, регрессия, алгоритмы Data Mining с использованием R [Текст] / В. К. Шитиков, С. Э. Мاستицкий // Тольятти, 2017.
9. Федотов, Д.В. О решении задачи классификации методом опорных векторов [Текст] / Д. В. Федотов // Математические методы моделирования, управления и анализа данных — 2013 — С. 1–3.
10. Кафтанников, И. Л. Особенности применения деревьев решений в задачах классификации [Текст] / И. Л. Кафтанников, А. В. Парасич // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника» — 2015. — С. 26–32.
11. Amazon Web Services. Что такое бустинг? [Электронный ресурс]: Режим доступа URL: <https://aws.amazon.com/ru/what-is/boosting/> (Дата обращения 23.11.2022).

12. Дудченко, П. В. Метрики оценки классификаторов в задачах медицинской диагностики [Текст] / П. В. Дудченко // Молодежь и современные информационные технологии: сборник трудов XVI Международной научно-практической конференции студентов, аспирантов и молодых ученых — 2019. — С. 164–165.
13. NASA. Promise software engineering repository [Электронный ресурс]: Режим доступа URL: <http://promise.site.uottawa.ca/SERepository/datasets-page.html> (Дата обращения: 29.11.2022).

УДК 004.891

Особенности распределенной экспертной системы поиска нарушений техники безопасности методом видеоанализа

Захаров Михаил Александрович

преподаватель кафедры Компьютерных систем и сетей
Московского государственного технического университета им. Н. Э. Баумана

Маранин Александр Юрьевич

магистрант Московского государственного технического университета
им. Н. Э. Баумана

***Аннотация:** В работе приводятся необходимые функции для программной экспертной системы, способной определять моменты нарушения техники безопасности на предприятии методом видеоанализа. Рассмотрены основные причины производственного травматизма. Предложены распределенная архитектура экспертной системы видеомониторинга, необходимый обслуживающий персонал и пользователи системы.*

***Abstract:** The paper provides the necessary functions for a software expert system capable of identifying moments of safety violations in the enterprise by video analysis. The main causes of occupational injuries are considered. The distributed architecture of the expert video monitoring system, the necessary maintenance personnel and users of the system are proposed.*

***Ключевые слова:** экспертная система, видеомониторинг, техника безопасности, распределенная архитектура.*

Keywords: expert system, video monitoring system, safety, distributed architecture.

Введение

На предприятиях 96% нарушений требований техники безопасности происходит из-за опасного поведения персонала или человеческого фактора, и лишь 4% — из-за опасных условий труда [1]. Каждая травма — это беда для сотрудника, его семьи и коллег по работе. Вывод из строя ключевого сотрудника может существенно замедлить выполнение проекта. Таким образом основной целью производственной безопасности является нулевой травматизм. Крупные организации для обеспечения производственной безопасности устанавливают большое количество видеокамер, которые могут использоваться для видеонаблюдения за сотрудниками, производственным процессом, а также опасными объектами. Записываемые материалами системами видеонаблюдения требуют регулярного просмотра и анализа для выявления нарушений до появления последствий.

Из многочисленных опытов по психологии и наблюдению за сотрудниками обеспечения безопасности можно сделать вывод: после 20 минут наблюдения всего за одной камерой видеонаблюдения внимание пользователя-оператора системы видеомониторинга притупляется, и он оставляет без внимания приблизительно 90–95% активных сцен, на которых могут произойти случаи нарушения техники безопасности на наблюдаемых объектах. Постепенно системы видеонаблюдения становятся более крупными, разветвленными, число камер видеонаблюдения увеличивается, при этом слежение за видеопотоком и анализ происходящих событий в ручном режиме для персонала сложно и дорого.

Анализ предметной области, основные причины производственного травматизма

Основными причинами производственного травматизма на опасных объектах предприятий могут быть:

- падение на поверхности одного уровня;
- падение с большой высоты;

- дорожно-транспортные происшествия;
 - электротравма (поражение электрическим током);
 - падение предмета на пострадавшего;
 - взаимодействие сотрудников с движущимися предметами, конструкциями, деталями;
 - противоправные действия сотрудников, различные другие неклассифицированные факторы;
 - ожоги (термические, электрические, химические, лучевые и др).
- Некоторые способы превентивного избежания несчастных случаев:
1. Регулярное доведение до сотрудников требований техники безопасности, проведение практических занятий по оказанию медицинской помощи.
 2. Падение на поверхности одного уровня — избавление от неровностей и загрязнений поверхности (ям, гололеда, луж), а также лишних предметов на пути;
 3. Падение с высоты — установка указателей, ограничительных барьеров, применение ремней и тросов безопасности;
 4. Дорожно-транспортные происшествия — использование общественно-го или специального транспорта, запрет использования личного транспорта, регулярная проверка правил дорожного движения у сотрудника, отслеживание пути сотрудника до места работы, установка тахографов для соблюдения дистанции пройденного пути и времени вождения;
 5. Взаимодействие сотрудников с движущимися предметами, конструкциями, деталями — контроль нахождения сотрудников вблизи опасных объектов и их аварийное отключение;
 6. Электротравма — использование перчаток, устранение открытых источников возможного контакта наэлектризованных объектов с сотрудником;
 7. Падение предмета на пострадавшего — ношение защитных касок.

Основные требования к разрабатываемой системе

Необходимо разработать решение, которое способно интеллектуально анализировать видеозаписи и видеопотоки в реальном времени и опре-

делять моменты, как предшествующие нарушениям, так и сами нарушения, чтобы можно было сработать на опережение несчастных случаев на производстве. Для этих целей лучше всего подходят экспертные системы, способные временно заменить специалиста-эксперта по технике безопасности. Экспертные системы через модуль накопления собирают собственную базу знаний, основанную на фактах и правилах, получая знания от экспертов по технике безопасности и инженеров по знаниям.

Основной набор функций экспертной системы видеомониторинга, способной заранее реагировать на возможные несчастные случаи на предприятии:

- Распознавание объектов, классификация и определение наличия средств индивидуальной защиты. Машинное зрение предоставляет возможности распознавания объектов, ставя в соответствие обнаруженный объект определенному классу. На промышленных производствах такими классами могут быть: работники предприятия, механизмы, техника. Машинное зрение определит наличие специального защитного снаряжения и экипировки, такие как каски, жилеты, перчатки, одежды. В системе могут присутствовать определенные правила для контроля заранее классифицированных объектов.
- Одним из наиболее распространенных функций видеоаналитики является модуль, позволяющий отслеживать движение объекта (сотрудника), а также анализировать его действия. Анализ может заключаться в контроле пересечения заданной линии, подсчете количества пересечений линии на входе и на выходе, нахождение сотрудника в заранее заданном квадрате на рабочем месте.
- Функция, близкая по смыслу к «пересечению линии», является «обнаружение присутствия в зоне». В этом случае система не только детектирует наличие объекта, но возможно задание промежутков времени нахождения или отсутствия в зоне. Таким образом, например, система может контролировать нахождение сотрудника в рабочей зоне, это может быть востребовано для рабочих для которых рабочее место точно определено.
- Увеличение количества устанавливаемых видеокамер наблюдения на предприятии требует пропорционального увеличения вычислительных

ресурсов, возможна установка специализированного вычислительного центра мониторинга, на котором обрабатываются как старые видеозаписи, так и видеопотоки, поступающие в реальном времени.

Решением могут быть как использование специализированных камер с внутренней аналитикой, или создание кластера вычислительных машин для обработки информации.

Первый способ требует настройки каждой камеры по отдельности, система становится менее централизованной. Обычно настройка одной камеры сложности не представляет и не требует специальной квалификации или знаний. С ростом количества камер ручная настройка усложняется. Использование специализированных камер с внутренней аналитикой не требует единого вычислительного центра. На сегодняшний день генерируемая ими информация довольно скудна, поэтому получив её, оператор в любом случае должен иметь возможность оценить изображение самостоятельно [3, с. 47].

Второй способ предполагает ввод в эксплуатацию дополнительных вычислительных машин, подключенных к основной сети. Возникают сложности с развертыванием специализированного программного обеспечения на новых машинах, настройка для работы в совместном режиме требует опыта работы с подобными системами. Развертывание экспертной системы таким образом может быть осуществлено вручную, включающее в себя установку и настройку программного обеспечения на каждый из узлов кластера вычислительного центра, либо возможно использование специального программного обеспечения для автоматизации развёртывания и управления приложениями с использованием контейнеров. Примером такой системы является Docker, позволяющий «упаковать» приложение и его окружение. Для управления группой контейнеров могут использоваться оркестраторы Docker Swarm или Kubernetes. Подобные системы просты в установке, позволяют решать базовые задачи для управления контейнерами, настроить виртуальную сеть между всеми узлами вычислительного кластера:

- Для реализации экспертной системы требуется разработка специальной модели знаний продукционного, фреймового или семантического типа. Плохая проработка модели знаний приводит к неудачной реали-

зации экспертной системы, что может выражаться в затруднении добавления новой информации и правил в систему, уменьшается технологичность системы, т.е. изменение такой системы может потребовать перепроектирования всей системы в целом.

- Для анализа поступившей информации необходима специальная система журналирования, фиксирующая все случаи нарушения требований техники безопасности в текстовом, фото или видео форматах. Настройки журналирования для каждой камеры наблюдения и сцены могут быть различными. В одних случаях достаточно зафиксировать факты нарушения техники безопасности записью в текстовом журнале, в другом — сохранить запись для последующего анализа и выяснения причин, которые привели к нарушению. Анализ журналов позволяет собирать статистику и превентивно проводить мероприятия (инструктажи и практические занятия) для предотвращения несчастных случаев. Также система журналирования увеличивает информационную безопасность системы в целом: используя журналы всегда можно определить, какие сотрудники и с какими целями получали доступ к данным.
- Для корректной работы системы журналирования необходима система для хранения информации, в которую входит программное обеспечение, видеархив, база знаний и основные базы данных, используемые программным обеспечением системы. Информацию следует хранить в нескольких датацентрах и использовать механизмы репликации данных для увеличения сохранности информации и балансировки нагрузки, запросов на запись и чтение.
- Экспертная система видеонаблюдения может иметь систему оповещения, т.е. иметь возможность отправлять мгновенные уведомления (push-уведомления) о случаях нарушения техники безопасности, недопустимых ситуациях на подконтрольных объектах как пользователю-оператору, так и сотрудникам-нарушителям.
- В экспертную систему должен быть встроен модуль тестирования, для проверки корректной работы системы согласно регламентам тестирования и технического обслуживания. Тестированию подлежат алгоритмы обнаружения, классификации и сопоставления объектов, исправ-

ность камер видеонаблюдения, работоспособность вычислительного центра, контроль выполнения заданных экспертом по технике безопасности правил, непротиворечивость правил и фактов модели знаний, а также комплексное тестирование системы. Тесты могут выполняться на регулярной основе как в строго определенное время, так и в наименее загруженные часы работы. Результаты могут сохраняться в виде журналов тестов для последующего анализа.

При выборе камер следует использовать современные цифровые IP-камеры. Цифровая IP-видеокамера отличается от аналоговой видеокамеры тем, что не только позволяет преобразовывать видеосигнал в цифровую форму, но и обеспечивает его одновременную передачу по IP-сети для последующего воспроизведения и/или сохранения [2, с. 140]. Использование подобных камер становится экономически оправданным в тех случаях, когда на предприятиях уже развернута локальная компьютерная сеть и есть другая физическая инфраструктура для ее функционирования.

Возможная архитектура распределенной экспертной системы видеомониторинга

Архитектура экспертной системы может быть монолитной или распределенной (сервисно-ориентированной или микросервисной).

Разработка программного обеспечения с монолитной архитектурой требует меньше затрат по времени и ресурсам, но при росте системы, могут возникнуть сложности с быстродействием. В конечном итоге приложение с монолитной архитектурой упрется в потолок определенного количества камер видеонаблюдения, которое оно может поддерживать. При дальнейшем увеличении камер существенно уменьшится точность работы всей системы и скорость реагирования на случаи нарушения техники безопасности.

Распределенная архитектура требует больших ресурсов на разработку, появляются дополнительные сложности при настройке, связывании распределенных узлов вычислительного кластера, развертывании, распределении нагрузки и комплексном тестировании системы. В случае распределенной архитектуры, ограничение масштабируемости системы зависят

только от каналов передачи информации. На рисунке 1 приведена возможная распределенная архитектура системы.

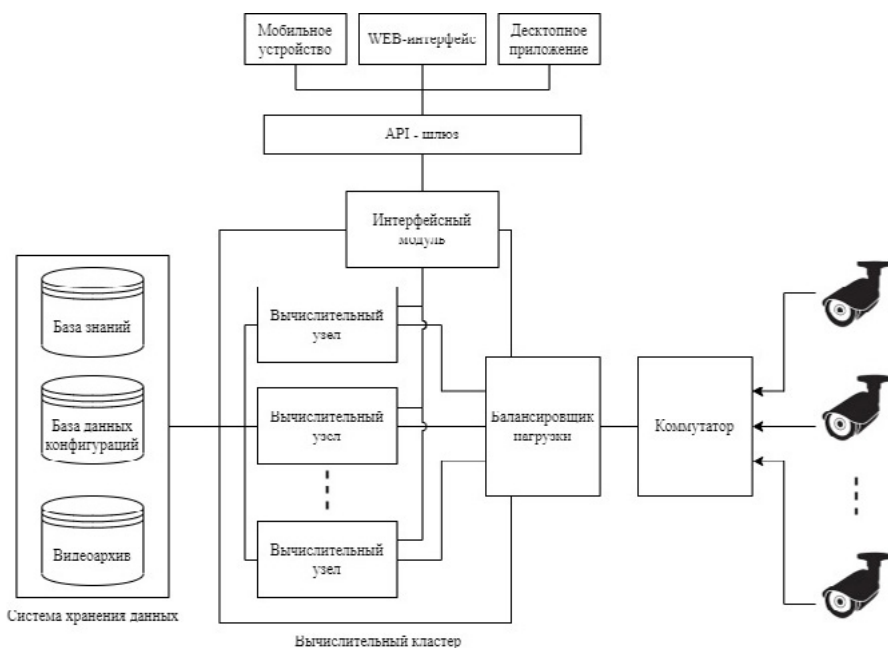


Рисунок 1. Распределенная архитектура экспертной системы

В базе данных могут храниться данные о пользователях системы, техническая информация о камерах видеонаблюдения, основные настройки программного обеспечения. В базе знаний — правила, факты и другая информация, необходимая механизму логического вывода для принятия решений.

Взаимодействие с системой возможно через мобильные, десктопные приложения, веб-интерфейс. API-шлюз позволяет установить единые стандарты запросов и ответов клиентов системы и облегчает дальнейшую разработку интерфейса. Модуль накопления знаний, оповещения и объяснения также могут взаимодействовать с разными группами пользователей через интерфейсный модуль.

Обслуживающий персонал и основные пользователи системы

Для корректной работы экспертной системы поиска нарушений техники безопасности необходим обслуживающий персонал для установки оборудования, развертывания и первоначальной настройки системы:

1. Монтажники для прокладки сетевых кабелей и установки камер видеонаблюдения, подготовки помещения для размещения вычислительного центра.
2. Системные администраторы для развертывания и настройки системы мониторинга.

Пользователи экспертной системы:

1. Эксперты-профессионалы по технике безопасности используют модуль накопления знаний экспертной системы и вносят основные правила, факты, конфигурации, занимаются разметкой линий и зон контроля, выделяют классы объектов слежения и реакцию системы на сработанные правила;
2. Инженеры по знаниям, используя записанные материалы из видеоархива, формируют новые датасеты, дорабатывают типовые наборы данных для увеличения точности алгоритмов классификации и обнаружения объектов, а также помогают экспертам формализовать их знания для последующего ввода в систему;
3. Операторы-наблюдатели, чью работу призвана сделать более продуктивной экспертная система видеомониторинга.

Заключение

Учитывая постоянный рост количества камер видеонаблюдения и сложность ручной обработки и анализа видеопотоков на предприятиях и опасных объектах, введение в эксплуатацию экспертных систем с распределенной архитектурой интеллектуального видеомониторинга является наиболее эффективным способом предотвращения производственного травматизма.

Список литературы

1. Зайцева С. О ситуации с безопасностью на площадках «Росатома», 2018 [Электронный ресурс] URL: <https://strana-rosatom.ru/2018/12/12/o-situacii-s-bezopasnostju-na-ploshhadk/> (дата обращения: 13.03.2023).
2. Пескин А. Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации.— 2-е изд., перераб. и доп. — М.: Горячая линия. — Телеком, 2021.— 368 с.: ил.
3. Торстен А. Видеоаналитика: мифы и реальность, 2-е переиздание / А. Торстен, И. Келлер, Х. Лутц. — М.: Секьюрити Фокус, 2019.— 186 с.: цв.ил. (Серия «Энциклопедия безопасности»).

УДК 004.891

Модель знаний экспертной системы поиска нарушений техники безопасности методом видеоанализа

Захаров Михаил Александрович

преподаватель кафедры Компьютерных систем и сетей
Московского государственного технического университета им. Н. Э. Баумана

Маранин Александр Юрьевич

магистрант Московского государственного технического университета
им. Н. Э. Баумана

***Аннотация:** В работе рассматриваются основные модели знаний экспертных систем: продукционная модель, фреймовая модель. Предложена схема фреймовой модели экспертной системы поиска нарушений техники безопасности методом видеоанализа.*

***Abstract:** The paper considers the basic knowledge models of expert systems which are product model and frame model. The scheme of the frame model of expert system for search of safety violations with video analysis method is proposed.*

***Ключевые слова:** экспертная система, продукционная модель знаний, фреймовая модель знаний, фреймы, техника безопасности, видеомониторинг.*

Keywords: *expert system, knowledge production model, knowledge frame model, frames, safety precautions, video monitoring system.*

Введение

Основной целью производственной безопасности на предприятиях является нулевой травматизм сотрудников. Крупные организации устанавливают разветвленные системы видеомониторинга для обнаружения случаев нарушения техники безопасности сотрудниками, производственным процессом и опасными объектами. Подобные системы помогают превентивно проводить мероприятия для предотвращения нарушений и способны значительно уменьшить последствия несчастных случаев.

Для анализа видеозаписей и приходящих видеопотоков в реальном времени лучше всего подходят экспертные системы, способные временно заменить специалиста-эксперта по технике безопасности. Основной отличительной особенностью экспертных систем от других автоматизированных систем является возможность накопления знаний и опыта в некоторой узкоспециализированной предметной области и в пределах этой области принимать решения на уровне профессионала.

База знаний, типы знаний

В системах видеомониторинга входными данными являются видеопотоки с камер, механизмами — модуль принятия решений экспертной системы, эксперты по технике безопасности, операторы-наблюдатели и инженеры по знаниям. Управление системы осуществляется базой знаний и наборами данных алгоритмов классификации объектов. На рисунке 1 приведена контекстная диаграмма экспертной системы видеомониторинга в нотации IDEF0.

Одним из основных компонентов экспертной системы является база знаний. База знаний хранит знания в формализованном виде. Под знаниями понимают различные правила, факты и другую информацию о свойствах сущностей. На основе знаний могут быть порождены новые знания. Мощность экспертной системы определяется мощностью базы

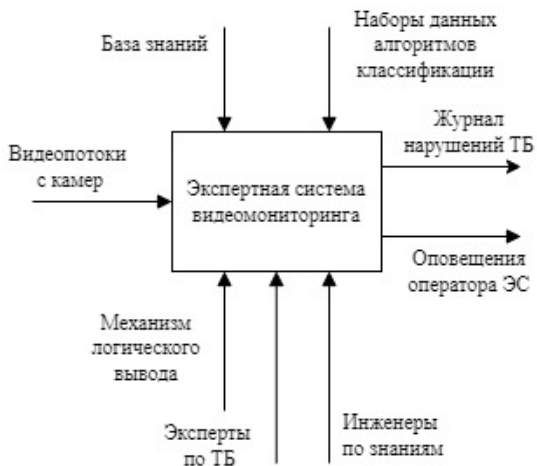


Рисунок 1. Контекстная диаграмма экспертной системы видеомониторинга

знаний и способностью получать, структурировать и использовать эти знания. Плохая проработка модели знаний может привести к неудачной реализации и низкой технологичности экспертной системы, в таком случае для модификации или добавлении новых знаний может потребоваться перепроектирование всей системы в целом.

Эксперты-специалисты в своей профессиональной деятельности принимают решения на интуитивном уровне, поэтому не всегда могут четко сформулировать свои знания. Знания могут передаваться в текстовом, звуковом, изобразительном виде, а также в виде жестов. Формализацией знаний обычно занимаются инженеры по знаниям, и вносят знания в систему, используя модуль накопления знаний экспертной системы.

Обычно в экспертных системах используются модели знаний трех типов: продукционная модель, фреймовая модель и семантические сети.

Под продукционной моделью понимают представление знаний при помощи фактов и правил.

Общий вид правил продукции:

$R \text{ is } \langle i, Q, P, A \rightarrow B, N \rangle$, где

R — знак правила;

i — имя правила;

Q — сфера применения правила;

$A \rightarrow B$ — ядро правила;

P — условие применимости ядра продукции;

N — постусловие продукции.

При этом ядра продукции могут быть детерминированные и недетерминированные. В детерминированных ядрах при актуализации ядра и при выполнении условия продукции выполнение постусловия обязательно. В недетерминированных — выполнение условия необязательно.

Общий вид механизма логического вывода можно представить в виде:

$S = (F, R, I)$, где

F — факты;

R — правила;

I — интерпретатор (решатель).

Решатель можно представить в виде:

$I = (V, M, C, W)$, где

V — механизм выбор активных фактов и правил;

M — процесс сопоставления;

C — процесс разрешение конфликтов при возникновении ситуаций противоречивости правил;

W — механизм выполнения означенного правила.

Недостатком продукционной модели является сложность проверки всех правил на непротиворечивость. Продукционную модель знаний обычно используется в небольших экспертных системах, количество правил в которых не превышает одну тысячу.

Семантические сети представляют собой модели знаний, в основе которых лежат понятия сетей, образованных с помощью вершин и дуг. Вершины в семантических сетях являются фактами или сущностями, дуги — предикаты, связывающие факты вместе.

Модель знаний, составленную из семантических сетей, обычно применяют для синтаксических и семантических анализаторов. Не все знания возможно представить с помощью семантических сетей. Для принятия решений в процессе поиска нарушений техники безопасности при обработке видеопотоков семантические сети сложно применимы.

Под фреймовой моделью знаний обычно понимают знания, представленные с помощью фреймов и шаблонов.

Фрейм — это отдельные единицы представления знаний, некий формальный шаблон, соответствующий событию, явлению или событию. Фрейм представляет собой структуру, в которой есть слоты для хранения других знаний. Имя фрейма также является знанием. У каждого слота есть имя и значение. Также у слота может быть присоединительная процедура, выполняющие какие-либо вычисления для конкретизации слота.

В общем виде фрейм можно представить:

F is $\{N(u_1, q_1, p_1), \dots, (u_n, q_n, p_n)\}$, где

F — знак фрейма;

N — имя фрейма;

u_i — имя слота;

q_i — значение слота;

p_i — присоединительная процедура;

n — количество слотов в фрейме.

Одной из важных особенностей фреймов является возможность “незаполнения” слотов. Слоты могут быть заполнены уже во время работы системы в реальном времени для конкретизации этого фрейма. Значением слотов могут быть данные, факты, другие фреймы и семантические сети [2, с. 355].

Для означивания фреймов может использоваться конъюнкция всех или части конкретизированных слотов, конкретизация определяющий слотов (по достаточному принципу), высчитыванием суммарного веса конкретизированных слотов. Группы семантически близких друг к другу фреймов объединены в систему фреймов [3, с. 7].

С помощью фреймовой модели можно представить все многообразие знаний о мире через: фреймы-структуры, фреймы-роли, фреймы-сценарии, фреймы-ситуации [1, с. 169]. Фреймы представляют собой процедурно-декларативные структуры, с помощью которых удобно описать предметную область, связанную с поиском нарушений техники безопасности.

Основным недостатком фреймовой модели является сложность изменения сети фреймов.

Схема фреймовой модели знаний экспертной системы

Эксперт вносит знания в экспертную систему, используя модуль накопления знаний. Вводимые знания включают в себя информацию о зонах, классифицируемых объектах (людях или механизмах), а также правила сопоставления зон и обнаруженных объектов.

Информация о зонах включает в себя:

- графическую информацию (разметку) зон, собранную при использовании интерфейсных инструментальных средств или выбором сегментов, на которые разделена сцена;
- класс зоны;
- дополнительные параметры зон, такие как пользовательское название зоны, цвет или описание.

Информация об обнаруженных объектах включает в себя:

- класс обнаруженного объекта, который может быть механизмом или человеком;
- дополнительные свойства объекта, такие как наличие средств индивидуальной защиты (защитных касок, перчаток, жилеты), особенности покраски.

Все фреймы объектов, зон и правил включают в себя уникальный номер фрейма, задаваемый системой автоматически.

Информация о правилах включает в себя:

- номер выбранной зоны;
- класс обнаруженного объекта;
- возможные дополнительные свойства объекта;
- постусловие (действие, выполняемое после выполнения ядра продукции).

На рисунке 2 изображена схема фреймовой модели экспертной системы видеомониторинга.

Для определения класса объекта используется модуль классификации. Подобный модуль может строиться на базе механизмов искусственных нейронных сетей или машинного обучения. Область машинного зрения предоставляет широкие возможности обнаружения и распознавания объектов, ставя в соответствие обнаруженным объектам определенные классы. Для корректной работы алгоритмов машинного зрения требуется спе-

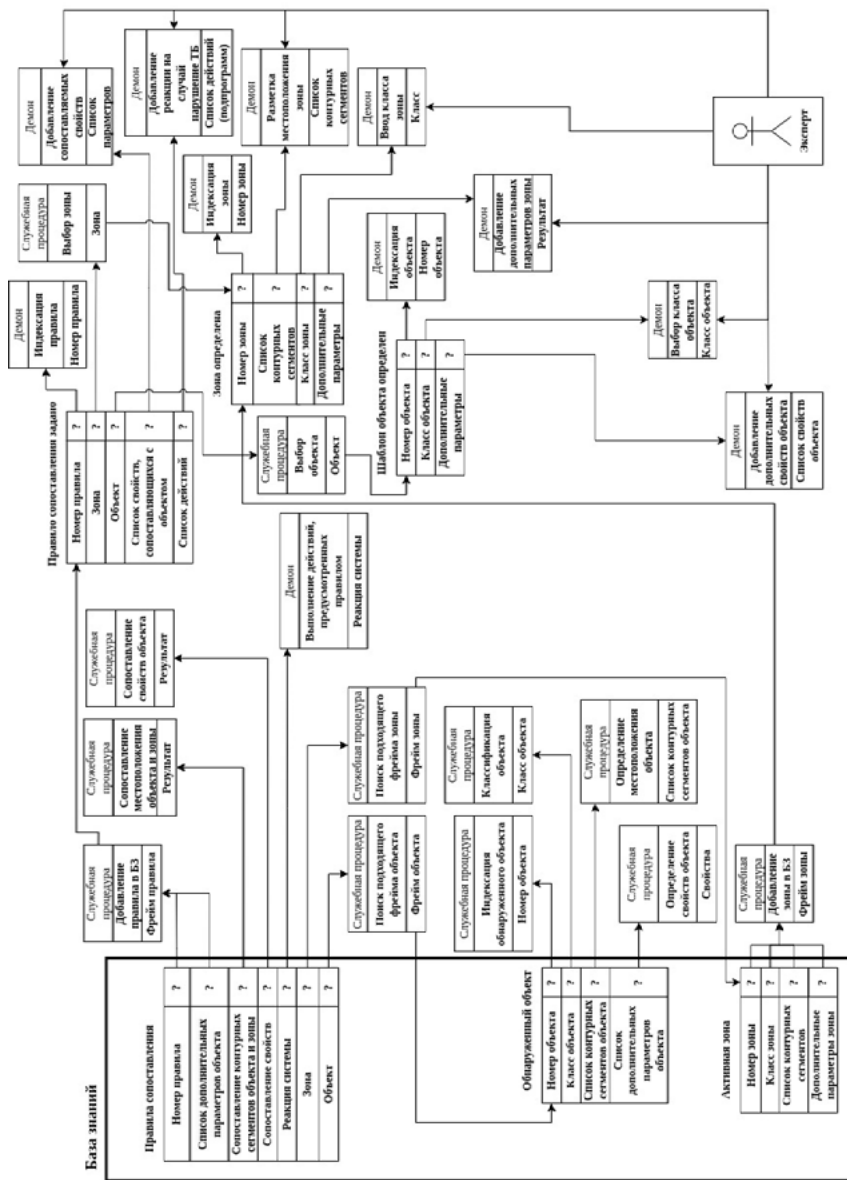


Рисунок 2. Схема фреймовой модели экспертной системы видеомониторинга

циально настроенный набор данных (датасет) для поиска нужных системе классов объектов.

Каждый обнаруженный объект представляет собой фрагмент знаний — факт. Модуль классификации пытается распознать класс этого объекта и его дополнительные свойства. Если класс объекта — человек, то дополнительными свойствами может быть наличие средств индивидуальной защиты (защитные каска и перчатки, жилет). После определения свойств объекта слоты фрейма заполняются и фрейм объекта конкретизируется.

Система постоянно проверяет фреймы правил, пытаясь найти соответствие между конкретизированными фреймами объектов и фреймов с размеченными зонами. При срабатывании фрейма-правила выполняется присоединительная процедура, заданная экспертом. Присоединительной процедурой может быть запись в журнал, сохранение кадра изображения или короткой видеозаписи, а также оповещение оператора наблюдателя.

Заключение

При разработке базы знаний экспертной системы видеомониторинга наиболее подходящими способами представления знаний является продукционная модель фреймовая модель знаний. Продукционная модель подходит для небольших систем с малым (до одной тысячи) количеством правил. Фреймовая модель подходит для больших систем, модификация модели знаний которых не планируется.

Список литературы

1. Гаврилова Т. А. Инженерия знаний. Модели и методы: учебник для вузов / Т. А. Гаврилова, Д. В. Кудрявцев, Д. И. Муромцев. — 6е изд., стер. — Санкт-Петербург: Лань, 2023. — 324 с.: ил. — Текст: непосредственный.
2. Минский М. Машина эмоций / Марвин Минский [перевод с английского В. Дегтяревой, А. Курышевой]. — Москва: Издательство АСТ, 2020. — 512 с.
3. Минский М. Фреймы для представления знаний: Пер. с англ. — М.: Энергия, 1979. — 152 с., с ил.

УДК 004

Сравнительный анализ OSINT-инструментов для проверки информации на достоверность

Ялыгин Дмитрий Юрьевич

студент Московского института электроники и математики им. А. Н. Тихонова
Национального исследовательского университета «Высшая школа экономики»

***Аннотация:** В статье приведено описание результатов сравнительного анализа 16 OSINT-инструментов для проверки информации на достоверность по 16 критериям. Автором статьи сделаны выводы на основании данных, представленных в четырех таблицах.*

***Abstract:** The paper describes the results of a comparative analysis of 16 OSINT tools for validation of information according to 16 criteria. The author of the article draws conclusions based on the data presented in four tables.*

***Ключевые слова:** OSINT, фактчекинг, достоверность информации.*

***Keywords:** OSINT, fact-checking, information reliability.*

Введение

Сегодня вопрос использования проверенной данных и надежных источников стоит особенно остро, так как на фоне большого потока информации в СМИ, социальных сетях и мессенджерах растет проблема распространения дезинформации. Данная проблема оказывает сильное воздействие на мышление, восприятие и действия разных людей. Для ее решения необходимо использовать критический подход и проводить оценку потребляемой информации.

Проверка информации — сложный трудоемкий процесс, который включает в себя множество аспектов, начиная от сбора и фильтрации информации, заканчивая анализом проверяемой информации и вынесением вердикта о ее достоверности. Традиционно такой проверкой занимаются журналисты и специалисты в области бизнес-разведки, которые выполняют этапы этого процесса либо полностью вручную, либо с использованием средств автоматизации, к которым относятся OSINT-инструменты.

OSINT (от англ. Open Source Intelligence) — аббревиатура, обозначающая разведку по открытым источникам [1].

OSINT-инструменты — это различные средства, в том числе программные и аппаратные, позволяющие автоматизировать, упростить и ускорить различные этапы проверки на достоверность информации, получаемой из открытых источников.

В настоящее время по всему миру насчитывается почти 400 инструментов проверки информации, однако в России таких средств практически нет [2]. В рамках исследования проблемы разработки OSINT-инструмента в целях повышения качества и эффективности проверки информации на достоверность был проведен сравнительный анализ, который позволил выявить сходства, различия, технические ограничения, трудности реализации и использования подобных инструментов.

Входные данные сравнительного анализа

Для проведения сравнительного анализа были выбраны 16 наиболее популярных ресурсов для проверки информации на достоверность. Сравнение проводилось на основании 16 критериев и в 4 этапа:

- выбор и сбор общих сведений об инструментах, попавших в выборку;
- оценка функциональных возможностей инструментов и UX/UI-дизайна;
- оценка степени автоматизации и выявление особенностей проверки информации на достоверность при использовании каждого из перечисленных инструментов;
- выявление зависимости используемых методов анализа информации на достоверность и заявленного режима проверки информации.

Результаты сравнительного анализа представлены в таблицах 1, 2, 3 и 4. В таблице 1 отражены общие сведения о каждом инструменте в том числе:

- статус ресурса и ссылка на него;
- режим обновления (или дата последнего обновления);
- языки проверки информации;
- назначение (как заявлено разработчиками каждого инструмента);
- тематика проверяемой информации;

- тип инструмента / платформы.

В таблице 2 отражены критерии, обобщающие функциональные возможности и аспекты, оказывающие влияние на пользовательский опыт взаимодействия с перечисленными инструментами:

- наличие описания механизма работы инструмента;
- наличие инструкции пользователя для работы с инструментом;
- заявленные функциональные возможности инструмента;
- наличие обучающего контента (обучение методам борьбы с дезинформацией);
- указанный тип лицензии или стоимость.

В таблице 3 представлены критерии, позволяющие подробно описать механизм организации проверки информации на достоверность с помощью инструментов, участвующих в сравнении:

- режим проверки информации;
- этапы проверки, которые проводятся в автоматическом режиме;
- входные и выходные данные проверки информации;
- наличие обоснования результатов проверки;
- основной показатель (показатели) оценки информации;
- рейтинг оценки информации.

В таблице 4 указаны заявленные методы проверки и анализа информации для каждого инструмента в соответствии с режимом проверки:

- режим проверки информации;
- методы проверки информации.

Общие сведения о сравниваемых OSINT-инструментах для проверки информации на достоверность

Несмотря на большое число средств для проверки информации на достоверность, как это было указано ранее, количество сравниваемых OSINT-инструментов оказалось ограниченным в связи с выявленными зависимостями между разными критериями сравнения. Другими словами, наличие 16 ресурсов оказалось достаточным для сравнения и формирования выводов, так как при дальнейшей оценке большего числа инструментов выявленные закономерности и тенденции повторялись.

Выбор конкретного перечня ресурсов, представленных в таблице 1, был определен их популярностью среди специалистов в области проверки информации и географией их разработки. Наибольшее число таких инструментов встречается в США, что можно объяснить исторической основой появления и развития OSINT-методологии, которая зародилась именно в этой стране [3].

Среди всех инструментов, вошедших в выборку для проведения сравнения, есть один неактивный проект — Emergent, который является одной из самых ранних разработок, направленных на автоматизацию проверки информации на достоверность. Данный ресурс был включен в список инструментов для оценки уровня развития разработок по данному направлению. Таким образом, можно сделать вывод о том, насколько сильно изменилась степень автоматизации и механизм процесса проверки с течением времени.

В основном все инструменты, участвующие в сравнении, имеют свежие обновления в виде выпуска новой версии инструмента или отчета о выполненной проверке информации на достоверность. Назначение большинства инструментов сводится к выполнению полного цикла проверки информации на достоверность, однако есть ряд ресурсов, с помощью которых можно выполнять только определенные этапы данного процесса (например, определение степени распространенности информации, фильтрация и тегирование сообщений). Кроме того, ряд ресурсов, в рамках использования которых проверка осуществляется полностью вручную, представляют собой проекты, нацеленные на формирование сообществ, активно борющихся с дезинформацией.

Большая часть сравниваемых инструментов осуществляет проверку информации в СМИ и сообщений в социальных сетях в основном на английском языке по теме политики. При этом есть уникальные по проверяемой тематике и назначению проекты, как, например, Fakespot, который предназначен для проверки отзывов на товары в интернет-магазинах.

Практически все инструменты представляют собой сайты с возможностью отправки пользователем запроса на проверку информации, но есть также отдельные ресурсы, допускающие их использование в качестве встроенных расширений браузеров или мобильных приложений на базе операционных систем iOS и Android.

Таблица 1. Сравнительный анализ OSINT-инструментов: общие сведения

№	Название инструмента	Страны	Язык проверки	Назначение	Тематика	Тип
1	AfricaCheck https://africacheck.org	ЮАР, Кения, Нигерия, Сенегал	Английский, французский	Проверка информации на достоверность, формирование сообщества для борьбы с дезинформацией	Публичные высказывания и информация в СМИ в Африке	Сайт
2	AIDR http://aidr.qcri.org	Катар	Английский, другие языки	Фильтрация, классификация сообщений из социальных сетей по тематике	Чрезвычайные ситуации, гуманитарные кризисы и помощь	Сайт
3	Meedan (проект Check) https://meedan.com/check	США	Английский, другие языки	Автоматизация процессов фактчекинга, в т.ч. валидация информации	Журналистика	Сайт + Чат-бот в WhatsApp
4	Chequeado http://chequeado.com	Аргентина	Испанский	Проверка информации на достоверность, формирование сообщества для борьбы с дезинформацией	Политика, экономика	Сайт
5	The Factual (бывш. CivicOwl) https://thefactual.com	США, Великобритания, Грузия	Английский	Проверка информации на информативность, фильтрация и тегирование информации	Сообщения в СМИ, новости различной тематики	Сайт, приложение на iOS/ Android, плагины для браузер Chrome
6	Emergent http://www.emergent.info	США	Английский	Проверка информации на достоверность, отслеживание обновлений сообщений	Новости на разные темы (политика, экономика и т.п.)	Сайт платформы

№	Название инструмента	Страны	Язык проверки	Назначение	Тематика	Тип
7	FactCheck.org https://www.factcheck.org	США	Английский	Отслеживание и проверка информации на достоверность, развенчание мифов	Политические новости и заявления в США, наука	Сайт
8	Fakespot https://www.fakespot.com	США	Английский	Проверка обзоров и продавцов в интернет-магазинах	Покупки в интернет-магазинах: Amazon, eBay, Walmart, Best Buy, Sephora, Shopify.	Плагин для браузера Mozilla Firefox, приложение на iOS/Android
9	FirstDraftNews Check https://chrome.google.com/webstore/detail/firstdraftnewscheck/japoскреааанknkhagilkgcle dflbfk	США	Английский	Проверка видеoinформации или изображений на предмет достоверности	Любые поисковые запросы в браузере	Плагин для браузера Chrome
10	FullFact https://fullfact.org/	Великобритания	Английский	Проверка информации на достоверность, формирование сообщества для борьбы с дезинформацией	Новости ЕС, политика, экономика, образование, преступления, иммиграция, законодательство, здравоохранение	Сайт, Набор инструментов фактчекинга
11	Hoaxy 2 Beta https://hoaxy.osome.iu.edu/	США	Разные языки (34 языка)	Проверка и отбражение степени распространения сообщений из соц.сети и обнаружение соц.ботов	Любая тематика сообщений из соц.сети Twitter	Сайт

Таблица 1 (продолжение)

№	Название инструмента	Страны	Язык проверки	Назначение	Тематика	Тип
12	InVID http://www.invid-project.eu/tools-and-services/invid-verification-plugin	США	Английский	Проверка видео информации и изображений на достоверность, инструмент в помощь журналистам для развенчivanja мифов	Любые поисковые запросы в браузере	Плагины для браузеров Chrome и Mozilla Firefox
13	Snores http://www.snores.com	США	Английский	Проверка информации на достоверность, развенчание мифов	Публичные высказывания, новости и информация в СМИ	Сайт
14	Truly Media http://www.truly.media	Греция, Германия	Английский	Проверка информации в социальных сетях на достоверность, инструмент для проверки информации журналистами	Любая тематика сообщений в соц.сетях	Сайт платформы
15	TrustServista https://www.trustservista.com	Румыния	Английский, другие языки	Проверка новостей и информации в социальных сетях на достоверность	Новости, любая тематика сообщений в соц.сетях	Сайт платформы, плагины для браузера Chrome, доступ через API
16	Лапша Медиа https://lapsha.media/	Россия	Русский	Проверка информации на достоверность, развенчание мифов	Новости на разные темы (политика, ЧС, культура, общество, экономика, здравоохранение и т.п.)	Сайт, боты в Viber, Telegram, ВКонтакте

Оценка функциональных возможностей OSINT-инструментов для проверки информации на достоверность

Как видно по данным, представленным в таблице 2, практически все инструменты имеют описание механизма работы и подробные инструкции пользователя. Большая часть инструментов доступна для пользователей на безвозмездной основе. Лишь отдельные проекты, которые предлагают в качестве инструментов мобильные приложения или сервисы, доступны платно с разовой оплатой доступа или по подписке.

Обучение методам борьбы с дезинформацией предлагают только те ресурсы, которые нацелены на формирование сообщества людей, мотивированных на критическое осмысление и проверку потребляемой ими информации. Такие ресурсы предлагают обучение в формате кратких видеоинструкций, памяток, статей с советами или тестов с элементами геймификации.

Наибольший интерес в таблице 2 представляет перечень функциональных возможностей каждого из инструментов, который зависит от степени автоматизации проверки информации на достоверность. Если инструмент представляет собой проект, в рамках которого процесс проверки осуществляется специалистами вручную, то, как правило, список возможностей будет ограничен формами отправки запросов на проверку и вопросов команде специалистов ресурса, а также поиском с фильтрацией по имеющей базе проверенной информации и отчетам о проверке. В данном случае сам процесс проверки остается для пользователя скрытым и неконтролируемым. В тех ситуациях, когда инструмент предлагает полную или частичную автоматизацию процесса проверки, перечень возможностей значительно шире и зависит от этапов процесса, которые подпадают под автоматизацию. Можно выделить следующие этапы процесса проверки информации на достоверность, которые могут быть автоматизированы за счет использования современных OSINT-инструментов:

- сбор и предобработка (фильтрация, тегирование, маркирование, категоризация, извлечение, обработка видео/ изображений) данных для проверки пользовательской информации;

Таблица 2. Сравнительный анализ OSINT-инструментов: функциональные возможности

№	Название OSINT-инструмента	Функциональные возможности	Обучение методам борьбы с дез(мис)информацией	Тип лицензии / Стоимость
1	AfisaCheck	<ul style="list-style-type: none"> – Формы отправки запроса на проверку утверждения и вопросы команде ресурса – Поиск информации с фильтрацией по надежным источникам и проверенной информации 	В формате видеозаписей, кратких памяток, тестов	бесплатно
2	AIDR	Невозможно проверить, т.к. доступны только после регистрации в соц.сетях Twitter, Facebook	Привлечение к участию в качестве MicroMappers (маркирующих сообщения)	открытая плат-форма, лицензия AGPL-3.0
3	Meedan (проект Check)	<ul style="list-style-type: none"> – Кастомизация чат-бота и меню на разных языках – Автоматизация категорий, обзоров и приоритизации ответов на запросы – Автоматизация публикаций в мессенджерах для распространения проверенной информации среди конечных пользователей 	–	не указано, доступна возможность запросить демо-версию

№	Название OSINT-инструмента	Функциональные возможности	Обучение методам борьбы с дез(ин)формацией	Тип лицензии / Стоимость
4	Chequeado	<ul style="list-style-type: none"> – Форма отправки запроса на проверку утверждения/ сообщения – Поиск по базе проверенных сообщений – Извлечение субтитров из видеозаписей 	<p>В формате видео-инструкций, подробных памяток и статей</p>	бесплатно
5	The Factual (бывш. CivicOwl)	<ul style="list-style-type: none"> – Отображение 5 самых актуальных тем новостей на каждый день – Отчет об оценке надежности (информативности) новости – Краткая справка по теме новостей – Отображение инфографики по наиболее популярным темам и надежным новостям – Просмотр обновляемого списка популярных новостей в режиме реального времени – Отображение временной линии с историей публикации различных новостей и обновлений по ним – Экран пользовательских настроек для контроля отображения новостей – Email рассылка 	<p>–</p>	условно-бесплатно (реклама в приложении)
6	Emergent	<p>Просмотр и поиск по фильмам результатов проверки сообщений на достоверность</p>	<p>–</p>	бесплатно

Таблица 2 (продолжение)

№	Название OSINT-инструмента	Функциональные возможности	Обучение методам борьбы с дез(мис)информацией	Тип лицензии / Стоимость
7	FactCheck.org	<p>Форма отправки запроса на проверку информации на достоверность, просмотр и поиск по проверенной информации</p>	—	бесплатно
8	Fakespot	<p>Плагина: — Поискная строка с фильтрацией по товарам/обзорам на просматриваемых сайтах магазинов. — Индикация статусов обзоров на товары и продавцов.</p> <p>Приложения: — Возможность покупки в разных интернет-магазинах из одного приложения с одновременной проверкой обзоров и продавцов выбранных товаров. — Фильтрация по надежным обзорам. — Сводная информация по статусам надежности товаров и продавцов.</p>	—	бесплатно

№	Название OSINT-инструмента	Функциональные возможности	Обучение методам борьбы с дез(мис)информацией	Тип лицензии / Стоимость
9	FirstDraftNews Check	Отображение индекса достоверности информации по показателям. Кнопка проверки для запуска функции проверки.	—	бесплатно
10	FullFact	<p>Сайта:</p> <ul style="list-style-type: none"> — Формы отправки запроса на проверку и вопросы команде ресурса — Поиск информации с фильтрацией по надежным источникам и проверенной информации — Информационная рассылка с проверенной информацией <p>ИИ-инструменты:</p> <p>невозможно проверить, доступ только для организаций</p>	3 онлайн курса обучения	Сайт — бесплатно, набор инструментов на базе ИИ — платно для коммерческого использования
11	Ноаху 2 Beta	Визуализация двух аспектов распространения сообщений в соц.сети: временные тенденции и сети распространения. Инструменты отображения: масштабирование, выбор временного интервала. Индикация оценки соц.ботов ценами.	—	бесплатно

№	Название OSINT-инструмента	Функциональные возможности	Обучение методам борьбы с дез(ин)формацией	Тип лицензии / Стоимость
12	InVID	<p>Отображение URL видео и изображений на веб-странице. Просмотр и проверка метаданных информации. Сегментация видео на ключевые кадры для их преобразования в нужный формат и поиска через поисковые сервисы Google, Yandex, TinEye, Vaidu. Поиск изображений через эти поисковые сервисы. Функции расширенного поиска в соц.сети Twitter по ключевым словам, по контрольному периоду, геолокации. Масштабирование изображений и видео с помощью алгоритма бикубической интерполяции для проведения анализа и экспертизы информации. Инструменты форензики для исследования контента видео или изображения и проверки информации.</p>	-	MIT-лицензия, бесплатно
13	Snopes	<p>Форма отправки запроса на проверку информации на достоверность, просмотр и поиск по проверенной информации</p>	Краткие советы и рекомендации	бесплатно

№	Название OSINT-инструмента	Функциональные возможности	Обучение методам борьбы с дез(ин)формацией	Тип лицензии / Стоимость
14	Truly Media	Создание потоков отслеживания контента социальных сетей (Twitter, Facebook, Youtube и др.), расширенный поиск, фильтрация данных, их сортировка по коллекциям и тегирование, создание общих рабочих пространств для организации совместной проверки информации и работы в режиме реального времени, импорт информации из памяти пользовательского устройства, инструменты визуализации (диаграммы, схемы), инструменты проверки (для определения месторасположения, поиска метаданных, поиска дополнительной информации и источников), создание и отслеживание работы над запросами на проверку	—	платно, доступна возможность запросить демо-версию
15	TrustServista	Многоязычный поиск информации, геополиск, автоматический перевод на английский язык, кластеризация тем для автоматического поиска сообщений, сортировка данных по результатам географического и тематического анализа, инструменты визуализации (графы, статистика), расширенный анализ и проверка контента любой веб-страницы, оценка достоверности новостей (анализ контекста, вероятность кликебейта, анализ источника, определение первоисточника)	—	платно, доступна возможность запросить демо-версию
16	Лапша Медиа	Форма отправки запроса на проверку информации на достоверность, просмотр и поиск по проверенной информации	В формате тестов	бесплатно

- расширенный поиск и просмотр результатов проверки;
- отображение проверенной информации и результатов проверки в структурированном виде при помощи встроенных инструментов визуализации (масштабирование, выбор временного интервала, интерактивная карта, инфографика, графы, статистика);
- выбор пользовательских настроек для мониторинга и кастомизации анализа информации на достоверность (выбор языка, выбор интересующей тематики, поиск и извлечение метаданных, встроенные инструменты форензики).

Следует отметить, что большинство исследуемых ресурсов представляет собой инструменты с конкретным перечнем функциональных возможностей. Отдельные проекты претендуют на звание полноценных платформ с расширенным функционалом для организации и автоматизации полного цикла проверки информации на достоверность. К таким проектам из числа сравниваемых можно отнести: Truly Media, Trust Servista, the Factual, FullFact.

Степень автоматизации и особенности проверки информации на достоверность при использовании OSINT-инструментов

Степень автоматизации работы инструментов, перечисленных в таблице 3, определяется в первую очередь режимом проверки информации на достоверность. В процессе исследования было выявлено 3 режима проверки:

- пользовательский режим (все этапы проверки выполняются специалистами вручную);
- автоматизированный режим (отдельные этапы выполняются автоматически, остальные — вручную);
- автоматический режим (полный цикл проверки выполняется автоматически).

Из 16 инструментов, участвующих в сравнении, 6 используют пользовательский режим проверки, 5 — автоматизированный, 5 — автоматический. Такой расклад доказывает наличие тенденции к автоматизации процесса проверки информации на достоверность. Однако далеко не все

проекты способны автоматизировать частично или полностью цикл проверки, что можно объяснить следующими причинами:

- низкие темпы цифровизации в развивающихся странах (например, страны Африки и Латинской Америки);
- высокая стоимость и трудоемкость проектов, нацеленных на разработку OSINT-инструментов, поддерживающих автоматический или автоматизированный режимы проверки;
- недостаточная реализация возможности контроля процесса проверки со стороны пользователя — для пользователя процесс анализа информации либо скрыт, либо неподконтролен (нет доступа к пользовательским настройкам);
- сложности реализации аналитической части инструмента.

Исходя из результатов сравнения, представленных в таблице 3, можно заметить, что для таких ресурсов, как AfricaCheck, Chequedo, свойственен пользовательский режим проверки на фоне активного формирования сообщества, нацеленного на критическое осмысление потребляемой информации. То, что недоступно в развивающихся странах в автоматическом или автоматизированном режимах, выполняется вручную.

Крупные проекты, имеющие автоматический режим работы, (такие как Truly Media, Trust Servista) предлагают только платное обслуживание, что связано с высокой стоимостью разработки (вплоть до 72 000 евро) [4].

Пользовательский режим проверки крайне трудоемок. У пользователя при таком режиме могут возникнуть сложности в проверке полученного результата и оценки степени объективности отчета по итогам выполненной оценки информации на достоверность. На качество полученного результата в таком режиме влияют:

- отбор и проверяемость информации (информация на проверку отбирается по критериям, а также проверяется, поддается ли оценке на достоверность полученная информация);
- время, затраченное на проверку;
- количество участников проверки и их квалификация в предметной области;
- успешное прохождение всех этапов проверки;
- объективность полученных результатов и вердикта по итогам проверки.

Таблица 3. Сравнительный анализ OSINT-инструментов: режимы и механизмы проверки информации на достоверность

№	Название инструмента	Режим проверки	Этапы проверки в автоматическом режиме	Показатель оценки информации	Рейтинг оценки информации
1	AfricaCheck	Пользовательский	—	достоверность	Верно/ неверно/ почти верно/ не доказуемо/ введение в заблуждение/ увеличение фактов/ преуменьшение фактов
2	AIDR	Автоматизированный	Сбор, фильтрация, тегирование (маркировка оценки степени ущерба от ЧС)	надежность сообщения в соц.сети	Надежное / ненадежное
3	Meedan (проект Check)	Автоматизированный	Формирование запроса; кластеризация данных; сортировка на базе пользовательских предпочтений; формирование, публикация и распространения обзора журналистов	—	—
4	Chequeado	Пользовательский	—	достоверность	Истина/ ложь/ вводит в заблуждение
5	The Factual (бывш. CivicOwl)	Автоматический	Фильтрация топовых новостей за контрольный период; анализ и тегирование новостей по степени информативности и надежности; вывод общей оценки информации и результатов проверки по разным показателям; вывод резюме с основной фактической информацией из новостей по теме, интересной пользователю	информативность, политическая направленность, качество сайта и источников, экспертиза автора публикации	Неинформативная/ умеренно-информативная/ очень информативная
6	Emergent	Автоматизированный	Сбор, классификация, отслеживание изменений сообщений	достоверность	Истина/ ложь/ не подтверждено/

№	Название инструмента	Режим проверки	Этапы проверки в автоматическом режиме	Показатель оценки информации	Рейтинг оценки информации
7	FactCheck.org	Пользовательский	—	достоверность	—
8	Fakespot	Автоматический	Фильтрация статусов надежности и тегирование обзоров на товары, продавцов, товаров в интернет-магазинах. Отображение результатов автоматической проверки в соответствии с запросом пользователя	достоверность обзоров; надежность продавцов	Разные статусы, например: «Обнаружен мошенник» (Scam-seller detected), «Ложный обзор» (Fake review).
9	FirstDraft NewsCheck	Автоматический	Расчет индекса достоверности видео или изображений и отображение результата расчета с подробным описанием	индекс достоверности видео или изображений	Процентное значение по показателям: Степень достоверности: оригинал или нет? Степень достоверности: подтверждение авторства? Контент видео/изображения: степень достоверности места, где сделано? Контент видео/изображения: степень достоверности даты, когда сделано?
10	FullFact	Пользовательский (сайт) Автоматизированный (ИИ)	Сбор и мониторинг данных; тегирование собранных данных; сопоставление утверждений; проверки в режиме реального времени	достоверность	Истина/ ложь/ верно/ неверно/ не подтверждено — нет доказательств

Таблица 3 (продолжение)

№	Название инструмента	Режим проверки	Этапы проверки в автоматическом режиме	Показатель оценки информации	Рейтинг оценки информации
11	Ноаху 2 Beta	Автоматический	Визуализация трендов, оценка сообщений из соц.сети, градация сообщений по типу сообщений, импорт/экспорт результатов в CSV и JSON форматах	уровень автоматизации учетной записи, типы сообщений	Градация цветом (5 оттенков цвета) от «Похоже на бота» (Bot like) до «Похоже на человека» (Human like) Градация цветом (5 оттенков цвета): ретвиты, упоминания, ответы, цитаты, разное
12	InVID	Автоматизированный	Сбор данных и метаданных, обработка изображений и видео, поиск, фильтрация, расширенный поиск	достоверность	Выводы о достоверности информации делаются пользователем самостоятельно
13	Snopes	Пользовательский	—	достоверность	Проверка в процессе / истина/ по большей части правда/ смесь истины и лжи/ по большей части ложь/ ложь/ необоснованное утверждение/ не доказуемо/ устарело/ некорректно/ правильная атрибуция/ неправильная атрибуция/ миф/ мошенничество/ законодательство/ сатира/ изначально было сатирой/ отзыв/ утерянные мифы

№	Название инструмента	Режим проверки	Этапы проверки в автоматическом режиме	Показатель оценки информации	Рейтинг оценки информации
14	Ttuly Media	Автоматизированный	Сбор, сортировка, тегирование данных и метаданных, расширенный поиск, фильтрация, интеграция различных инструментов, необходимых журналисту для проведения проверки (GoogleMaps, TinEye, WolframAlpha, Google Reverse Image Search, Yandex, Snopes, Pipl) и др.)	статус проверки	Вердикт достоверности определяется пользователем самостоятельно, изменяется только статус выполнения задачи на проверку (наименование статусов пользователь назначает сам)
15	TrustServista	Автоматический	Анализ контекста проверяемой информации, оценка достоверности, кластеризация, категоризация, сортировка, тегирование, визуализация данных, полный цикл проверки	достоверность	Процентное значение по показателям: качество контента; вероятность кликбейта; эмоциональная окрасченность; общий уровень достоверности
16	Лапша Медиа	Пользовательский	—	достоверность	Публикация только разоблаченных «фейковых» новостей и сообщений

Реализация аналитической части OSINT-инструмента для проверки информации на достоверность представляет особую сложность из-за выбора:

- показателей для оценки,
- градации (рейтинга) достоверности,
- методов для расчета показателей оценки информации.

Согласно данным в таблице 3 можно сделать вывод о том, что инструменты в одних и тех же режимах могут проверять разные показатели (например, не только достоверность, но и информативность, надежность источников, уровень автоматизации учетной записи — автор сообщения — бот или человек). Кроме того, у одного показателя может насчитываться до 19 степеней (уровней), как это реализовано в инструменте Snopes.

Аналитические методы в OSINT-инструментах для проверки информации на достоверность

Выбор методов анализа информации по выбранным показателям зависит от реализуемого режима проверки, как это показано в таблице 4, а также от типа информации и целей проверки. Если при пользовательском режиме очевидно, что все процессы осуществляются вручную командой экспертов, то в автоматическом и автоматизированном методы могут различаться.

По итогам проведенного сравнительного анализа можно выделить группы аналитических методов, которые используются в автоматическом и автоматизированном режимах:

- методы обработки естественного языка, которые позволяют извлекать информацию из неструктурированных текстовых данных и выделять утверждения и факты;
- алгоритмы машинного обучения, которые могут быть использованы для обучения системы на проверенных данных для выявления закономерностей и отличительных черт истинных и ложных утверждений;
- графы знаний, которые представляют собой структурированное представление информации для выявления противоречий;
- экспертные правила, которые представляют собой наборы правил для логического вывода для автоматического тегирования ложной информации;

- гибридные методы, которые сочетают в себе несколько методов и подходов для организации более качественной проверки информации.

Следует отметить, что последняя группа методов мало где реализуется. Как правило, OSINT-инструменты ограничиваются только одним набором методов, и лишь в немногих ресурсах используется сочетание методов.

Таблица 4. Сравнительный анализ OSINT-инструментов: методы

№	Название OSINT-инструмента	Режим проверки информации	Заявленные методы проверки информации на достоверность
1	AfricaCheck	Пользовательский	Проверка осуществляется вручную
2	AIDR	Автоматизированный	NLP, методы фильтрации сообщений (по словам и темам), Human-Based Computation (вычисления с использованием человеческих ресурсов на определенных шагах процесса вычисления)
3	Meedan (проект Check)	Автоматизированный	NLP, методы, основанные на (экспертных) правилах, анализ на сходства, методы категоризации, обзора и приоритизации утверждений на проверку
4	Chequeado	Пользовательский	Проверка осуществляется вручную
5	The Factual (бывш. CivikOwl)	Автоматический	Методы и алгоритмы машинного обучения
6	Emergent	Автоматизированный	Базовые методы машинного обучения
7	FactCheck.org	Пользовательский	Проверка осуществляется вручную
8	Fakespot	Автоматический	Методы и алгоритмы машинного обучения
9	FirstDraft NewsCheck	Автоматический	Не указаны
10	FullFact	Пользовательский (сайт)	На сайте проверка осуществляется командой вручную. С помощью ИИ-инструментов проверка осуществляется на базе методов машинного обучения, но с участием и контролем со стороны пользователя
		Автоматизированный (инструменты ИИ)	
11	Ноаху 2 Beta	Автоматический	Графы знаний (в т.ч. декомпозиция k-ядра)

Таблица 4 (продолжение)

12	InVID	Автоматизированный	Автоматический поиск, сбор и фильтрация информации, обработка видео и изображений
13	Snopes	Пользовательский	Проверка осуществляется вручную
14	Truly Media	Автоматизированный	Автоматический поиск, сбор, сортировка, тегирование и фильтрация информации
15	TrustServista	Автоматический	NLP, графы знаний, семантическое сравнение
16	Лапша Медиа	Пользовательский	Проверка осуществляется вручную

Выводы

Проведенный сравнительный анализ OSINT-инструментов для проверки информации на достоверность показал, что современные средства такого типа не совершенны и требуют доработки. Кроме того, поскольку в России ощущается острая нехватка подобных ресурсов, необходима разработка OSINT-инструмента с учетом полученных результатов сравнения. Для повышения качества и эффективности процесса проверки информации на достоверность разрабатываемый OSINT-инструмент должен соответствовать ряду требований, в числе которых:

- поддержка русского языка и сбора информации в российском сегменте Интернета;
- гибкость инструмента за счет предоставления пользователю возможности выбора режима использования (пользовательский/ автоматизированный/ автоматический);
- гибкость инструмента, достижимая за счет предоставления пользователю возможности внесения изменений в настройки процесса проверки информации;
- использование гибридных методов анализа информации при проверке на достоверность;
- возможность выбора пользователем показателей для проверки, методов анализа и создания собственного рейтинга достоверности информации.

Список литературы

1. Сайт поисковой системы по словарям и энциклопедиями «Академик» [Электронный ресурс]: <https://academic.ru/> (дата обращения: 12.02.2023).
2. Сайт Duke Reporters' LAB [Электронный ресурс]: <https://reporterslab.org/fact-checking/> (дата обращения: 12.02.2023).
3. Воксанаев В. П. Разведка по открытым источникам: уроки прошлого/ ISBN: 5–93550–188–5/ Рязань: Поверенный — 2007 г., 174 с.
4. Сайт Newtral [Электронный ресурс]: <https://www.newtral.es/automated-fact-checking/> (дата обращения: 15.02.2023).

УДК 65.011.54

Автоматизация отчетности Confluence с помощью Python

Григорьева Анна Алексеевна

бакалавр Национального исследовательского университета
«Высшая школа экономики»

Муклаев Сабур Мергенович

магистр Национального исследовательского университета
«Высшая школа экономики»

***Аннотация:** При работе с Confluence самой распространенной задачей, требующей автоматизации, является необходимость регулярно автоматически обновлять данные. В статье описаны методы автоматического обновления содержимого страницы, чтения и дополнения содержимого страницы, добавления вложений. Предложены примеры реализации методов чтения, редактирования и добавления вложений. Статья предлагает практический взгляд на решение задачи автоматизации процессов с помощью Confluence. На каждом этапе описанного процесса автоматизации предложены рекомендации разработчику, которые были выработаны исходя из практики применения исследуемых методов.*

***Abstract:** When working with Confluence, the most common task that requires automation is the need to update data automatically on a regular basis. This article describes methods for automatically updating page content, reading, and appending page content, and adding*

attachments. It offers examples of how to implement methods of reading, editing, and adding attachments. The article offers a practical view on solving the task of process automation with Confluence. Each step of the automation process described includes recommendations to the developer which have been developed based on the practice of the methods under study.

Ключевые слова: автоматизация бизнес-процессов, Atlassian Confluence, Python, FastAPI, Atlassian Python API, Windows Task Scheduler.

Keywords: business process automation, Atlassian Confluence, Python, FastAPI, Atlassian Python API, Windows Task Scheduler.

Поддерживать актуальность наполнения страницы проекта на Confluence тем важнее, чем больше участников в проекте. Существует библиотека методов Python для работы с Confluence, позволяющих автоматизировать работу с содержимым страниц таким образом, чтобы решать широкий пласт регулярных задач, с которыми встречаются специалисты в самых разных отраслях, в короткие сроки.

Цель: определить подход к автоматизации отчетности Confluence с помощью Python.

Объект исследования: автоматизация корпоративных бизнес-процессов.

Предмет исследования: методы и средства автоматизации процессов обработки, анализа и визуализации данных с помощью Confluence и Python.

Методы исследования: анализ, синтез.

Часть сущности страницы Confluence, отвечающая за отображаемую приложением визуализацию, хранится в параметре *body* [1,2]. Эта часть представляет собой HTML разметку. С *body* можно ознакомиться в контекстном меню, в пункте “View Storage Format”. Суть обновления страницы Confluence так или иначе состоит в манипуляциях с *body*. В случаях работы со вложениями ссылка на них в *body* не меняется при обновлении версии вложения без изменения его имени.

Большую часть самых распространенных задач автоматизации можно решить за три шага:

1. Чтение (если требуется интерактивное взаимодействие с содержимым);
2. Запись обновленного *body*;

3. Добавление вложений (если требуется обновление файлов или изображений).

Чтение содержимого страницы. Любая работа с сервисами Confluence помощью `python` начинается с объявления элемента аутентификации (Рис. 1).

```

1  from atlassian import Confluence
2
3  confluence = Confluence(
4      url="", #подставить адрес корпоративного сервера
5      username="", #подставить логин
6      password="", #подставить пароль
7  )
8

```

Рисунок 1. Объявление элемента аутентификации

Для идентификации страницы используется связка пространства (`space`) и `id` страницы (`page_id`). И то, и другое можно увидеть в явном виде в URL адресе страницы, открыв её в браузере. Если возникли сложности с определением имени пространства, можно воспользоваться функцией (Рис. 2).

```
space = confluence.get_page_space(page_id)
```

Рисунок 2. Функция определения имени пространства

Чтение `body` предлагается проводить напрямую вызовом `get request` (Рис. 3). Существует стандартная функция получения сущности страницы в `python`, однако велика вероятность обнаружить в ней только информацию о `body`, без самого содержимого.

Далее следует парсинг содержимого `body`. Мы рекомендуем разработчику организовать размещение и редактирование пользователем интерактивной части информации на странице в таблицах и заранее

```

9 import requests
10
11
12 def get_html(pageId, confluence):
13     contentApiUrl = '/rest/api/content'
14     requestUrl = '{confluenceBaseurl}/{contentApiurl}/{pageid}?expand=body.storage'.format(confluenceBaseurl = confluence.url,
15                                                                                       contentApiurl = contentApiUrl,
16                                                                                       pageid = pageId)
17     requestResponse = requests.get(requestUrl, auth=(confluence.username, confluence.password))
18     return requestResponse.json()['body']['value']
19
20
21 html = get_html(123456789, confluence)

```

Рисунок 3. Чтение body

[3,4]. В таком случае возможно получение всей необходимой информации функцией `pandas.read_html`. Положительные стороны такого подхода особенно проявляются при проведении множества проектов по автоматизации страниц Confluence параллельно, так как в противном случае придется реализовывать несколько уникальных парсеров, вместо одного унифицированного. Если размещение интерактивной части в табличном формате невозможно, то следует рассмотреть использование библиотеки `bs4` (класс `BeautifulSoup`) или регулярные выражения (библиотека `re`).

Запись обновленного `body`. Опыт практического применения python для автоматизации Confluence показывает, что чаще всего используется один из двух подходов к редактированию `body`: заполнение `body` по шаблону и замена фрагментов по регулярным выражениям. Мы рекомендуем начать с заполнения по шаблону. Суть этого подхода заключается в создании текстового шаблона, с метками для функции python `string.format`. На рисунке 4 приводится пример отображаемого содержимого страницы. На рисунке 5 приводится сравнение `body` этой страницы(слева) и его шаблона(справа).

Testing automatization

Создатель Muklaev Sabur Mergenovich, отредактировано только что · 98 views by 7 users since 27 Apr 2022 [Add Approval](#)

Дата обновления:

📅 01.04.2023

Участники:

@ Muklaev Sabur Mergenovich

Содержание:

Company	Contact	Country
Alfreds Futterkiste	Maria Anders	Germany
Centro comercial Moctezuma	Francisco Chang	Mexico

Рисунок 4. Пример отображаемого содержимого страницы

```

1 <h3>Дата обновления:</h3>
2 <h3> <time datetime="2023-04-01"/> </h3>
3 <h3>Участники:</h3>
4 <p>
5 <ac:link>
6 <ri:user ri:userkey="---"/>
7 </ac:link>
8 </p>
9 <h3>Содержание:</h3>
10 <table>
11 <colgroup>
12 <col/>
13 <col/>
14 <col/>
15 </colgroup>
16 <tbody>
17 <tr>
18 <th>Company</th>
19 <th>Contact</th>
20 <th>Country</th>
21 </tr>
22 <tr>
23 <td>Alfreds Futterkiste</td>
24 <td>Maria Anders</td>
25 <td>Germany</td>
26 </tr>
27 <tr>
28 <td>Centro comercial Moctezuma</td>
29 <td>Francisco Chang</td>
30 <td>Mexico</td>
31 </tr>
32 </tbody>
33 </table>
34 <p class="auto-cursor-target">
35 <br/>
36 </p>
37
1 <h3>Дата обновления:</h3>
2 <h3> <time datetime="{0}"/> </h3>
3 <h3>Участники:</h3>
4 <p>
5 <ac:link>
6 <ri:user ri:userkey="---"/>
7 </ac:link>
8 </p>
9 <h3>Содержание:</h3>
10 {1}
11 <p class="auto-cursor-target">
12 <br/>
13 </p>
14

```

Рисунок 5. Сравнение body страницы(слева) и его шаблона(справа)

```

1 import magic
2 from atlassian import confluence
3 import os
4
5 import pandas as pd
6
7 import requests
8
9 path = os.path.dirname(os.path.abspath(__file__))
10
11 confluence = Confluence(
12     url="https://confluence.veon.com",
13     username="", #подставить данные
14     password="", #подставить данные
15 )
16
17 page_id = 182506759
18
19 #get_page_by_id - информация о странице, организована по типу словаря, в данном случае ищем в нем title
20 title = pd.DataFrame(confluence.get_page_by_id(page_id, expand=None, status=None, version=None))['title'][0]
21 space = confluence.get_page_space(page_id)
22
23 #добавить любой файл в папку files и он автоматически добавляется на страницу
24 for file_name in os.listdir(path=path+"\\files"):
25     file_location_with_page = path.replace('\\', '/') + "/files/" + file_name
26     #эта функция дает тип контента, он зависит от файла, который подгружается
27     content_type = magic.from_file(file_location_with_page, mime=True)
28     confluence.attach_file(filename=file_location_with_page, name=file_name, content_type=content_type, page_id=page_id, space=space )

```

Рисунок 6. Пример добавления всех файлов из каталога в качестве вложений

Добавление вложений. В качестве вложений могут добавляться многие самые распространенные типы документов, а также изображения в разных форматах [5]. В частности, мы предлагаем разработчику формировать диаграммы, графики или иную инфографику в удобном формате изображений, и после создания шаблона страницы с указанием ссылки на изображение обновлять вложение. На рисунке 6 приводится пример добавления всех файлов из каталога в качестве вложений.

Приведенные в этой статье методы автоматизации не заменяют полноценного веб-сервиса, но помогут средствами доступными любому python разработчику в короткие сроки автоматизировать большой спектр задач от элементарных до весьма специфических.

Список литературы

1. Confluence [Электронный ресурс] // Atlassian URL: <https://www.atlassian.com/ru/software/confluence> (дата обращения: 30.02.2023).
2. Jira Software [Электронный ресурс] // Atlassian URL: <https://www.atlassian.com/ru/software/jira> (дата обращения: 30.02.2023).
3. Atlassian Python API. Confluence module [Электронный ресурс] // URL: <https://atlassian-python-api.readthedocs.io/confluence.html> (дата обращения: 30.02.2023).
4. Atlassian Python API wrapper [Электронный ресурс] // URL: <https://github.com/atlassian-api/atlassian-python-api> (дата обращения: 30.02.2023).
5. Atlassian Confluence: расширяем на python [Электронный ресурс] // URL: <https://habr.com/ru/companies/alfastrah/articles/460929> (дата обращения: 30.02.2023).

УДК 004.912

Система электронного документооборота как элемент цифровизации предприятия

Потехина Елена Витальевна

профессор кафедры Информационных технологий, искусственного интеллекта и общественно-социальных технологий цифрового общества
Российского государственного социального университета

Купцова Ксения Михайловна

магистрант Российского государственного социального университета

***Аннотация:** Одним из направлений реализации цифровой трансформации выступает построение корпоративных автоматизированных документных систем, составной частью которых являются системы электронного документооборота. В статье рассмотрены преимущества внедрения и использования систем электронного документооборота на предприятиях как элемента глобального тренда на цифровизацию экономики.*

***Abstract:** One of the directions of digital transformation implementation is the construction of corporate automated document systems, an integral part of which are electronic document flow management systems. The article describes the advantages of the introduction and use of electronic document flow management systems in enterprises as an element of the global trend of digitalization of the economy.*

***Ключевые слова:** электронный документооборот, системы электронного документооборота, цифровая экономика, цифровизация предприятия.*

***Keywords:** electronic document management, electronic document management systems, digital economy, digitalization of the enterprise.*

На смену информатизации и компьютеризации пришел новый тренд — цифровизация. Как новый шаг развития информационных технологий, цифровизация настаивает на развитии новых технологических, технических подходов и применении современных программных продуктов для работы на предприятиях.

Переход к электронным документам и данным есть источник цифровой трансформации для управления компанией, а также основа в государ-

ственном управлении, при обеспечении кооперации общества и государства в рамках цифровой экономики.

Правительством Российской Федерации утверждена программа «Цифровая экономика Российской Федерации» (распоряжение от 28.07.2017 № 1632-р), которая должна обеспечить продвижение современных информационных технологий в значимых для экономики и общества отраслях. Намеченный курс так же окажет воздействие на многие бизнес-процессы: оптимизируют старые и создаст новые, что в свою очередь коснется работы с документами, как неизменного атрибута множества бизнес-процедур.

Цифровая экономика предполагает трансформацию правоотношений коммерческих структур между собой, а также между ними и государством в полностью электронный вид там, где это возможно. И с электронным документооборотом такой переход тесно связан.

В современных условиях цифровой экономики важным аспектом становится юридически значимый электронный документооборот (ЮЗЭДО) и технический функционал СЭД по защищенному хранению в электронном виде свидетельств взаимоотношений между контрагентами, документов и других данных, имеющих юридическую силу.

Решением Президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 25.12.2020 № 34) была утверждена Концепция электронного документооборота в хозяйственной деятельности, разработанная Федеральной налоговой службой совместно с причастными органами власти и заинтересованными представителями бизнес-сообщества.

На сайте ФНС размещен «Калькулятор эффективности внедрения электронного документооборота в компании», который на основе введенных данных по организации помогает рассчитать основные финансовые и экономические показатели на ЮЗЭДО как с внешними контрагентами, так и внутри организации, а также эффект от внедрения СЭД.

На сегодняшний день в Российской Федерации все органы государственной власти различных уровней, а так же многие коммерческие структуры перешли на использование систем электронного документооборота, которые позволяют автоматизировать документооборот на всех стадиях

жизненного цикла документа: от момента его создания до списания в архив. Такая масштабная трансформация подтверждает общепризнанный факт, что системы электронного документооборота упрощают доступ ко всем документам и необходимым данным, обеспечивают их надежное хранение, а также позволяют достичь более высокого уровня эффективности операционной деятельности в мире информационных технологий и передовых коммуникаций.

Еще одним импульсом (с 2019 года) ускорения цифровизации послужила пандемия новой коронавирусной инфекции с дистанционным взаимодействием людей и обществ. За очень короткий промежуток времени привычным в деловом обиходе стал дистанционный формат работы, значительно расширился набор услуг в электронном виде, в т.ч. государственных, в оборот вошло множество бизнес-приложений и цифровых решений, позволяющих на расстоянии эффективно коммуницировать внутри общества, то есть без физического взаимодействия. Теперь все это стало неотъемлемой частью нашей жизни.

По состоянию на конец 2022 года собраны сведения о 7,3 тыс. проектов внедрения СЭД/ЕСМ-систем, по которым можно сделать выводы об отраслевом распределении проектов. На Рисунке 1 видно, что на лидирующих позициях находятся государственные структуры (более 14% от всех внедрений); также весомое количество приходится на отрасль строительства и финансовых услуг (доля каждой превышает 8%) [4].

По итогам 2021 года для отечественного рынка СЭД оказались довольно результативным. Развертывание проектов по внедрению СЭД/ЕСМ-систем происходило активно, важным импульсом в росте стал тренд на импортозамещение. Рынок показал подъем, о чем свидетельствуют финансово-экономические результаты [5].

Аналитики оценивают рост показателей российского рынка СЭД/ЕСМ-систем в 2022 и 2023 годах в 10%, что представлено на Рисунке 2.

На практике отождествляют два термина ЭДО (электронный документооборот) и СЭД (система электронного документооборота), под которыми объединяют сразу нескольких понятий:

- внутренний документооборот, организованный в пределах компании. Отдельно выделяют бухгалтерский, управленческий, архивный,



Рисунок 1. Отраслевое распределение проектов внедрения СЭД/ЕСМ-систем, в %

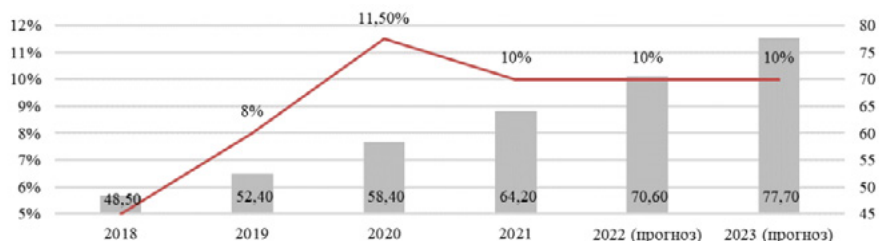


Рисунок 2. Объем российского рынка СЭД/ЕСМ-систем, в 2018–2023 годах, в млрд рублей

кадровый (примеры систем: Directum, Docsvision, 1С: Документооборот и пр.);

- межкорпоративный (внешний) документооборот, который обеспечивает отправку и получение от контрагентов цифровых договоров, закрывающих документов и т.д. (примеры: Контур, Тензор и пр.);
- электронный документооборот с государственными органами, например, для подачи отчетности в ФНС, взаимодействия с Федеральным казначейством и другими регуляторами.

Более подробно рассмотрим системы электронного документооборота для организации внутреннего документооборота на предприятиях.

Стоит отметить, что нормативной базы, регулирующей разработку данного вида систем недостаточно, и разработчики СЭД, в свою очередь ориентируются на регламентирующие документы для «классического» делопроизводства, а именно:

- Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ, Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ и т.д.;
- письма Минюста РФ, Минфина РФ, приказы Росстандарта и Росархива, а также отраслевые правила и требования, других государственных органов;
- постановления правительств федерального и региональных уровней;
- стандарты и ГОСТы по делопроизводству, архивам, системам распорядительной документации — Р 7.0.8–2013, ГОСТ Р 7.0.97–2016 и другие.

Стоит отметить, что некоторые нормативные акты «конфликтуют» друг с другом, а ГОСТы носят рекомендательный характер, при этом разработчики системы стараются делать ее адаптивной, гибкой и готовой к изменениям. Кроме того, следует брать в расчет регулярные новации в работе с электронными подписями (далее — ЭП), которые имеют принципиальное значение для ЮЗЭДО. Документооборот — сложнорегулируемая и трудоемкая сфера деятельности предприятий.

Если объединить обмен документами, актуальный для бухгалтерских и юридических подразделений, территориально-распределенных участков предприятия, в единой системе, то формируется цифровая экосистема, в которой данные передаются без искажений и утраты, в цифровом виде, что делает максимально прозрачными все процессы обработки и обмена информацией. ЮЗЭДО упрощает и ускоряет внутрикорпоративное согласование, обмен документами с внешними партнерами, процессы подготовки и предоставления отчетности в контролирующие службы.

У отечественного рынка систем электронного документооборота уникальная черта — сращивание понятий СЭД и ЕСМ/EDMS-систем. Вполне возможно, что при употреблении понятия «система электронного

документооборота», подразумевают функциональные характеристики ЕСМ-системы.

Основной компонент в СЭД является — документ, состоящий из набора информации и реквизитов, а функционал системы состоит из учета, регистрации и контроля над результатами организационно-распорядительной деятельности предприятия. С течением развития СЭД дополнился отдельными функциями по работе с договорами, первичными учетными документами, обращениями и пр.

Этот функционал имеется и в ЕСМ-системах (Enterprise Content Management), при этом сверхцельная — этот класс систем обеспечивает формирование единого информационного пространства предприятия. В отличие от СЭД, которая работает только с документами, ЕСМ работает со всем корпоративным контентом, образующийся в результате деятельности компании: документы, переписка медиафайлы, записи нормативно-справочной информации и т.д. Помимо того, появляется инструмент по управлению потоками работ (Work Flow), формированию бизнес-процессов и управлению доступом к данным.

Нередко СЭД так же называют EDMS (Electronic Document Management System), которая представляет собой взаимосвязанный механизм по сбору, хранению, поиску, просмотру и доступу к электронным документам. Однако EDMS является составляющей принципа управления корпоративным контентом или вышеназванной ЕСМ-системы, но эти термины все же шире, чем «классический» СЭД.

Представленные системы электронного документооборота на современном российском рынке фактически являются ЕСМ-системами, просто термин СЭД более привычен.

В процессе развития СЭД постепенно освоила логику всего жизненного цикла документа и следом автоматизировала кросс-функциональные бизнес-процессы, взаимосвязанные с документооборотом, и как результат отчасти приняла на себя функции BPM-систем (Business Process Management).

BPM подход в свою очередь позволяет выстроить бизнес-процессы и настроить маршрутизацию документа в соответствии со стратегией предприятия, что приводит к достижению целевой производительности,

финансово-экономических показателей за счет повышения качества работ на уровне отдельного подразделения, предприятия в целом и на стыках между организациями.

Такое разнообразие систем, подход к данным и документам требуют переосмысления методов работы в области документационного обеспечения.

Происходящая трансформация СЭД стала частью стратегического развития государственных структур и коммерческих организаций необходимой для успешной реализации стратегических задач цифровизации. Эта модернизация значительно повышает эффективность предприятий, снижает финансовые издержки на обеспечение их деятельности и позволяет подняться на новый уровень предоставления товаров и услуг.

Список литературы

1. Указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года».
2. Распоряжение Правительства РФ № 1632-р, утверждающее программу «Цифровая экономика Российской Федерации».
3. Концепция развития электронного документооборота в хозяйственной деятельности (утверждена решением президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 25.12.2020 № 34).
4. Российский рынок СЭД, ECM и CSP-систем: Оценки и итоги // TAdviser URL: <https://www.tadviser.ru/index.php/%D0%A1%D0%AD%D0%94> (дата обращения: 08.05.2023).
5. Отраслевая специфика внедрений СЭД/ECM // TAdviser URL: <https://clck.ru/QXAg2> (дата обращения: 08.05.2023).

УДК 004.023

Важность, факторы, подходы, обобщенная модель оптимизации расписания в высших учебных заведениях

Головизов Денис Иванович

студент магистратуры направления «Информатика и вычислительная техника»
Самарского государственного технического университета

***Аннотация:** Данная статья посвящена рассмотрению предпосылок создания системы автоматизации расписания занятий, подходам для решения данной задачи. В результате анализа предметной области приведены факторы процесса планирования, метрики и ограничения. Рассмотрены и проанализированы три основных компонента модели оптимизации.*

***Abstract:** This article is devoted to the prerequisites for creating a system for automating the schedule of educational classes and approaches for solving this problem. As a result of the analysis of the subject area, the factors of scheduling process, metrics and constraints are given. The three main components of the optimization model are considered and analyzed.*

***Ключевые слова:** оптимизация, учебный процесс, расписание, студент, ВУЗ, факторы, подходы, модель.*

***Keywords:** optimization, educational process, schedule, student, university, factors, approaches, model.*

.....

Качество подготовки специалистов в вузах и особенно эффективность использования научно-педагогического потенциала зависят в определенной степени от уровня организации учебного процесса. Немалую роль в котором играет учебное расписание [1].

Современный переход на новые образовательные стандарты требует изменить систему подготовки специалистов и оценки ее качества [2].

Автоматизация составления расписания является классической задачей в системах по управлению учебными заведениями, но пока что не существует единого и общепринятого способа её решения [3].

Составление расписания — это реальная проблема оптимизации, которая связана с планированием событий с фиксированным количеством

временных интервалов и ресурсов, удовлетворяющих мягким и жестким ограничениям и максимально приближенным к необходимым целям. Задача составления расписания является NP-сложной (задача с ответом «да» или «нет», к которой можно свести любую другую задачу из этого класса за полиномиальное время) и требует огромного объема вычислений для поиска решений, который экспоненциально растет с увеличением размера задачи.

Оптимизация расписания занятий в высших учебных заведениях важна по нескольким причинам:

1. Оптимизированное расписание занятий может помочь студентам пройти нужные им программы обучения без задержек по времени, что может привести к большему удовлетворению, вовлеченности и, в конечном итоге, к лучшим академическим результатам.
2. Оптимизация расписания занятий может помочь высшим образовательным учреждениями более эффективно использовать свои ресурсы, такие как пространство в аудиториях, а также рабочее время преподавателей, что может привести к экономии средств и повышению эффективности работы организации.
3. Повышение производительности преподавателей. Оптимизированное расписание занятий может помочь преподавателям более эффективно управлять своим временем, гарантируя, что они преподают курсы, соответствующие их опыту и интересам.
4. Хорошо оптимизированное расписание занятий может помочь учебным заведениям привлекать и удерживать высококвалифицированных студентов и преподавателей, что может повысить их репутацию и конкурентоспособность в сфере высшего образования.

Подытоживая важность оптимизации расписания занятий в высших учебных заведениях, можно отметить, что она имеет решающее значение для обеспечения успеха студентов, повышения эффективности учебного заведения и улучшения результатов как студентов, так и преподавателей. Эта задача требует тщательного планирования, анализа данных и использования соответствующих стратегий и инструментов.

Важно понимать, что в России ВУЗы составляют расписание студентов и преподавателей одновременно. У данного подхода имеется огромный

минус, ведь работа ведется довольно монотонным и однообразным образом, допускающим возникновение ошибок и приводящим к необоснованному расходу времени [4].

Оптимизация расписания занятий в высших учебных заведениях может быть сложной задачей из-за большого количества задействованных ограничений и переменных. Однако существует несколько подходов, которые можно использовать для решения этой задачи:

1. Программное обеспечение для автоматического планирования. Использование программного обеспечения для автоматического планирования может помочь оптимизировать расписания занятий, принимая во внимание такие факторы, как доступность курсов, наличие помещений (аудиторий) и преподавателей, а также предпочтения и ограничения учащихся.
2. Блокировка по времени. Одной из стратегий оптимизации расписания занятий является использование блокировки по времени, когда определенные блоки времени назначаются для определенных курсов, что может помочь уменьшить конфликтность в расписании и гарантировать, что учащиеся имеют доступ к нужным им курсам.
3. Последовательность курсов. Оптимизация последовательности курсов также может помочь улучшить расписание занятий. Например, планирование подготовительных курсов позволяет гарантировать, что учащиеся обладают необходимыми знаниями и навыками для успешного прохождения основного курса.
4. Гибкость. Предоставление студентам различных вариантов расписания, таких как разное время занятий и форматы (например, онлайн, гибридные), может помочь оптимизировать расписание занятий и удовлетворить потребности разнообразного студенческого контингента.

Рассмотрим основные факторы процесса планирования:

- доступные ресурсы могут включать персонал, оборудование, программное обеспечение, помещения и т. д.;
- объем работы, который необходимо выполнить, может относиться к прогнозируемому уровню спроса на учебные часы, который необходимо удовлетворить, количеству теоретических и практических занятий и т.д.;

- денежные расходы — это любые операционные или капитальные затраты, влияющие на результат: начисление заработной платы, компенсации сверхурочных рабочих часов, амортизация оборудования, затраты на хранение и так далее.;
- жесткие операционные ограничения — это ограничения, которые нельзя изменить и которые необходимо учитывать. они включают трудовые нормы (например, количество рабочих и сверхурочных часов в неделю), физические ограничения, точное количество и состав оборудования, количество преподавателей и студентов.

В эту категорию также могут быть включены ограничения вместимости аудиторий и пропускной способности лабораторных стендов, количество студентов, которых может принять аудитория, количество времени, необходимое для объяснения учебного материала и т.д.

Мягкие ограничения — это те, которые желательны, но не обязательны, например, индивидуальные предпочтения сотрудников учебных заведений, приоритизация направлений подготовки и т.д.

Метрики или ключевые показатели эффективности — это измерения, которые показывают эффективность расписания, и их можно сравнивать для поддержки принятия решений.

Оптимизированный график расписания — это тот, который не только соответствует максимальному количеству ограничений, но и помогает достичь определенных целей.

Составление расписания относится к области оперативных исследований и включает в себя такие известные задачи оптимизации. Они нацелены на поиск решения/графика в рамках набора ограничений, которые были бы оптимальным балансом затраченных ресурсов и объема произведенной работы. Все они изучались десятилетиями, и сегодня существует ряд технологических подходов, помогающих решить проблему планирования.

Традиционным подходом к оптимизации расписания является создание модели оптимизации. Выделяют три основных компонента обобщенной модели оптимизации (рисунок 1):

- набор возможных переменных решения (управляемые решения, такие как, число занятий в неделю, длительность курса, число групп на занятии);

- набор ограничений, которые накладываются на переменные, исключая определенные значения (общее количество студентов, преподавателей, аудиторий, их максимальная вместимость);
- целевая функция, которая представляет собой математическое выражение, описывающее цель модели, например, максимизировать загрузку аудиторий или минимизировать издержки на заработную плату преподавателей.



Рисунок 1. Входные и выходные данные обобщенной модели оптимизации

Таким образом, на выходе модели оптимизации будут значения переменных, которые позволяют минимизировать или максимизировать целевую функцию, при этом соблюдая ограничения.

Задача оптимизации учебного процесса ищет наилучшее расписание, удовлетворяющее заданным критериям, в виде набора заданных ресурсов, которые могут содержать лекторов, группы студентов, аудитории и/или лаборатории. Разработка расписания является фундаментальным требованием для нормального функционирования всех образовательных учреждений. Однако такие факторы, как наличие часов, количество предметов и распределение преподавателей, делают проблему расписания очень сложной.

Создание бесконфликтного расписания, которое могут использовать преподаватели, является одной из проблем, с которыми сталкивается большинство университетов. Как правило, расписание представляет собой таблицу различных событий и их даты и время.

Таким образом, в университетском расписании учебное заведение распределяет курсы, пройденные студентами и проводимые преподавателями, по определенному конечному набору ресурсов, включая временные интервалы и классы. Этот процесс сопряжен со многими проблемами.

Например, в типичном ВУЗе имеется несколько групп учащихся, которые могут или не могут изучать один и тот же курс в одно и то же время. Таким образом, при планировании лекций необходимо убедиться, что учащиеся, лекторы и лекционные залы не конфликтуют между собой. Эта необходимость делает составление расписания сложной и трудоемкой задачей.

В целом, оптимизация расписания занятий в высших учебных заведениях требует тщательного рассмотрения широкого круга факторов, включая доступность курсов, наличие помещений, наличие преподавателей, предпочтения и ограничения студентов и многое другое. Используя комбинацию стратегий, таких как программное обеспечение для автоматизированного планирования, временная блокировка, последовательность курсов, гибкость и анализ данных, учебные заведения могут создавать расписания занятий, отвечающие потребностям как студентов, так и преподавателей.

Список литературы

1. Шишканова Т. А. Алгоритм оптимизации учебного расписания в вузе». — Горный информационно-аналитический бюллетень (научно-технический журнал), 2015. — С. 416–421.
2. Иванченко И. В. Проблема повышения качества образования в вузе // Молодой ученый.— 2016.— № 5.1. — С. 18–21. — URL <https://moluch.ru/archive/109/26315/> (дата обращения: 13.08.2018).
3. Назарова, О. Б. Расписание учебного процесса в вузе: автоматизация и оптимизация / О. Б. Назарова, Р. Р. Усманова // Наука. Информатизация. Технологии. Образование: материалы XI международной научно-практической конференции, г. Екатеринбург, 26 февраля — 2 марта 2018 г. — Екатеринбург: Издательство РГППУ, 2018. — С. 557–563.
4. Задорнова Н.А., Хамдамова Д.Т., Дементьева А.М., Шаипова Л. А. Процессы повышения качества образования путем оптимизации порядка составления расписания. — Системные технологии.— 2018.— № 29. — С. 131–135.

УДК 004.023

Обзор видов ограничений и различных методов планирования и оптимизации расписания в учебных заведениях

Головизов Денис Иванович

студент магистратуры направления «Информатика и вычислительная техника»
Самарского государственного технического университета

***Аннотация:** Данная статья посвящена рассмотрению видов ограничений, который присутствуют в задачах оптимизации составления расписаний, а также обзору различных методов планирования и оптимизации расписания в учебных заведениях, их особенностей, достоинств и недостатков.*

***Abstract:** This article deals with the types of constraints that are present in scheduling optimization problems and reviews various methods of scheduling planning and optimization in educational institutions, their features, advantages, and disadvantages.*

***Ключевые слова:** оптимизация, учебный процесс, расписание, ограничение, метаэвристика, модель.*

***Keywords:** optimization, learning process, schedule, constraint, metaheuristics, model.*

.....

Расписание занятий имеет важнейшее значение в организации учебного процесса. От грамотно составленного расписания зависит полнота творческой отдачи и трудовой ритм преподавателей, а также успешность обучения студентов [1].

Оптимизация учебного процесса связана с планированием занятий в определенное время в заданных аудиториях с конкретными обучающимися, которые должны в них присутствовать. В лучшем случае результатом решения проблемы являются планы, позволяющие всем студентам посещать занятия в определенном месте и в определенное время.

Однако существуют жесткие (нельзя нарушать) и мягкие (нежелательно, но можно нарушать) ограничения на распределение ресурсов (таблица 1).

Сотрудники, занимающиеся составлением расписания, должны учитывать все эти ограничения, чтобы добиться оптимального результата.

Таблица 1. Мягкие и жесткие ограничения

Мягкие ограничения	Жесткие ограничения
<p>Выпускные и общие курсы должны быть запланированы на непересекающиеся временные интервалы.</p> <p>Мягкие ограничения</p>	<p>Курсы с общими студентами не могут быть распределены в одно и то же время в один и тот же день.</p> <p>Общее количество доступных периодов суточного расписания составляет 8 часов (максимум)</p> <p>Жесткие ограничения</p>
<p>Количество студентов, проходящих курс, должно соответствовать отведенной аудитории.</p> <p>Каждый дополнительный студент сверх вместимости аудитории считается нарушением.</p>	<p>Аудитория не может быть назначена более чем для одной лекции в определенный период.</p> <p>Курсы, входящие в учебную программу, должны быть отнесены к разным периодам.</p> <p>Курсы, читаемые лектором, должны быть отнесены к разным периодам.</p>
<p>Лекции по данному учебному предмету должны быть последовательными.</p>	<p>Расписание должно быть запланировано на основе университетского календаря:</p> <ul style="list-style-type: none"> — учитывает загруженность преподавателей. — учитывает свободное время (т.е. рабочие часы) лекторов. <p>— каждый курс должен быть привязан к месту проведения в определенный временной интервал.</p> <ul style="list-style-type: none"> — запланированные курсы не должны превышать вместимость аудитории. — лекционные аудитории нельзя бронировать дважды на одно и то же время. — все лекционные помещения должны быть запланированы один раз, а не дважды.
	<p>Ни одна студенческая группа не проводит два мероприятия одновременно.</p> <p>Ни у одного лектора нет двух мероприятий одновременно.</p> <p>Ни одно мероприятие не проводится в помещении с меньшей вместимостью, чем количество студентов в группе.</p>

Из-за сложности этой проблемы сотрудники тратят значительное количество времени на поиск наилучшего решения. Однако даже при наличии большого опыта найденное разрешение может оказаться не оптимальным из-за большого количества возможных комбинаций.

Описывая реальную задачу математическими функциями, можно проводить поиск значений в моделях с использованием методов оптимизации. Таким образом, ставится задача найти решение, максимально использующее имеющиеся человеческие ресурсы и удовлетворяющее потребности всех вовлеченных сторон. Этот подход становится очень сложным по мере появления новых ограничений.

Особо актуальными в сфере оптимизации учебного процесса считаются подходы, основанные на метаэвристике, которые обещают точные и оптимальные решения проблемы планирования расписания. Известные подходы такого рода включают:

1. Жадный рандомизированный адаптивный поиск (GRASP — Greedy Randomized Adaptive Search).

Это многозаходная метаэвристика для задач комбинаторной оптимизации, в которой каждая итерация состоит в основном из двух фаз: построения и локального поиска. На этапе построения строится допустимое решение, окрестность которого исследуется до тех пор, пока не будет найден локальный минимум на этапе локального поиска. В результате сохраняется лучшее общее решение.

2. Алгоритм имитации отжига (SA — Simulated Annealing).

Это метод решения задач оптимизации без ограничений и со связанными ограничениями. Метод моделирует физический процесс нагревания материала с последующим медленным понижением температуры для уменьшения количества дефектов, минимизируя, таким образом, энергию системы. На каждой итерации моделируемого алгоритма отжига случайным образом генерируется новая точка. Расстояние новой точки от текущей или объем поиска основаны на распределении вероятностей со шкалой, пропорциональной температуре. Алгоритм принимает все новые точки, которые снижают цель, а также, с определенной вероятностью, точки, которые повышают цель.

Таблица 2. Обзор различных методов планирования и оптимизации расписания в учебных заведениях

Техника	Недостатки	Достоинства
Поиск с запретами	<p>Плохо работает в задачах большой размерности.</p> <p>Поскольку у него нет памяти, для его эффективной работы требуются другие алгоритмы или дополнительные компоненты.</p>	<p>Его можно использовать для более точного исследования итерационных задач, чем другие алгоритмы.</p> <p>Игнорирует недавно исследованные районы, чтобы избежать выбора локального оптимального решения.</p>
Алгоритм великого потока (GD)	Сложный в реализации.	Имеет короткое вычислительное время.
Алгоритм Бройдена-Флетчера-Гольфарба-Шанно (BFGS)	Плохо работает в контексте негладкой оптимизации.	Имеет лучшую сходимость, чем большинство алгоритмов.
Целочисленное программирование	Не может решить проблемы рассеяния.	Иметь более высокую вероятность/эффективность.
Метаэвристические методы	Долго вычисляет оптимальное решение.	Может быстро сходиться.
Гиперэвристика	Сложный в реализации.	Может быть оптимальным.
Подходы, основанные на фиксации и оптимизации метаэвристики	Не эффективны в рабочих задачах, связанных с рассеянием.	Не перекрывается и не мутирует.

Таблица 1 (продолжение)

Техника	Недостатки	Достоинства
Целочисленное программирование	Трудно определить исходные параметры проекта.	Ограниченное число параметров, которые необходимо настроить.
Алгоритм искусственной пчелиной семьи	Сходится преждевременно, что приводит к отсутствию решений в некоторых случаях.	Прост в использовании и может эффективно взаимодействовать с другими алгоритмами.
Алгоритм имитации отжига	Требует улучшений для эффективного функционирования.	Постепенно сходится к глобальному оптимальному решению и тем самым уходит от локального решения.
Стохастический градиентный спуск	Гиперпараметры необходимо настраивать вручную. Следовательно, сложен в изучении и использовании.	Прост в реализации и быстро работает при применении к небольшим наборам данных.
Оптимизация колонии элитных иммунных муравьев (EIACO)	Сложный для реализации.	Сочетает в себе сильные стороны муравьиной колонии и иммунного алгоритма.
Многоцелевая оптимизация	Может преждевременно сходиться.	Умеет выполнять параллельные вычисления.
Линейная целочисленная модель	Сложный в реализации.	Эффективен в решении задач, не имеющих точных математических моделей.
Рой частиц (PSO)	Сходится не быстро.	Простота реализации.

3. Поиск с запретами (TS — Tabu Search).

Это метаэвристика, которая используется для решения задач оптимизации. Производительность TS была улучшена по сравнению с методом локального поиска за счет ухода от уже посещенных решений задачи и их соседей. Это останавливает поиск локальных оптимальных решений. TS создает кандидатов, которые в основном представляют собой набор различных целочисленных переменных. Эти кандидаты отличаются на один или несколько бит от текущего оптимального решения и отбрасываются из списка, созданного TS. Затем подзадачи исходной задачи решаются для каждого кандидата с помощью метода, основанного на градиенте. Чтобы создать ресурс для следующего поколения, выбирается один существующий кандидат с наилучшей объективной ценностью.

4. Генетический алгоритм (GA — Genetic Algorithm).

Это метод решения задач оптимизации с ограничениями и без, основанный на естественном отборе — процессе, управляющем биологической эволюцией. Генетический алгоритм неоднократно модифицирует совокупность индивидуальных решений.

Система штрафов является механизмом, позволяющим регулировать процесс оптимизации расписания [2].

Проблемы планирования обычно решаются с помощью эвристических методов из-за их структуры и сложности. Некоторые из общих метаэвристических стратегий включают эволюционные алгоритмы, муравьиную колонию, локальный поиск, симуляцию отжига и запретный поиск, но ни одну из них нельзя выделить как лучшую.

В таблице 2 приведены сводные данные некоторых из алгоритмов оптимизации составления расписания [3].

Следует отметить, что выбор конкретного метода зависит от множества ограничений, которые присутствуют в каждом конкретном случае.

Список литературы

1. Масляев Д. А. Современное состояние задачи автоматизации составления оптимального учебного расписания в вузе / Вестник Сыктывкар-

- ского университета. Серия 1: Математика. Механика. Информатика. 2022. Выпуск 1 (42). — С. 23–40.
2. Яндыбаева Н. В. Генетический алгоритм в задаче оптимизации учебного расписания ВУЗа // Современные наукоемкие технологии.— 2009.— № 11. — С. 97–98.
 3. Кохендерфер У. Алгоритмы оптимизации. — Вильямс, 2020.— 528 с. — ISBN: 978–5–907144–76–7.

УДК 004

Инновации и их значимость в современном мире

Порошин Даниил Олегович

студент кафедры Инноватики и интегрированных систем качества
Санкт-Петербургского государственного университета аэрокосмического
приборостроения

***Аннотация:** Целью данной работы является анализ значимости инноваций в современном мире. Методология исследования включает анализ научных статей и публикаций, а также проведение опроса среди представителей бизнес-сообщества. Основные результаты исследования показывают, что инновации являются неотъемлемой частью современного бизнеса и оказывают значительное влияние на развитие экономики. Область применения инноваций включает все сферы жизни, начиная от технологий и заканчивая общественными отношениями. Выводы работы подчеркивают необходимость инноваций в современном мире и значимость их развития для общества.*

***Abstract:** The purpose of this paper is to analyze the significance of innovation in the modern world. The research methodology includes an analysis of scientific articles and publications, as well as a survey of the business community. The main results of the study show that innovation is an integral part of modern business and has a significant impact on economic development. The scope of innovation includes all areas of life, from technology to social relations. Conclusions of the work emphasize the necessity of innovations in the modern world and the importance of their development for the society.*

***Ключевые слова:** инновации, экономика, технологии, общество, бизнес, методология.*

***Keywords:** innovation, economics, technology, society, business, methodology.*

Введение

Современный мир характеризуется быстрыми темпами развития технологий и глобализацией экономики. В таких условиях инновации играют все более значимую роль в различных сферах жизни.

Инновации — это новые идеи, продукты, услуги, технологии или процессы, которые изменяют существующие способы производства, потребления и общественные отношения. Они помогают повысить эффективность бизнеса, улучшить качество жизни и обеспечить устойчивое развитие экономики [1].

Актуальность исследования

Инновации оказывают значительное влияние на экономику и общество в целом. Они позволяют создавать новые рабочие места, повышать уровень жизни населения, улучшать качество продуктов и услуг, а также снижать издержки производства. Инновационный подход является основой конкурентоспособности в современном бизнесе и позволяет компаниям выживать в условиях жесткой конкуренции. В связи с этим, исследование значимости инноваций является актуальной темой для бизнес-сообщества и научного сообщества.

Целью данной работы является анализ значимости инноваций в современном мире. Для достижения данной цели необходимо рассмотреть следующие задачи:

1. Изучить теоретические аспекты инноваций и их роль в современной экономике и обществе.
2. Оценить практическую значимость инноваций на примере различных отраслей экономики.
3. Рассмотреть методы и инструменты разработки и внедрения инноваций в бизнес-процессы.
4. Предложить практические рекомендации по использованию инноваций для повышения конкурентоспособности бизнеса и улучшения качества жизни населения.

Методы и организация исследования

Для проведения данного исследования были использованы следующие методы:

1. Анализ научных статей и публикаций по теме исследования.
2. Опрос среди представителей бизнес-сообщества для оценки практической значимости инноваций.
3. Сравнительный анализ примеров успешного использования инноваций в различных отраслях экономики.
4. Интервью с экспертами в области инноваций и экономики.

Организация исследования

Для организации исследования был проведен литературный анализ научных статей и публикаций по теме исследования. Для проведения опроса был составлен опросник, который был распространен среди представителей бизнес-сообщества. Были также проведены интервью с экспертами в области инноваций и экономики. Для анализа полученных данных были использованы статистические методы [2].

Результаты исследования и их обсуждение

Анализ научных статей и публикаций показал, что инновации являются неотъемлемой частью современного бизнеса. Они позволяют компаниям улучшать свои продукты и услуги, сокращать издержки производства и повышать конкурентоспособность. Инновации также оказывают значительное влияние на экономику и общество в целом, способствуя созданию новых рабочих мест и улучшению качества жизни населения.

Опрос среди представителей бизнес-сообщества показал, что большинство компаний придает большое значение инновациям и считают их важным фактором успеха. Однако, некоторые компании сталкиваются с трудностями при внедрении инноваций из-за недостатка квалифицированных кадров, отсутствия финансовых ресурсов и недостаточной поддержки со стороны государства.

Сравнительный анализ примеров успешного использования инноваций в различных отраслях экономики показал, что компании, которые активно используют инновации, имеют преимущество перед конкурентами и могут эффективно справляться с вызовами современного рынка. Например, компания Tesla, которая внедрила инновационный подход в производстве электромобилей, стала одним из лидеров в отрасли и добилась значительных успехов в продажах.

Интервью с экспертами в области инноваций и экономики подтвердили важность инноваций для развития бизнеса и экономики в целом. Эксперты выделили несколько ключевых факторов, которые способствуют успешному внедрению инноваций, включая наличие квалифицированных кадров, инвестиции в исследования и разработки, партнерства с другими компаниями и поддержку со стороны государства.

Обсуждение полученных результатов.

Результаты исследования подтверждают значимость инноваций в современном мире и их роль в улучшении конкурентоспособности бизнеса и качества жизни населения. Однако, для успешного внедрения инноваций необходимо преодолеть некоторые трудности, такие как нехватка квалифицированных кадров и отсутствие финансовых ресурсов.

На основе полученных результатов исследования можно предложить следующие практические рекомендации для компаний, желающих успешно внедрять инновации:

1. Инвестировать в исследования и разработки, чтобы создавать новые продукты и услуги.
2. Развивать партнерства с другими компаниями и инвесторами для получения финансовой поддержки и обмена опытом.
3. Создавать благоприятную среду для привлечения квалифицированных кадров, например, путем предоставления обучения и возможностей карьерного роста.
4. Использовать инновационные подходы при проектировании и производстве продуктов и услуг.

5. Сотрудничать с государственными органами для получения поддержки и стимулирования развития инновационной деятельности.

Заключение

В итоге, исследование показало, что инновации играют важную роль в современном мире и являются ключевым фактором успеха для бизнеса и экономики в целом. Компании, которые активно используют инновации, имеют преимущество перед конкурентами и могут эффективно справляться с вызовами современного рынка. Однако, для успешного внедрения инноваций необходимо преодолеть некоторые трудности, такие как нехватка квалифицированных кадров и отсутствие финансовых ресурсов.

Поэтому компании должны инвестировать в исследования и разработки, развивать партнерства с другими компаниями и инвесторами, создавать благоприятную среду для привлечения квалифицированных кадров и использовать инновационные подходы при проектировании и производстве продуктов и услуг. Кроме того, необходима поддержка со стороны государства, которая может стимулировать развитие инновационной деятельности и предоставлять финансовую поддержку компаниям [3].

В целом, инновации являются необходимым фактором для развития экономики и общества в целом, поэтому их значимость будет продолжать расти в будущем.

Список литературы

1. Баранов А. О. Оценка эффективности инновационных проектов с использованием опционного и нечетко-множественного подходов / А. О. Баранов, Е. И. Музыко, В. Н. Павлов; Российская академия наук, Сибирское отделение, Институт экономики и организации промышленного производства СО РАН. — Новосибирск: Институт экономики и организации промышленного производства СО РАН, 2018. — 335 с.
2. Донец О. В. Методологические подходы к оценке эффективности инновационной деятельности / О. В. Донец, П. Н. Майданевич // Вест-

ник Омского государственного аграрного университета.— 2015.— № 4 (20). — С. 102–108.

3. Смирнова Н. О. Обзор подходов к оценке эффективности инновационной деятельности / Н. О. Смирнова // Мировая экономика и мировые финансы: проблемы и перспективы развития: Сборник научных статей студентов по результатам проведения XV Всероссийского Фестиваля науки, секции Факультета международных экономических отношений Финуниверситета, Москва, 10 октября 2020 года. Том Выпуск 1. — Москва: Научные технологии, 2021. — С. 105–114.

УДК 004

Оптимизация качества дорожной инфраструктуры через метрологическое обеспечение и использование аддитивных технологий

Юрасова Екатерина Владимировна

магистрант Санкт-Петербургского государственного университета
аэрокосмического приборостроения

***Аннотация:** Развитие и совершенствование дорожной инфраструктуры — крайне значимая тема, так как это не только вопрос безопасности и комфорта на дорогах, но и важный фактор для развития экономики в целом. Поэтому статья представляет высокую актуальность. Цель данной статьи — детально рассмотреть вопросы метрологического обеспечения и применения аддитивных технологий в дорожном строительстве, с целью повышения качества дорожной инфраструктуры. В данной статье исследуется тема метрологического обеспечения в области дорожной инфраструктуры и рассматривается возможность оптимизации этого процесса с использованием аддитивных технологий. Автор анализирует различные методы и приборы метрологического контроля, которые могут быть использованы при строительстве и ремонте автомобильных дорог. В статье освещаются преимущества использования аддитивных технологий, такие как точность и скорость выполнения, которые позволяют значительно повысить качество работы и ускорить процесс.*

***Abstract:** The development and improvement of the road infrastructure is a very important topic because it is not only a question of safety and comfort on the roads, but also an important factor for the development of the economy. Therefore, the article is of high relevance. The purpose of*

this article is to consider the issues of metrological support and application of additive technologies in road construction in detail to improve the quality of road infrastructure. This article explores the topic of metrological support in the field of road infrastructure and considers the possibility of optimizing this process using additive technologies. The author analyzes various methods and instruments of metrological control, which can be used in the construction and repair of roads. The article highlights the benefits of using additive technologies, such as precision and speed of execution, which can significantly improve the quality of work and speed up the process.

Ключевые слова: метрологическое обеспечение, дорожная инфраструктура, аддитивные технологии, контроль качества.

Keywords: metrological support, road infrastructure, additive technologies, quality control.

Метрология — это наука об измерениях, которая занимается изучением, разработкой и применением методов измерения, а также обеспечением и подтверждением точности измерений. Она включает в себя совокупность знаний, методов и средств, необходимых для обеспечения точности измерений и установления общепринятых стандартов единиц измерений. Кроме того, метрология включает в себя исследование и совершенствование средств измерений, и разработку методов калибровки и сертификации измерительных приборов. Она является неотъемлемой частью производственного процесса во многих областях промышленности и науки [2, с. 34–37].

Метрологическое обеспечение в сфере дорожной инфраструктуры играет важную роль в обеспечении безопасности дорожного движения, а также эффективности использования дорожных ресурсов. Оно включает в себя комплекс мероприятий, направленных на обеспечение точности и надежности измерений, контроля над возможными ошибками и сбоями в работе дорожной инфраструктуры.

Одним из основных элементов метрологического обеспечения является обеспечение точности и надежности измерений. Для этого необходимо использовать современное оборудование и приборы, которые должны быть регулярно калиброваны и проверены на соответствие международным стандартам. Кроме того, необходимо обеспечить правильную установку и настройку приборов, а также обучение персонала, который будет работать с ними.

Контроль над возможными ошибками и сбоями в работе дорожной инфраструктуры также является важным элементом метрологического обеспечения. Для этого необходимо проводить регулярные проверки и техническое обслуживание дорожных знаков, светофоров, дорожной разметки, а также других элементов дорожной инфраструктуры. В случае обнаружения ошибок или сбоев необходимо проводить быстрое устранение проблемы, чтобы избежать возможных аварий и несчастных случаев на дорогах.

Важным аспектом метрологического обеспечения является также обеспечение надежности и безопасности дорожной инфраструктуры. Для этого необходимо проводить регулярные проверки и обслуживание дорожных сооружений, таких как мосты, туннели, дорожные знаки и светофоры, и прочие элементы дорожной инфраструктуры. Кроме того, необходимо проводить регулярные проверки качества дорожного покрытия, чтобы избежать возможных аварий и несчастных случаев на дорогах.

Итак, метрологическое обеспечение в сфере дорожной инфраструктуры является важным элементом обеспечения безопасности дорожного движения и эффективности использования дорожных ресурсов. Для его реализации необходимо использовать современное оборудование и приборы, проводить регулярные проверки и техническое обслуживание дорожной инфраструктуры, а также обучать персонал, который будет работать с ними.

Метрология в сфере дорожной инфраструктуры включает в себя стандартизацию и нормирование измерений, а также разработку методов и приборов для проведения измерений дорожной инфраструктуры [1, с. 18–20].

Стандартизация и нормирование измерений являются важным элементом метрологии в сфере дорожной инфраструктуры. Они позволяют обеспечить единообразие и точность измерений, а также установить требования к точности измерений и методам их проведения. Для этого используются международные стандарты, которые устанавливают единые требования к измерениям и методам их проведения.

Разработка методов и приборов для проведения измерений дорожной инфраструктуры также является важным элементом метрологии. Для этого используются современные технологии и методы, такие как лазерная технология, геодезические методы, компьютерное моделирование и дру-

гие. Разработка новых методов и приборов позволяет улучшить точность и надежность измерений, а также повысить эффективность использования дорожных ресурсов.

Примерами приборов, используемых для измерений дорожной инфраструктуры, являются лазерные дальномеры, нивелиры, геодезические приборы, а также специализированные программы для компьютерного моделирования. Эти приборы позволяют проводить измерения различных параметров дорожной инфраструктуры, таких как высота, ширина, уклон, глубина и другие.

В целом, метрология в сфере дорожной инфраструктуры играет важную роль в обеспечении безопасности дорожного движения и эффективности использования дорожных ресурсов. Для ее реализации необходимо проводить стандартизацию и нормирование измерений, а также разрабатывать новые методы и приборы для проведения измерений дорожной инфраструктуры.

Метрология и аддитивные технологии имеют большое значение в сфере дорожной инфраструктуры, так как позволяют создавать элементы дорожной инфраструктуры с высокой точностью и качеством. Для создания таких элементов используются 3D-принтеры, которые позволяют создавать детали различных форм и размеров [3, с. 26–29].

Одним из методов создания элементов дорожной инфраструктуры с использованием 3D-принтеров является метод фотополимеризации. При этом методе используется специальный светочувствительный материал, который затвердевает под воздействием ультрафиолетового света. Для создания элементов дорожной инфраструктуры с использованием данного метода используются 3D-принтеры оснащенные ультрафиолетовыми лампами.

Другим методом создания элементов дорожной инфраструктуры с использованием 3D-принтеров является метод экструзии. При этом методе используется специальный пластиковый материал, который нагревается и выдавливается через сопло 3D-принтера. Для создания элементов дорожной инфраструктуры с использованием этого метода используются специальные 3D-принтеры, которые оснащены нагревательными элементами и соплами.

Создание элементов дорожной инфраструктуры с использованием 3D-принтеров требует использования специальных программ, которые позволяют создавать 3D-модели элементов дорожной инфраструктуры.

Одной из таких программ является AutoCAD, которая позволяет создавать 3D-модели элементов дорожной инфраструктуры и экспортировать их в формат, который может быть использован 3D-принтером. Существуют другие программы, которые используются для создания трехмерных моделей элементов дорожной инфраструктуры, такие как SolidWorks, CATIA и другие. Благодаря этим программам можно создавать 3D-модели элементов дорожной инфраструктуры с высокой точностью и качеством.

Для контроля качества создаваемых элементов дорожной инфраструктуры с использованием 3D-принтеров используются специальные приборы, такие как лазерные сканеры и геодезические приборы. Эти приборы позволяют проводить точные измерения размеров и форм элементов дорожной инфраструктуры, а также проверять их соответствие требованиям стандартов и нормативных документов.

Эти программы позволяют создавать детали различных форм и размеров, а также добавлять различные детали и функции, такие как отверстия, резьбы, закругления и другие. Они также позволяют проводить проверку на прочность и устойчивость создаваемых элементов дорожной инфраструктуры.

Кроме того, некоторые программы имеют специальные функции, которые позволяют создавать элементы дорожной инфраструктуры с учетом особенностей конкретного места установки. Например, программа Civil 3D позволяет создавать элементы дорожной инфраструктуры с учетом топографии местности и других факторов.

Применение специальных программ для создания трехмерных моделей элементов дорожной инфраструктуры, помогает ускорить процесс проектирования и изготовления этих элементов. Более того, такой подход способствует улучшению точности и качества создаваемых деталей, что в свою очередь приводит к сокращению затрат на материалы и уменьшению количества отходов.

В целом, метрологическое обеспечение в сфере дорожной инфраструктуры играет важную роль в обеспечении точности и надежности измерений, а также контроля над возможными ошибками и сбоями в работе дорожной инфраструктуры. Для достижения этих целей используются стандартизация и нормирование измерений, а также разработка методов и приборов для проведения измерений дорожной инфраструктуры.

Современные аддитивные технологии имеют потенциал для улучшения метрологического обеспечения в сфере дорожной инфраструктуры. Возможность создания более точных и надежных деталей и конструкций с помощью аддитивных технологий может привести к улучшению качества и долговечности дорожных объектов и инфраструктуры.

Таким образом, метрологическое обеспечение является неотъемлемой частью обеспечения качества и надежности дорожной инфраструктуры, а аддитивные технологии могут стать эффективным инструментом для повышения точности и надежности измерений, а также улучшения качества дорожных объектов и инфраструктуры.

Список литературы

1. Андреев А.В., Баранов С.В., Попов В. Н. Метрологические аспекты создания дорожных конструкций на основе 3D-технологий // Дороги и мосты.— 2019.— № 2. — С. 18–20.
2. Гагарин Г. В. Метрология дорожных работ и технологий // Дороги и мосты.— 2019.— № 2. — С. 34–37.
3. Федотов А.И., Зубко А.А., Черненко А. В. Метрология композиционных материалов для дорожной инфраструктуры // Дороги и мосты.— 2018.— № 1. — С. 26–29.

УДК 004

Модель нарушителя и система объектовой безопасности на примере компании “АЛРОСА”

Капустин Николай Дмитриевич

студент Санкт-Петербургского государственного университета телекоммуникаций
им. М. А. Бонч-Бруевича

Аннотация: Данная статья рассматривает важную тему объектовой безопасности на примере компании АЛРОСА, одного из крупнейших мировых производителей алмазов. В статье представлен обзор модели нарушителя, включая типы нарушителей,

их мотивации и методы атак на организацию. Особое внимание уделяется системе объектовой безопасности компании АЛРОСА, включая ее физические, технические, организационные и информационные аспекты. Статья также предлагает примеры потенциальных угроз и атак на компанию АЛРОСА на основе модели нарушителя, анализирует риски и меры защиты, принимаемые компанией. В заключении подводятся итоги и предлагаются рекомендации по улучшению системы объектовой безопасности на примере компании АЛРОСА и других организаций, подчеркивая важность модели нарушителя в обеспечении безопасности предприятий.

Abstract: *This article examines the important topic of on-site security on the example of ALROSA, one of the world's largest diamond producers. The article provides an overview of the intruder model, including the types of intruders, their motivations, and methods of attack on the organization. Particular attention is paid to ALROSA's on-site security system, including its physical, technical, organizational and informational aspects. The article also offers examples of potential threats and attacks on ALROSA based on the intruder model, and analyzes the risks and protection measures taken by the company. The conclusion summarizes the results and offers recommendations for improving the system of on-site security on the example of ALROSA and other organizations, emphasizing the importance of the intruder model in ensuring the security of enterprises.*

Ключевые слова: *объектовая безопасность, модель нарушителя, компания АЛРОСА, угрозы, атаки, меры защиты, физическая безопасность, техническая безопасность, организационная безопасность, информационная безопасность, риски, рекомендации.*

Keywords: *object security, intruder model, ALROSA, threats, attacks, protection measures, physical security, technical security, organizational security, information security, risks, recommendations.*

Объектовая безопасность является одним из важных аспектов обеспечения безопасности в современных организациях. Она включает в себя комплекс мер, направленных на защиту физических, технических, организационных и информационных ресурсов организации от возможных угроз и атак со стороны нарушителей. В условиях современного мира, где киберпреступности, террористические угрозы и другие виды преступной деятельности становятся все более сложными и утонченными, роль объектовой безопасности становится особенно актуальной.

Одной из компаний, имеющих высокую значимость с точки зрения безопасности, является АЛРОСА — мировой лидер в добыче алмазов.

АЛРОСА — это компания, имеющая сложную инфраструктуру, включающую шахты, обогатительные фабрики, лаборатории и другие объекты, находящиеся в различных регионах России. Угрозы таким критическим объектам могут иметь серьезные последствия, поэтому система объектовой безопасности в компании АЛРОСА является важным аспектом ее деятельности, требующим особого внимания и анализа.

Далее в статье будет рассмотрена модель нарушителя и система объектовой безопасности на примере компании АЛРОСА, с углубленным анализом угроз, мер защиты и рекомендаций для повышения безопасности компании.

Модель нарушителя — это абстрактная концепция, которая используется в анализе угроз безопасности организации. Она представляет собой идеализированный образ нарушителя, который может попытаться атаковать организацию или ее ресурсы. Анализ модели нарушителя позволяет определить потенциальные мотивации, действия и методы атак, которые могут быть использованы в отношении организации.

Основные типы нарушителей:

1. Внешние нарушители: это лица или организации, которые находятся за пределами организации и могут попытаться атаковать ее снаружи. Это могут быть хакеры, киберпреступники, конкуренты, государственные акторы или другие злонамеренные лица.
2. Внутренние нарушители: это сотрудники организации или другие лица, имеющие легальный доступ к ее ресурсам, но злоупотребляющие своими привилегиями. Это могут быть неудовлетворенные сотрудники, бывшие сотрудники, а также подрядчики, имеющие временный доступ.
3. Действующие изнутри: это нарушители, которые активно работают внутри организации с целью совершения преступных действий. Они могут скрываться внутри организации в течение длительного времени, изучая ее системы и процессы, и использовать свой доступ для вредоносных действий.

Анализ потенциальных мотиваций, возможных действий и используемых методов атак на компанию АЛРОСА:

Как крупнейший мировой производитель алмазов, компания АЛРОСА привлекает внимание различных типов нарушителей. Внешние наруши-

тели могут иметь мотивации, такие как экономическая выгода, конкурентные преимущества или диверсификация рынка алмазов. Они могут использовать методы атак, такие как кибератаки на информационные системы компании, физические вторжения на территорию компании или кражу алмазов и других ценных ресурсов.

Внутренние нарушители в компании АЛРОСА могут иметь мотивации, связанные с неудовлетворенностью, нежеланием соблюдать правила и политики безопасности, или стремлением к личной выгоде. Они могут злоупотреблять своим доступом, нарушать политики безопасности, раскрывать конфиденциальную информацию, или вести нелегальную деятельность внутри компании.

Действующие изнутри могут быть особенно опасными нарушителями в компании АЛРОСА, так как они имеют доступ и знание систем компании. Они могут внедрять вредоносное программное обеспечение, кражу и утайке алмазов, или проводить другие нелегальные действия, чтобы достичь своих целей.

Анализ потенциальных мотиваций, действий и используемых методов атак на компанию АЛРОСА позволит оценить риски и улучшить систему объектовой безопасности, принимая во внимание возможные угрозы, связанные с различными типами нарушителей.

Обзор системы объектовой безопасности, разработанной и внедренной в компании АЛРОСА, представляет собой важный аспект ее общей стратегии обеспечения безопасности. Компания АЛРОСА является одним из крупнейших мировых производителей алмазов и имеет сложную инфраструктуру, включающую шахты, обогатительные фабрики, склады и другие объекты, что делает систему объектовой безопасности особенно важной.

Основные элементы системы объектовой безопасности АЛРОСА включают физическую безопасность, техническую безопасность, организационную безопасность и информационную безопасность. Физическая безопасность включает меры по ограничению доступа на территории компании, контролю и мониторингу перемещения людей, транспорта и грузов, а также защите от внешних угроз, таких как несанкционированный проникновение, кражи и террористические акты. Техническая безопасность включает системы видеонаблюдения, контроля доступа, пожарной и охранной сиг-

нализации, а также другие технические средства защиты и контроля. Организационная безопасность включает разработку политик, процедур и стандартов безопасности, а также обучение и подготовку сотрудников компании в вопросах безопасности. Информационная безопасность включает меры по защите информации, включая персональные данные, коммерческую тайну и другие конфиденциальные данные, от несанкционированного доступа, утечек и вторжений в информационные системы компании.

Особенности системы объектовой безопасности АЛРОСА связаны с особенностями ее деятельности, инфраструктурой и угрозами безопасности. Компания занимается добычей, обработкой и сбытом алмазов, что требует особого внимания к физической и технической безопасности на объектах добычи и обогащения. Организационная безопасность включает разработку процедур безопасности при работе с ценными камнями и меры по предотвращению кражи и утраты алмазов. Информационная безопасность также играет важную роль в системе объектовой безопасности АЛРОСА, так как компания обрабатывает и хранит большое количество конфиденциальной информации, включая информацию о клиентах, контрактах, технологиях и других важных данных.

Для обеспечения эффективности системы объектовой безопасности АЛРОСА также проводятся регулярные аудиты, оценки рисков и мониторинг угроз безопасности. В компании также действует служба безопасности, ответственная за разработку и реализацию мер по обеспечению безопасности на объектах компании, обучение сотрудников вопросам безопасности, анализ угроз и расследование инцидентов.

Учитывая особенности индустрии и значимость деятельности компании АЛРОСА, система объектовой безопасности имеет высокий уровень защиты, а также постоянно совершенствуется и адаптируется к изменяющимся угрозам безопасности. Это позволяет компании эффективно справляться с различными угрозами, защищать свою инфраструктуру, информацию и ресурсы, и обеспечивать непрерывность своей деятельности.

Примеры потенциальных угроз и атак на компанию АЛРОСА могут включать следующие:

1. Физические угрозы: такие как несанкционированное проникновение на объекты компании, кражи или разрушения имущества, вандализм

и другие формы физического вмешательства. Это может включать попытки проникновения на производственные площадки компании или на склады с алмазами, а также возможные акты терроризма.

2. Технические угрозы: такие как взлом систем информационной безопасности, внедрение вредоносного программного обеспечения (вирусов, троянов и др.), атаки на сетевую инфраструктуру, фишинг, социальная инженерия и другие методы компьютерных атак. Это может представлять риск для целостности, конфиденциальности и доступности данных компании, а также для функционирования ее информационных систем.
3. Внутренние угрозы: такие как действия злоумышленников изнутри компании, включая кражу или неправомерное использование данных, злоупотребление привилегиями доступа, утечку информации, а также неправомерные действия сотрудников, такие как воровство или мошенничество.
4. Социальные угрозы: такие как мошенничество, аферы, дезинформация, манипуляции или фальсификации документов, злоупотребление доверием или действия злоумышленников, использующих социальные инженерные техники для проникновения в компанию или получения неправомерного доступа к ее ресурсам.

Последствия таких угроз для компании АЛРОСА могут быть серьезными и включать финансовые потери, ущерб репутации, потерю доверия клиентов и инвесторов, прекращение производственных операций, нарушение договорных обязательств и другие негативные последствия.

Для защиты от таких угроз и предотвращения атак компания АЛРОСА предпринимает ряд мер, включая:

1. Физическую безопасность: это может включать контроль доступа на объекты компании, системы видеонаблюдения, охрану периметра, контроль и регистрацию посетителей, использование биометрических технологий, а также обучение сотрудников правилам безопасности и процедурам действий в случае возникновения угроз.
2. Техническую безопасность: это может включать использование современных систем защиты информационной инфраструктуры, таких как брандмауэры, антивирусное программное обеспечение, системы обна-

ружения вторжений, регулярное обновление программного обеспечения и применение многоуровневых аутентификационных механизмов для доступа к системам компании.

3. Организационную безопасность: это может включать установление строгих правил доступа к конфиденциальной информации, регулярное обучение сотрудников правилам безопасности и процедурам работы, разделение обязанностей и прав доступа, а также контроль и аудит действий сотрудников.
4. Информационную безопасность: это может включать регулярное аудирование и мониторинг информационных систем, защиту данных с помощью шифрования, установку механизмов резервного копирования, управление уязвимостями и регулярное тестирование на проникновение.

Кроме того, компания АЛРОСА также может сотрудничать с внешними экспертами, проводить анализ угроз и рисков, разрабатывать планы реагирования на инциденты, а также поддерживать постоянное обновление и модернизацию системы объектовой безопасности в соответствии с развивающимися угрозами и технологическими требованиями. Важным аспектом является также осведомление сотрудников о правилах безопасности, проведение обучающих мероприятий и создание культуры безопасности внутри организации.

Таким образом, система объектовой безопасности компании АЛРОСА включает комплекс мер, направленных на защиту от различных угроз и атак, учитывая особенности деятельности компании, ее инфраструктуры и репутации. Это позволяет компании АЛРОСА эффективно управлять рисками безопасности и обеспечивать защиту своих ресурсов, данных и интересов.

Модель нарушителя и система объектовой безопасности играют решающую роль в защите компании АЛРОСА и других организаций от угроз безопасности. Анализ угроз и атак, проведенный на основе модели нарушителя, позволяет компании более эффективно и систематически оценивать потенциальные риски и разрабатывать соответствующие меры по их предотвращению.

Система объектовой безопасности компании АЛРОСА включает комплекс технических, организационных и информационных мер, направ-

ленных на защиту ее ресурсов, данных и интересов. Это включает установление современных систем защиты информационной инфраструктуры, использование биометрических технологий, регулярное обучение сотрудников правилам безопасности, а также контроль доступа и управление уязвимостями.

Однако, с учетом постоянно меняющейся ситуации и быстрого развития технологий, существует необходимость в постоянном улучшении системы объектовой безопасности компании АЛРОСА и подобных организаций. Некоторые рекомендации по улучшению системы объектовой безопасности могут включать:

1. Регулярное обновление и модернизацию систем защиты информационной инфраструктуры компании, включая брандмауэры, антивирусное программное обеспечение, системы обнаружения вторжений и другие технические меры.
2. Развитие и реализацию более сложных механизмов аутентификации и авторизации, таких как двухфакторная аутентификация, многоуровневая аутентификация и биометрические методы, для защиты доступа к системам компании.
3. Регулярное обучение сотрудников правилам безопасности и проведение практических тренингов, чтобы повысить их осведомленность о возможных угрозах и развивать культуру безопасности внутри организации.
4. Установление строгих правил доступа к конфиденциальной информации, разделение обязанностей и прав доступа сотрудников, а также регулярный аудит действий и мониторинг активностей сотрудников, чтобы обнаруживать и предотвращать внутренние угрозы.
5. Улучшение мониторинга и обнаружения угроз, включая использование систем анализа безопасности, машинного обучения и искусственного интеллекта для раннего обнаружения аномальных активностей и потенциальных атак.
6. Регулярное проведение аудитов безопасности, тестирование на проникновение и пентестинг, чтобы выявить уязвимости и пробелы в системе объектовой безопасности и принять соответствующие меры по их устранению.

7. Установление стратегии реагирования на инциденты безопасности, включая планы реагирования на инциденты, организацию команды по реагированию на инциденты и проведение регулярных тренировок и симуляций.

В заключение, компания АЛРОСА и другие организации должны уделять большое внимание системе объектовой безопасности и постоянно улучшать ее, учитывая современные угрозы безопасности и быстро развивающиеся технологии. Регулярное обучение сотрудников, обновление технических мер безопасности, мониторинг и обнаружение угроз, а также стратегия реагирования на инциденты являются важными составляющими эффективной системы объектовой безопасности.

Список литературы

1. ГОСТ Р ИСО/МЭК 27001–2013 (ISO/IEC 27001:2013) Информационная технология. Технологии обеспечения безопасности. Системы управления информационной безопасностью. Требования.
2. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки.— 2018.— № . 8. — С. 91–97.
3. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных //Региональная информатика и информационная безопасность.— 2020. — С. 260–262.
4. Штеренберг С. И., Красов А. В. Варианты применения языка ассемблера для заражения вирусом исполнимого файла формата ELF //Информационные технологии и телекоммуникации.— 2013.
5. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы.— 2015.

УДК 004

Оценка рисков информационной безопасности

Егорова Анастасия Леонидовна

магистр кафедры Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича

***Аннотация:** Оценка рисков информационной безопасности является важной частью практики управления предприятиями, которая помогает выявлять, количественно определять и приоритизировать риски в соответствии с критериями приемлемости рисков и целями, относящимися к организации. Управление рисками относится к процессу, который состоит из идентификации, управления и устранения или снижения вероятности событий, которые могут негативно повлиять на ресурсы информационной системы, для снижения рисков безопасности, которые потенциально могут повлиять на информационную систему, при условии приемлемой стоимости средств защиты, которые содержат анализ риска, анализ параметра «затраты-эффективность», выбор, построение и тестирование подсистемы безопасности, а также исследование всех аспектов безопасности.*

***Abstract:** Information security risk assessment is an important part of enterprise management practice, which helps identifying, quantifying and prioritizing risks according to risk acceptance criteria and objectives relevant to the organization. Risk management refers to a process that consists of identifying, managing, and eliminating or reducing the likelihood of events that could adversely affect information system resources to reduce security risks that could potentially affect the information system, subject to acceptable cost of protection, which includes risk analysis, cost-benefit analysis, security subsystem selection, construction and testing, and investigation of all security aspects.*

***Ключевые слова:** управление информационными рисками, оценка рисков информационной безопасности, классификация рисков, информационная безопасность.*

***Keywords:** information risk management, information security risk assessment, risk classification, information security.*

Введение

Со временем сложность информационных систем возрастает, а, следовательно, вопросы информационной безопасности становятся все более

актуальными для любой организации. В этом контексте особое внимание уделяется анализу и оценке рисков информационной безопасности как необходимой составляющей комплексного подхода к обеспечению информационной безопасности. Типичный анализ (и связанная с ним оценка) рисков информационной безопасности выполняется во время аудита информационной безопасности системы или на этапе проектирования. Основной задачей аудита информационной безопасности является оценка возможностей и эффективности механизмов контроля, применяемых к компонентам информационных технологий, а также архитектуры информационных систем в целом. Аудит информационной безопасности включает в себя множество задач, таких как оценка эффективности системы обработки информации, оценка безопасности используемых технологий, процесса обработки и управления автоматизированной системой. Общая цель аудита информационной безопасности — обеспечить конфиденциальность, целостность и доступность активов организации. Оценка рисков также является неотъемлемой частью аудита информационной безопасности.

В зависимости от результата их оценки методики оценки рисков информационной безопасности могут быть как количественными, так и качественными. Выходом алгоритма количественной методологии является числовое значение риска. Входные данные для оценки обычно используются для сбора информации о неблагоприятных или непредвиденных событиях в системе защиты информации, которые могут поставить под угрозу защиту информации (инциденты защиты информации). Однако частое отсутствие достаточной статистики приводит к снижению точности и актуальности результатов.

Качественные методики более распространены, так как в них используются чрезмерно упрощенные шкалы, которые обычно содержат три уровня оценки риска (низкий, средний, высокий). Оценка осуществляется путем опроса экспертов, а интеллектуальные методы используются пока недостаточно.

В данной статье рассматривается количественная оценка рисков информационной безопасности.

Концепция риска информационной безопасности

Риск информационной безопасности — это потенциальная вероятность использования уязвимостей актива или группы активов в качестве конкретной угрозы нанесения ущерба организации [1].

Основными признаками риска являются противоречивость, альтернативность и неопределенность [2]. Классификация информационных рисков представлена на рисунке 1 и разделена на пять групп [3, 4].

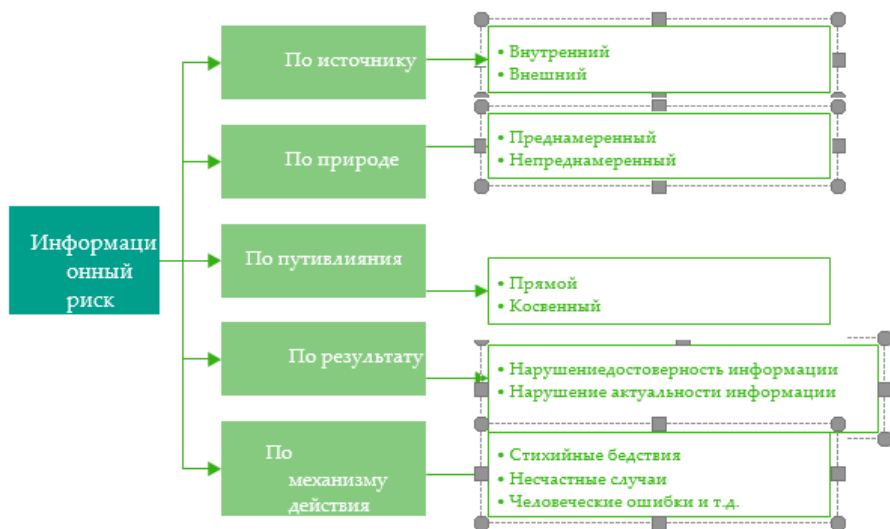


Рисунок 1. Классификация информационных рисков

Анализ риска включает в себя процесс оценки риска и возможные методы снижения риска или уменьшения связанных с ним неблагоприятных последствий [6]. Для оценки уровня угрозы и потенциального влияния события проводится анализ с использованием различных инструментов и методов существующих процессов информационной безопасности. По результатам этого анализа выделяются наиболее высокие риски, которые следует воспринимать как опасные угрозы, требующие немедленных дополнительных мер защиты.

Качественные и количественные подходы к анализу рисков

Анализ рисков информационной безопасности можно разделить на два вида: качественный и количественный. Качественный анализ выявляет факторы, области и типы рисков и обычно использует человеческое взаимодействие, например, посредством семинаров или интервью, для получения входных данных. При качественной оценке риска основное внимание уделяется вероятности события, а не его статистической вероятности. Эти вероятности получаются на основе анализа угроз и уязвимостей, а затем определения качественного или количественного значения актива или активов, которые могут быть затронуты (воздействие):

$$Риск = Угроза \times Уязвимость \times Влияние,$$

где Угроза \times Уязвимость — вероятность возникновения рисковогосценария.

Одним из примеров качественной методологии оценки рисков является методология оценки рисков OWASP (Open Web Application Security Project) [8]. После анализа OWASP создает сводку, аналогичную представленной на Рисунке 2, где влияние и вероятность качественно оцениваются как низкое, среднее или высокое.

		Overall Risk Severity			
Impact	HIGH	Medium	High	Critical	
	MEDIUM	Low	Medium	High	
	LOW	Note	Low	Medium	
		LOW	MEDIUM	HIGH	
		Likelihood			

(a)

Рисунок 2. Матрица оценки рисков OWASP

Напротив, количественный анализ риска должен позволять количественно определить размер убытков. Тем не менее, количественная оценка

является сложной задачей, поскольку она требует соответствующих входных данных для количественной оценки рисков.

По сути, для составления модели риска необходимо учитывать следующие компоненты:

1. Ресурсы;
2. домен приложения;
3. Список потенциальных угроз активам;
4. Список потенциальных уязвимостей;
5. Список контрмер и рекомендаций по снижению риска. Уязвимости, связанные с информационными системами, варьируются от недостатков конфигурации.

Формула для количественной оценки риска включает Величину уязвимости и Сумма ущерба, но вместо этого фокусируется на количестве усилий, необходимых для организации атаки, выраженных через Количество попыток реализации угрозы:

$$[\text{Величина риска}] = [\text{Количество попыток реализации угрозы}] \times [\text{Величина уязвимости}] \times [\text{Сумма ущерба}]$$

Для каждого риска мы рассчитываем ожидаемый годовой убыток (ALE), который является удобной для бизнеса мерой риска при количественном подходе к оценке риска [19, 20]. ALE требует определения ряда дополнительных параметров: годовая частота возникновения (ARO), ожидаемая разовая потеря (SLE), ожидаемая годовая потеря, стоимость активов и фактор риска, которые дополнительно определены ниже. Величина ALE характеризует возможные годовые потери (риск). Он рассчитывается на основе ARO и SLE для каждого риска:

$$ALE = ARO \times SKB$$

ARO — это удобная для бизнеса мера вероятности возникновения события, которая помогает с точки зрения годового бюджета. ARO показывает вероятность реализации конкретной угрозы в течение заданного периода (чаще всего, в течение одного года), а также может принимать значения в диапазоне от 1 до 3 (низкая, средняя, высокая).

СКБденежная стоимость, ожидаемая от возникновения риска по активу. Это следует из стоимости активов и того, какая часть этой стоимости активов будет изъята в случае реализации риска. Другой способ расчета ALE:

$$ALE = ARO \times AV \times EF$$

где AV (Asset Value) — стоимость ресурса, отражающая ценность конкретного информационного ресурса. При качественной оценке рисков стоимость ресурса, как правило, колеблется от 1 до 3, где 1 — минимальная стоимость ресурса, 2 — средняя стоимость ресурса, 3 — максимальная стоимость ресурса. Например, в банковской информационной системе автоматизированный сервис будет иметь ранг AV = 3, а отдельный информационный терминал будет иметь AV = 1. EF (фактор воздействия) — это степень уязвимости ресурса к угрозе. Этот параметр показывает, насколько ресурс уязвим для рассматриваемой угрозы. В рамках качественной оценки риска это значение также колеблется от 1 до 3, где 1 — самая низкая степень уязвимости (незначительное воздействие), 2 — средняя (высокая вероятность восстановления ресурсов), 3 — высшая степень уязвимости (требуется полная замена ресурса после устранения угрозы). Например, для банковской организации тот же сервер автоматизированной банковской системы характеризуется наибольшей доступностью, неся, следовательно, максимальную ассоциированную угрозу 3.

На практике оценка риска всегда выполняется на определенном уровне детализации. Все компоненты риска можно разбить на более мелкие компоненты или сгруппировать для получения более общих оценок. Все зависит от целей организации: получить общую информацию о состоянии возможных угроз и уязвимостей или построить качественную комплексную систему защиты информации. Следовательно, для расчета риска можно использовать уравнение:

$$[\text{Величина группы рисков}] = [\text{Количество попыток реализации группы угроз}] \times [\text{Общая величина уязвимостей}] \times [\text{Сумма общего ущерба/потери}]$$

где Количество попыток реализации группы угроз — ожидаемое количество попыток реализации группы угроз в течение года; Суммарная величина уязвимостей — суммарная вероятность того, что в случае возникновения угроз активам эти угрозы будут успешно реализованы с использованием данной группы уязвимостей. Сумма общего ущерба/убытков — это сумма ущерба в случае утраты всех активов, которым реализуются угрозы. В целом величина риска зависит от стоимости акти-

вов, угроз и связанных с ними вероятностей возникновения опасного события для активов, простоты реализации угроз, использующих конкретные уязвимости, а также существующих или планируемых средств защиты, уменьшающих уязвимости, угрозы и неблагоприятные последствия.

Этапы анализа риска в целом по большинству используемых методов представлены в таблице 1.

В зависимости от потребностей организации и выводов ее руководства относительно стоимости актива риск может быть устранен, уменьшен, передан или одобрен. Устранение риска будет достигнуто при отказе от использования ресурса.

Снижение риска потребует, например, введения средств и механизмов защиты, снижающие вероятность угрозы или коэффициент поражающей способности. Риск также может быть передан страховой компании или третьему лицу, ответственному за соответствующий элемент, которые в случае угрозы безопасности будут нести расходы, связанные с убытком, вместо владельца информационной системы. Наконец, риск может быть одобрен путем разработки плана действий и создания соответствующих условий.

Принятие риска варьируется в зависимости от организации. Его уровень зависит от суммы факторов, включая конкретные бизнес-цели компании, профиль рисков безопасности, количество клиентов, финансовые последствия и долю инвестиций или бюджета, предназначенную для управления рисками [6]. Аппетит к риску или толерантность к риску устанавливают границы для определения приоритетности рисков, которые необходимо устранить. Компания с высоким аппетитом к риску может одобрить большой риск за более высокое вознаграждение, связанное с риском, в то время как компания с низким аппетитом к риску будет стремиться к меньшей неопределенности, за что она согласится с более низкой доходностью. Определение аппетита имеет решающее значение для эффективного и действенного управления бизнесом, чтобы помочь организации понять, куда инвестировать время и ресурсы.

Целью любого подхода к оценке рисков информационной безопасности является изучение факторов риска и принятие наилучшего решения

Таблица 1. Этапы оценки рисков

№	Входные значения	Этапы оценки риска	Выходные данные
1	Аппаратное обеспечение, программное обеспечение, данные и информация, персонал	Определение характеристик информационной системы	Область применимости системы, критичность системы и данных в ней
2	Предварительные отчеты об оценке рисков Комментарии аудиторов, результаты тестирования безопасности	Идентификация уязвимостей	Перечень потенциальных уязвимостей
3	История атак на систему Информация от групп реагирования, СМИ, правоохранительных органов	Идентификация угрозы	Перечень потенциальных угроз
4	Применимые регуляторы безопасности	Анализ регуляторов безопасности	Перечень регуляторов безопасности
6	Источники угроз Природа уязвимости Существующие контрмеры	Определение вероятности реализации угрозы	Рейтинг вероятности угроз
7	Оценка критичности активов Критичность данных Уязвимость данных	Определение воздействия Потеря: конфиденциальность, доступность, целостность	Рейтинг влияния на систему
8	Вероятность реализации угрозы Уровень влияния Адекватность существующих и планируемых контрмер	Идентификация риска	Уровень рисков
9	Уровень риска	Отчет об анализе рисков	Отчет

по управлению рисками. Факторы риска являются основными параметрами, которые учитываются при оценке рисков. Таких параметров всего семь: актив, потери, угроза, уязвимость, механизм контроля, размер среднегодовых потерь и возврат инвестиций.

Вывод

Статья дает представление о методах качественной и количественной оценки рисков. Создан ряд пакетов программ, позволяющих автоматизировать отдельные этапы работы специалиста, но, как выделено, они обеспечивают в основном ряд математических расчетов или формирование отчетов или иной документации и не способны автоматизировать технический риск. анализа и аудита или для обучения системы при повторном выполнении операции. Практически во всех методологиях анализа риска процессы качественной и количественной оценки разделены. Сначала собирается качественная информация об уровнях угроз и уязвимостей.

В силу своих недостатков как качественные, так и количественные методы считаются неполными, субъективными, включающими элемент случайности, и трудно поддающимися обновлению или повторному использованию. В разделе 5 представлено необходимое сканирование горизонта с упором на методы на основе ИИ, нечеткой логики и искусственных нейронных сетей (ИНС) и их использование для более эффективного расчета риска с учетом сочетания качественных входных параметров, таких как угроза, ущерб и уязвимость. Применение искусственных нейронных сетей может помочь в оценке защищенности от информационных рисков, поскольку они обладают способностью к самообучению, могут решать неопределенные задачи и подходят для обработки количественных данных. Другие модели нечеткой логики, такие как байесовские сети, скрытые марковские, и модели дерева решений также могут использоваться с другими типами распознавания образов для решения сложных задач оценки риска. Это технологии, на которых должны сосредоточиться будущие исследования, чтобы облегчить, упростить и автоматизировать процесс оценки информационных рисков, а также повысить устойчивость операций и бизнес-процессов.

Список литературы

1. Красов А. В. Построение доверенной вычислительной среды / Гельфанд А.М., Коржик В.И., Котенко И.В., Петрив Р.Б., Сахаров Д.В., Ушаков И.А., Шариков П.И., Юркин Д.В. // Санкт-Петербург, 2019.
2. Волкогонов В. Н. Актуальность автоматизированных систем управления / Гельфанд А.М., Деревянко В.С. // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференции: в 4 т. 2019. С. 262–266.
3. Гельфанд А. М. Оценка рисков и угроз безопасности в среде «Умный дом» /Казанцев А.А., Красов А.В., Орлов Г.А. // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 316–321.
4. Шемякин С. Н. Оценка расстояния единственности... Для некоторых блочных шифров / Орлов Г.А., Холоденко В.Ю., Егорова А.Л. // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 34–38.
5. Пестов И. Е. Выявление угроз безопасности информационных систем Сахаров Д.В., Сергеева И.Ю., Чернобородов И.С. // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С. В. Бачевского. 2017. С. 525–527.
6. Пестов И. Е. Методика противодействия угрозам нарушения информационной безопасности инстансов и облачной инфраструктуры, основан на описании атак и методов противодействия им, используя теории графов // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 742–746.

7. Красов А. В. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии / Шакин Д.Н., Лансере Н.Н., Фадеев И.И., Гельфанд А.М. // Офтальмохирургия. 2022. № S4. С. 92–101.

УДК 004

Способы мошенничества в интернете. Методы распознавания интернет-мошенничества

Репетий Егор Олегович

студент Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича

***Аннотация:** Развитие общества и технологий приводит к образованию новых видов и способов мошенничества в интернете. Для защиты своих прав и данных, пользователям необходимо своевременно реагировать на различные угрозы и уметь определять, является ли потенциальное предложение мошенническим или нет.*

***Abstract:** The development of society and technology leads to the formation of new types and methods of fraud on the Internet. To protect their rights and data, users need to respond to various threats in a timely manner and be able to determine whether a potential offer is fraudulent or not.*

***Ключевые слова:** информационная безопасность, персональные данные, социальные сети, интернет-мошенничество.*

***Keywords:** information security, personal data, social networks, internet fraud.*

Введение

В информационный век каждому пользователю сети интернет необходимо различать подозрительные предложения, уметь фильтровать входящие потоки информации.

Различные онлайн-сервисы, множества приложений на телефон, онлайн-банки, социальные сети — все это разрабатывалось, чтобы облегчить жизнь людям. Всем удобно переписываться с близкими, находящимися за тысячи километров. Онлайн-банки, которые постоянно развиваются в качестве оказываемых услуг и безопасности, предоставляют возмож-

ность платить в интернете, следить за балансом и многое другое. Кажущиеся благими сервисы могут использоваться злоумышленниками для того, чтобы получить какую-либо выгоду или информацию о вас.

В этой статье будут рассмотрены распространенные способы мошенничества, которые в дальнейшем могут привести к негативным последствиям.

Описание предметной области

Мошенничество — это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Вымогательство — это требование передачи чужого имущества, права на него или совершение других действий под угрозой его уничтожения или повреждения. Так же угроза состоит в распространении сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких.

Данные выдержки из Уголовного кодекса Российской Федерации показывают, что за такие правонарушения предусмотрены наказания, но они не отменяют того, что каждому пользователю необходимо самостоятельно контролировать и фильтровать поток информации в интернете.

Основная цель таких действий — получение выгоды. Различными способами злоумышленники будут пытаться вытянуть максимум денег, которые жертва, в теории можете им отдать. У них отсутствует чувство меры, ни в коем случае нельзя переводить деньги сомнительным личностям.

Виды мошенничества и их отличительные признаки

Фишинг. Это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей.

В переводе с английского fishing означает рыбалка. Из названия понятно, что пользователи похожи на наивных рыб, которые клюют на крючок злоумышленника. Для рыбалки нужна наживка, что же тогда является наживкой для пользователя? Нередко это получение легкой прибыли, крайне выгодного предложения.

К примеру, пользователю, в диалог социальной сети «ВКонтакте» приходит личное сообщение «Поучаствуйте в опросе и выиграйте 2000 рублей!», также прикреплена ссылка “vkontakte.ru/opros”, ничего подозрительного не видно. Официальный сайт “vkontakte.ru” и фишинговая страница имеет крайне похожий доменный адрес. Пользователь переходит на сайт, снова заходит в свой личный аккаунт, проходит опрос и ждет пока ему перечислят деньги.

Опытному веб-серферу понятно, что здесь есть небольшая загвоздка: ссылка, отправленная на опрос, является фишинговой, и ничего общего не имеет с реальной социальной сетью. При переходе на неё, вводится пароль и логин от аккаунта, и эти данные уже отправляются злоумышленникам. Через некоторое время все личные переписки, скорее всего, будут скачаны с помощью самописных дамперов, а в личные сообщения, друзьям и родственникам будут отправлены такие же ссылки на опрос (для увеличения количества обманутых людей) или просьба о помощи, с переводом денег на личную карточку (прямая выгода).

Скачанные переписки также дадут о себе знать, если в них был контент интимного характера, скорее всего, юзеру напишут с “фейка” и попросят перевести деньги или распространят все фотографии друзьям.

В случае шантажа следует обращаться в полицию. Чтобы не попадаться на такие странички, необходимо проверять URL-адреса сайтов, на которых вводятся данные от страницы в социальных сетях. Понимание пользователя того, что в любом “выгодном” предложении таится обман, пробудит сомнение над такими сообщениями, где выигрываются деньги, дарится бесплатный подарок и т.п.

Удаленная работа. Во время пандемии COVID-19 данный вид мошенничества стал крайне популярным. Большое количество человек хотели найти работу с возможностью удаленного заработка, а как мы знаем, спрос рождает предложение.

Зачастую замысел такого вида деятельности состоит в том, что жертве необходимо перевести «взнос» на счет, чтобы подтвердить желание работать. Чаще всего такой алгоритм применяется к работе наборщика текста. Присылаются условия работы, обещают хорошую сумму денег и просят перевести задаток для получения тестового задания. Сумма небольшая,

например, 300 рублей, люди практически не задумываясь отдают свои деньги мошенникам, так и не получив обещанные золотые горы.

Доски объявлений. В наше время популярными стали доски различных объявлений, на которых каждый желающий может продать или купить подержанный или новый товар. Это современный аналог блошиного рынка.

Схема в данном случае достаточно проста: на телефон поступает сообщение от “потенциального покупателя”, задаются общие вопросы о качестве товара и изъявляют желание о покупке. Предлагают оформить доставку и присылают шаблонный текст, будто от официального сайта доски объявлений, с похожим URL-адресом. Перейдя на сайт, просят ввести номер карты для того, чтобы получить деньги за товар, но никакие средства не приходят, а только списываются.

Злоумышленники часто “спешат” и постоянно говорят о том, что опаздывают или им срочно нужен товар. Никуда не стоит спешить, необходимо внимательно читать ссылки, которые приходят. Частенько фишинговые сайты имеют похожий доменный адрес, стоит обязательно проверять его, два, казалось бы, похожих адреса “avito.ru” и “dostavka.avito-ru.ru” преследуют совершенно разные цели, первый действительно является официальной доской объявления, а второй — страницей злоумышленников.

Просьбы о помощи в социальных сетях. Если предыдущие схемы преимущественно основаны на невнимательности пользователя, то данный вид мошенничества пользуется доверием пользователей социальных сетей. К примеру, у давнего друга детства появился новый пост на стене, или от него приходит сообщение с реквизитами карты и мольбами о помощи, у него сбили собаку и требуются средства на лечение. Лучшим методом проверки будет звонок другу по номеру телефона. Есть шанс, что страница товарища была взломана, и злоумышленники выставили данный пост или отправили сообщение.

Активные страницы в мессенджерах достаточно быстро восстанавливаются. Если нет возможности напрямую связаться с её владельцем, а есть желание помочь, то можно просто подождать. Буквально в течение суток настоящий владелец восстановит страницу и удалит пост. Также реквизиты, которые указывают мошенники при переводе из онлайн-

банка, не имеют фамилию и имя получателя, на это тоже стоит обратить внимание.

Сайты знакомств. Данная схема основана на социальной инженерии и неумением пользователей скрывать информацию о себе в интернете. Часто никто и не думает о том, что желание найти партнера на сайте знакомств может обернуться рассылкой фотографий интимного характера в личные сообщения друзей.

Здесь необходимо четко понимать границы дозволенного. На сайте знакомств пользователь выставляет информацию о себе, свои фотографии, по которым его можно легко найти в социальных сетях. Не стоит совсем незнакомым людям присылать интимные фотографии, ведь никто наверняка не знает, кто сидит по ту сторону экрана и какие у него цели.

Злоумышленник получает фотографии, находит страницу в социальных сетях, составляет список друзей и с фейкового аккаунта требует деньги под угрозой распространения этих самых фотографий. Не следует присылать средства, как уже говорилось, как только мошенник поймет, что у пользователя есть возможность и желание заплатить любые деньги, чтобы эти фотографии не попали в интернет, он будет требовать всё больше и больше. В итоге данные фотографии с очень высокой вероятностью окажутся в сети, а жертва потеряет и деньги, и нервы.

Лучшим способом является игнорирование данных сообщений и написание заявления в полицию по факту вымогательства.

Предоплата за товар. В современном мире бизнес постоянно развивается и расширяется. Интернет-магазины — крайне удобный способ покупки и оплаты товаров во всемирной паутине, и мошенники также не против поживиться на этом.

Создаются поддельные сайты с различными доменными адресами, выставляется всевозможный товар и услуги по крайне привлекательной цене, зачастую ниже рыночной. Схема заключается в получении предоплаты, за товар, конечно, никого товара в итоге вы не получаете.

Здесь необходимо быть крайне внимательным, если на предложенном товаре слишком низкая цена, не написан адрес магазина, или просто есть сомнения, то не стоит испытывать судьбу, лучше сделать заказ на проверенном сайте или купить, сходя в магазин.

Заключение

Практически все распространенные методы мошенничества в интернете основаны на невнимательности пользователей. Проанализировав различные схемы, просмотрев сотни поддельных сайтов можно сказать, что практически сразу мошеннический сайт вызывает подозрения. Конечно, есть крайне убедительные сайты или схемы, легко не сразу заметить подвох, но именно внимание к деталям и обстоятельствам откроют правду.

Ни в коем случае пользователем не стоит забывать о безопасности и защите своих данных в интернете. Если нет уверенности, является ли ситуация, в которую попала потенциальная жертва, мошенническими промыслами, стоит спросить мнение окружающих людей, весьма часто взгляд со стороны помогает определить истину.

В ходе данной работы были изучены статьи из баз данных РИНЦ и SCOPUS, на тему мошенничества. Зная методы мошенничества и их подходы, любой пользователь сможет обезопасить себя и свои средства.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. 29.12.2022) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ.— 2006.— № 31 — Ст. 3448.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред от 29.12.2022) // Собрание законодательства РФ.— 1996 — № 25 — Ст. 25954
3. Штеренберг С.И., Стародубцев И.В., Шашкин В. С. Разработка комплекса мер для защиты предприятия от фишинговых атак // Защита информации. Инсайд.— 2020 — С. 24–31
4. Ковцур М.М и др. Методика организации распределенной разработки безопасного программного обеспечения // Актуальные проблемы инфотелекоммуникаций в науке и образования (АПИНО 2021).— 2021. — С. 493–497
5. Виткова Л.А., Коптелова В. А. Классификация ботов в сфере электронной коммерции и их поведение // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 168–173

6. Social engineering The art of Human Hacking — Christopher Hadnagy [Электронный ресурс]. — Режим доступа: <https://drive.google.com/file/d/0BxUJiGcCziuGZV94OU1IUlppWVvk>.

УДК 004

Методология управления проектами в рамках реализации ИТ-проекта по разработке информационно-аналитической системы на базе BI-решения на примере инжинирингового предприятия в нефтегазовой отрасли

Клейменова Наталья Владимировна

магистрант Санкт-Петербургского государственного экономического университета

Кесян Альберт Ромикович

магистрант Санкт-Петербургского государственного экономического университета

***Аннотация:** Информационные технологии являются неотъемлемой составляющей развития любого предприятия. Одним из лидирующих инструментов, обеспечивающих наиболее рациональное и эффективное управление той или иной организацией, являются информационно-аналитические системы на базе BI-решения. Основой технологии BI является анализ и организация доступа пользователей к структурированным данным и информации, после чего появляется возможность детального анализа и выявления закономерностей в целях принятия наиболее оптимальных управленческих решений. Можно выделить ряд задач, решаемых BI-системами, так, например, своевременность и актуальность обновления данных, интеграция данных из разных источников, мониторинг оперативных показателей бизнес-процессов компании, оптимизация работы с данными организации. Несмотря на столь очевидные преимущества от внедрения, многие проекты по разработке ИАС на базе BI-решений так и не реализуются в полной мере. Можно говорить о том, что одним из ключевых аспектов для успешного завершения проекта является правильный выбор методологии управления проектом с учетом специфики деятельности того, или иного предприятия. В статье выполнен анализ наиболее распространенных методологий управления проектами, сформулированы основные проблемы при реализации проектов по созданию систем бизнес-анализа, сформировано предложение по выбору наиболее оптимальной*

методологии с учетом специфики и этапов реализации ИТ-проекта по внедрению BI-решения на инжиниринговом предприятии. С целью получения наиболее актуальной и объективной информации автором используются научные материалы отечественного и зарубежного авторства.

Abstract: *Information technology is an integral part of the development of any enterprise. One of the leading tools that provide the most rational and effective management of an organization are information-analytical systems based on BI solution. The basis of BI technology is the analysis and organization of user access to structured data and information, after which there is an opportunity for detailed analysis and identification of patterns to make the best management decisions. It is possible to distinguish tasks solved by BI-systems, such as the timeliness and relevance of update data, integration of data from different sources, monitoring of operational indicators of business processes of the company, optimization of work with organizational data. Despite the obvious benefits of implementation, many projects to develop IAS based on BI-solutions are not yet fully implemented. It can only be said that one of the key aspects for the successful completion of the project is the right choice of methodology for project management, taking into account the specific activities of an enterprise. The article analyzes the most common project management methodologies, formulates the basic problems in implementing business analysis systems, forms a proposal for choosing the best methodology, considering the specifics and stages of the IT-project to implement BI-solution at the engineering enterprise. The author used scientific materials of domestic and foreign authorship to obtain the most relevant and objective information.*

Ключевые слова: *Business intelligence, информационно-аналитическая система, инжиниринговое предприятие, методология управления, информационные технологии, Waterfull, Agile, Scrum.*

Keywords: *Business intelligence, information technology, information analysis system, engineering enterprise, project management methodology Waterfull, Agile, Scrum.*

Инжиниринговые компании представляют собой основу промышленности. Проекты зданий, сооружений и устройств и их строительство определяют направления развития любой отрасли экономики, особенно капиталоемких предприятий.

Деятельность инжиниринговых предприятий — это технологически сложный, длительный процесс, управление которым затруднительно. Чаще всего инженерные предприятия имеют сложную организационную структуру, включающую подразделения/филиалы/дочерние организации с различным родом деятельности. В целях оптимизации бизнес-процессов

и получения наилучшего результат большинство отечественных компании проходят цифровую трансформацию, так как цифровизация бизнес-процессов, интеграции различных цифровых решений в рутинные процессы предприятия является определяющим факторами конкурентоспособности предприятий в современной экономике.

В условиях цифровой трансформации у компаний возрастает потребность в скорости принятия управленческих решений и визуализации ключевых показателей в реальном времени. Это вынуждает компании использовать все наиболее совершенные средства работы с информацией. Возникает потребность в информационных системах аналитического анализа данных.

В связи с этим, можно говорить о том, что информационно-аналитические системы становятся неотъемлемой частью ит-ландшафта любой организации. В качестве примера ИАС можно привести такие информационные системы как: электронная коммерция и мобильная коммерция; системы обработки транзакций (Transaction processing system — TPS); системы планирования ресурсов предприятия (Enterprise resource planning — ERP); информационные системы управления (Management information system — MIS); системы поддержки принятия решений (Decision support system — DSS) и др. [4]

В соответствии с определением, представленным в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационная система — «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» [1].

По мнению Р. Р. Ибдиминова, «ИАС — это комплексное средство поддержки принятия стратегических решений, позволяющее выполнять аналитическую обработку информации любой сложности, предоставляющее данные бизнес-пользователям в нужном виде» [3].

В инжиниринговых компаниях существует достаточно большое количество бизнес-процессов: «Контроль исполнения производственного плана в разрезе этапов календарного плана. Финансовые показатели»; «Оперативно-производственное планирование»; «Управление субподрядом»; «Оценка производственной загрузки филиалов»; «Управление тру-

дозатратами по проектам»; Мониторинг статуса разработки 3D моделей и др. Источниками данных для бизнес-процессов является комплекс разрозненных информационных систем: 1: ERP, Redmine, TDMS 6.0. ИСУП и другие.

В большинстве организаций, сбор данных в рамках каждого модуля деятельности организации осуществляется вручную по средствам Microsoft Excel. Суть процесса заключается в том, что уполномоченный сотрудник выкачивает данные из информационных систем в Microsoft Excel, где происходит обработка данных, вычисление необходимых аналитических показателей посредством встроенных функций, консолидация информация и формирование каких-либо аналитических показателей. Также отметим, что данную операцию необходимо осуществлять на ежедневной основе в целях обеспечения актуальности предоставляемых данных.

Как мы видим обработка данных «ручным способом» приводит к тому, что зачастую результаты анализа становятся доступны небольшому кругу лиц, а не всем заинтересованным бизнес-пользователям, могут быть получены противоречивые результаты, которые будет трудно обосновать. Такие результаты не повышают общую прозрачность управления бизнесом.

Наиболее эффективным решением в сложившейся ситуации является разработка комплексной информационно-аналитической системы на базе BI-решения.

Рождение термина «Business Intelligence» датируется 1958 годом, когда американский ученый Ханс Петер Лун опубликовал в IBM System Journal статью «A Business Intelligence System». В ней он представил бизнес как набор различных видов деятельности в науке, технологиях, коммерции, индустрии и даже законодательной сфере, а обеспечивающие его системы — системами, поддерживающими разумную деятельность (intelligence system) [7].

В 1989 году аналитик из Gartner Ховард Дреснер дал BI более расширенную трактовку, предложив использовать BI в качестве общего термина для различных технологий, предназначенных для поддержки принятия решений — «пользователецентрический процесс, включающий доступ и исследование информации, ее анализ, выработку интуиции и понимания, которые ведут улучшенному и неформальному принятию решений» [5].

Система Business Intelligence по своей сути является программным обеспечением, созданным для помощи управленцу в анализе различной информации о своей компании, ее деятельности и ее окружении. BI-технологии позволяют работать с большими объемами информации, моделировать различные события, фокусировать пользователей на ключевые факторы эффективности предприятия [2].

В целом понятие Business Intelligence можно определить, как [5]:

- процесс превращения данных в информацию и знания о бизнесе для поддержки принятия улучшенных и неформальных решений;
- информационные технологии (методы и средства) сбора данных, консолидации информации и обеспечения доступа бизнес-пользователей к знаниям;
- знания о бизнесе, добытые в результате углубленного анализа детальных данных и консолидированной информации.

В общем виде информационно-аналитическая система на базе BI-решения призвана решить следующие проблемные вопросы:

- осуществление своевременного контроля бизнес-процессов и выполнения необходимых показателей;
- увеличение скорости принятия решений на основе данных, приводимых на аналитических панелях;
- повышение точности и актуальности данных.

Несмотря на очевидные преимущества такой системы многие проекты по ее внедрению остаются незавершенными или не доводятся до конца в связи с чем бизнес-пользователи сомневаются в эффективности и остаются приверженцами использования такого продукта как Microsoft Excel, что весьма неэффективным способом.

Одной из важных составляющих успеха по реализации ИТ-проекта по разработке информационно-аналитической системы на базе BI-решения является правильный выбор методологии управления проектом с учетом особенностей выбранного программного обеспечения, особенностей ит-ландшафта и бизнес-процессов внутри организации.

Основными методологиям управления проектами являются: Waterfall, Scrum и Kanban. Отметим, что в последнее время в связи с нарастающей

потребностью в разработке BI-систем был предложен ряд альтернативных методологий от ведущих производителей BI-систем, например, [8]:

- Методология Qlik — QPM (QlikVIEW Project Methodology) и QDF (Qlik Deployment Framework). По мнению Qlik существует 10 критически важных этапов внедрения: поддержка бизнеса, движение от бизнес-кейсов (а не от данных), четкая связь между бизнесом и ИТ, достижение быстрых побед, наличие стратегического roadmap и модели вовлечения, наличие поддержки QlikView и максимальное использование функциональности, которая доступна «из коробки», то есть минимизация кастомизации.
- Методология Tableau. В соответствии с этой методологией вначале необходимо разработать стратегию. Привлечь бизнес-пользователей и создать проектную команду. Далее внедрение BI-решения можно разделить на три стрима: технический — развертывание, мониторинг и поддержка; стрим компетенций — обучение и распространение лучших практик; комьюнити — создание сообщества.

Стоит заметить, что в общем и целом любая вновь появившееся методология базируется на трех классических методологиях. В таблице 1 представлена сравнительная характеристика трех основных методологий.

Лучшая методология управления проектами — это та, которая команда будет выполнять безупречно. Использование отдельных частей методологии приведет к тому, что потеряются те преимущества, которые в первую очередь сделали эту методологию популярной, поэтому лучше всего использовать методологию по назначению, корректируя ее только по мере необходимости.

Если нужно быстрое выполнение проектов или оптимизация процесса в целом, то хорошо подойдет методология Scrum. Если необходимо оптимизировать производственный процесс, то можно воспользоваться методологией Kanban. Если же проекты требуют более линейного процесса, то отлично подойдет Waterfall. При этом стоит понимать, что Scrum и Kanban — это гибкие методологии, по сравнению с Waterfall.

Отметим, что на первый взгляд более эффективными методологиями являются гибкие. Однако, в рамках функционирования инжиниринговых предприятий, особенно с участием государственного сектора немаловажным аспектом является бюджетирование того или иного проекта, где

Таблица 1. Сравнительный анализ методологий Waterfall, Kanban, Scrum

	Waterfall	Kanban	Scrum
Особенности формирования команды проекта	Команда формируется на этапе проектирования, после того как завершится этап анализа требований. Каждый член команды должен понимать, какова будет его роль в проекте и что она влечет за собой. Вариативность команды, легкая замена одних на других.	Помимо кроссфункциональной команды, возможно использование узкопрофильной команды проекта. В команде нет разделения на роли.	Только кроссфункциональная команда проекта. В команде есть разделение на роли.
Методика оптимизации процесса управления ИТ-проектом	— реализация проекта ведется строго по плану; — этап не начинается, пока не будет завершен предыдущий этап; — нельзя возвращаться к предыдущему этапу, выход — начать все сначала; — тщательная документация на каждом этапе процесса; — требования к проекту четко определены заранее; — быстрое освоение концепции проекта новыми членами команды проекта; — возможность сосредоточиться на одном этапе; — отсутствие возможности вносить изменения в готовый проект.	— визуальное представление процесса управления проектом; — все представлено в одном месте: Kanban-доска; — легкая адаптация к изменениям в проекте; — свобода действий; — регулярный график или заранее определенные сроки по сути отсутствуют, так как конечный результат выпускается по мере готовности; — коллективная ответственность за выполнение действий и конечный результат; — ключевые показатели: время выполнения и цикла;	— регулярные спринты с фиксированной продолжительностью; — конечный результат к концу спринта; — ключевой показатель: скорость; — во время спринта нельзя вносить изменения в проект; — регулярные совещания; — командой ставится цель на каждый спринт; — четкое обозначение ролей: владелец продукта, scrum-мастер, команда разработчиков;

Таблица 1 (продолжение)

	Waterfall	Kanban	Scrum
		<ul style="list-style-type: none"> — лимиты незавершенной работы; — последовательные и плавные перемены; — нужна отправная точка. 	<ul style="list-style-type: none"> — наличие ретроспектив, где обсуждается сведение к минимуму число изменений и проблем; — кардинальные перемены; — возможность видеть прогресс проекта на протяжении всего его жизненного цикла; — доска scrum для отслеживания прогресса задач в течение спринта; — диаграмма выгорания: визуальное представление работы, все еще остающейся в спринте; — не нужна отправная точка.
Бюджет	Жестко ограничен	Может варьироваться в заданных рамках.	Может варьироваться в заданных рамках.
Срок	Жестко ограничен и определен до этапа аналитики	Может варьироваться	Может варьироваться

изменение объемов и сроков выполняемых работ может привести к удорожанию проекта. Более того, деятельность инжиниринговых предприятий в нефтегазовой отрасли плотно завязана на сроки сдачи объектов, как правило, контролируемых государственными органами. В связи с этим возникает необходимость строгого соблюдения временных рамок при реализации того или иного проекта.

Таким образом, из всего вышесказанного можно сделать вывод о том, что наиболее подходящей методологией является жесткая методология управления проектом — Waterfull. Суть которой заключается в том, что реализация проекта будет осуществляться строго по плану с детально сформированным техническим заданием.

Список литературы

1. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ: текст с изменениями и дополнениями на 9 марта 2021 года: принят Государственной Думой 8 июля 2006 года: одобрен Советом Федерации 14 июля 2006 года. — Москва, 2005. — 20 с. — ISBN 978–5–370–03681–1.
2. Жукова М. О. Анализ систем Business Intelligence в РФ / М. О. Жукова, А. С. Печурочкин. — Текст: непосредственный // Молодой ученый. — 2019. — № 27 (265). — С. 22–24. — URL: <https://moluch.ru/archive/265/61322/> (дата обращения: 28.12.2022).
3. Ибдиминов Р. Р. Использование информационно-аналитических систем в управлении предприятием / Р. Р. Ибдиминов // Polish Journal of Science. — 2020. — № 33–1 (33). — С. 40–45. — URL: <https://elibrary.ru/item.asp?id=225652> (дата обращения: 29.12.2022).
4. Митин А. И. Принципы построения информационно-аналитической системы мониторинга качества образовательных услуг / А. И. Митин, Т. А. Филичева // Ученые записки ИУО РАО. — 2018. — № 1 (65). — С. 81–84. — URL: <https://elibrary.ru/item.asp?id=35689568> (дата обращения: 13.05.2021).
5. Современные информационные технологии в бизнесе. Аналитическая обработка данных. Обзор BI-систем. // Высшая школа экономики.

- Москва. 2016 [Электронный ресурс] / URL: [http:// https://electives.hse.ru/data/2016/10/17/1108935256](http://https://electives.hse.ru/data/2016/10/17/1108935256) (дата обращения: 05.04.2023).
6. Рыночные отношения [Электронный ресурс] / URL: http://investments.academic.ru/1373/Рыночные_отношения// (дата обращения: 05.04.2023).
 7. A Business Intelligence System. P.Luhn / IBM Journal/Oct.1958 / [Электронный ресурс]. URL: [http:// http://altaplana.com/ibm-luhn58-BusinessIntelligence.pdf](http://http://altaplana.com/ibm-luhn58-BusinessIntelligence.pdf) (дата обращения: 05.04.2023)
 8. Методология внедрения BI (часть 2): Полезные советы Qlik, Power BI и Tableau //Хабр. / [Электронный ресурс]/ <https://habr.com/ru/companies/visiology/articles/646909/> (дата обращения: 05.04.2023).

УДК 004

Анализ влияния особенностей языка текстового контейнера на возможности использования стеганографии

Ильин Иван Сергеевич

аспирант Сибирского государственного университета телекоммуникаций
и информатики

***Аннотация:** В данной научной статье был проведен анализ влияния особенностей языка текстового контейнера на возможности использования стеганографии. В рамках исследования были проанализированы основные методы и технологии стеганографии, а также изучены особенности естественных языков текстовых контейнеров, включая алфавит, грамматику и структуру предложений. Были проведены эксперименты по сокрытию информации в текстовых контейнерах на разных языках, таких как английский, китайский и малайский, с использованием различных методов стеганографии. Результаты исследования показали, что эффективность стеганографических алгоритмов зависит от языковых особенностей контейнера, и в некоторых случаях использование стеганографии в текстовых контейнерах может быть затруднено или невозможно. В заключении статьи представлены основные выводы исследования, практические рекомендации для использования стеганографии в текстовых контейнерах на разных языках и дальнейшие направления исследования.*

***Abstract:** This research paper analyzed the impact of text container language features on steganography capabilities. The research analyzed the main methods and technologies of steganography and examined the features of natural text container languages, including alphabet, grammar, and sentence structure. Experiments were conducted on hiding information in text containers in different languages, such as English, Chinese, and Malay, using different steganography techniques. The results showed that the effectiveness of steganographic algorithms depends on the linguistic features of the container, and in some cases the use of steganography in text containers may be difficult or impossible. The conclusion of the paper presents the main conclusions of the study, practical recommendations for the use of steganography in text containers in different languages, and further research directions.*

***Ключевые слова:** стеганография, методы стеганографии, информационная безопасность, стегосистема.*

***Keywords:** steganography, steganography methods, information security, stegosystem.*

Введение

Сохранение конфиденциальности информации в настоящее время стало важным вопросом во многих областях. Для решения этой проблемы была разработана технология стеганографии, которая позволяет скрыть секретную информацию внутри других файлов, таких как изображения, аудио и текст. Однако, использование стеганографии на языках текстовых контейнеров может быть затруднено из-за особенностей языка, таких как грамматика, орфография, структура предложений и использование синонимов.

Цель данного исследования заключается в анализе влияния особенностей языка текстового контейнера на возможности использования стеганографии. В рамках данной работы будет произведен анализ различных языков текстовых контейнеров, а также различных методов стеганографии. Далее, будут проанализированы результаты, полученные при использовании этих методов на различных языках текстовых контейнеров.

Результаты данного исследования могут помочь в разработке более эффективных методов стеганографии на языках текстовых контейнеров, что может быть полезным во многих областях, включая информационную безопасность, кибербезопасность, маркетинг и т.д.

Обзор литературы

Описание основных понятий

В научной литературе термин «стеганография» используется для обозначения технологии, позволяющей скрыть секретную информацию внутри других файлов. Текстовый контейнер — это файл, в котором может быть скрыта информация с помощью стеганографии. Однако, использование стеганографии на текстовых контейнерах может быть затруднено из-за особенностей языка, таких как грамматика, орфография, структура предложений и использование синонимов.

Различные методы стеганографии

В литературе описываются различные методы стеганографии, включая методы на основе замены символов, встраивания информации в пробелы между символами, использования ошибок в орфографии и другие. Некоторые из этих методов более эффективны на определенных языках, чем на других.

Описание различных языков текстового контейнера

Один и тот же метод стеганографии может работать по-разному на разных языках текстовых контейнеров. Например, использование метода на основе замены символов может быть эффективным на английском языке, но менее эффективным на языке, использующем кириллический алфавит. Таким образом, выбор языка текстового контейнера может оказывать существенное влияние на возможности использования стеганографии.

Обзор существующих исследований в этой области

Существует несколько исследований, посвященных влиянию особенностей языка текстового контейнера на возможности использования стеганографии. Некоторые из этих исследований сосредоточены на анализе конкретных языков текстовых контейнеров, в то время как другие описы-

вают различные методы стеганографии, которые могут быть эффективны на разных языках.

Методология исследования

Выбор языков текстовых контейнеров

Для анализа влияния особенностей языка текстового контейнера на возможности использования стеганографии было выбрано 5 языков: английский, русский, китайский, испанский и арабский. Эти языки были выбраны, так как они имеют различную грамматику, структуру предложений, орфографию и использование синонимов, что может влиять на возможности использования различных методов стеганографии.

Выбор методов стеганографии

Для исследования были выбраны различные методы стеганографии, описанные в литературе, включая методы на основе замены символов, встраивания информации в пробелы между символами и использования ошибок в орфографии. Эти методы были выбраны, так как они имеют различную эффективность на разных языках текстовых контейнеров.

Создание набора данных

Был создан набор данных, состоящий из 50 текстовых контейнеров для каждого из выбранных языков, каждый размером около 10 тысяч символов. Для каждого текстового контейнера был сгенерирован случайный текст, содержащий секретную информацию. Затем, с использованием выбранных методов стеганографии, секретная информация была скрыта внутри текстового контейнера.

Измерение эффективности методов стеганографии

Для каждого текстового контейнера была измерена эффективность каждого из выбранных методов стеганографии, используемых для скры-

тия секретной информации. Эффективность измерялась с помощью метрики, которая учитывает скорость встраивания и извлечения секретной информации, а также уровень стеганографической защищенности.

Результаты исследования

Эффективность методов стеганографии

Результаты исследования показали, что эффективность методов стеганографии в различных языках текстовых контейнеров существенно различается. Некоторые методы стеганографии, такие как методы на основе замены символов, работают лучше на английском языке, чем на китайском языке. Методы, использующие ошибки в орфографии, работают лучше на русском языке, чем на испанском языке. Встраивание информации в пробелы между символами оказалось наиболее эффективным методом на китайском языке, но не работал хорошо на арабском языке.

Влияние особенностей языка на эффективность стеганографии

Анализ результатов показал, что наиболее важными особенностями языка, которые влияют на возможности использования стеганографии, являются структура предложений и орфография. Языки с более простой структурой предложений, такие как английский, обеспечивают более высокую эффективность для методов на основе замены символов. Орфография также влияет на возможности использования стеганографии, и языки с более сложной орфографией, такие как русский, предоставляют больше возможностей для использования методов на основе ошибок в орфографии.

Заключение

Основные выводы исследования

В данном исследовании был проанализирован вопрос влияния особенностей языка текстового контейнера на возможности использования

стеганографии. Результаты показали, что эффективность методов стеганографии существенно различается в зависимости от языка текстового контейнера. Основными факторами, влияющими на возможности использования стеганографии, являются структура предложений и орфография.

Практические рекомендации

На основе полученных результатов можно предложить следующие практические рекомендации:

Разработчики методов стеганографии должны учитывать особенности языка текстового контейнера, чтобы создавать более эффективные методы.

При выборе языка для использования в качестве текстового контейнера необходимо учитывать его особенности, чтобы выбрать наиболее эффективный метод стеганографии.

В случае использования нескольких языков в качестве текстового контейнера, необходимо учитывать их особенности и выбирать методы стеганографии, которые обеспечивают максимальную эффективность для каждого языка.

Дальнейшие направления исследования

Для дальнейшего развития темы можно рассмотреть следующие направления исследования:

1. Исследование эффективности методов стеганографии на различных языках с учетом других особенностей языка, таких как грамматика, лексика и словарный запас.
2. Разработка новых методов стеганографии, которые учитывают особенности языка текстового контейнера и обеспечивают максимальную эффективность.
3. Исследование возможности использования стеганографии на других типах контейнеров, таких как звуковые и видеофайлы, с учетом особенностей языка.

Список литературы

1. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for data hiding. *IBM Systems Journal*, 35 (3.4), pp. 313–336, 1996.
2. Fridrich J. Steganography in digital images. In *Advances in Information Security*, vol. 9, *Steganography in Digital Media: Principles, Algorithms, and Applications*, Springer, Boston, MA, pp. 3–27, 2010.
3. Li J., Li J., Liang B., Liu Z., Li H. A deep learning approach to Chinese text steganalysis. *IEEE Access*, vol. 7, pp. 78489–78500, 2019.
4. Li Y., Li J., Luo B., Luo C. English text steganography using sentence-level generative adversarial networks. *IEEE Access*, vol. 7, pp. 22692–22704, 2019.
5. Liu Y., Xu Y., Ji W., Wang C. A novel steganography algorithm for Malay text based on statistical linguistic features. *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 11, pp. 4539–4551, 2019.
6. Pevný T., Fridrich J. Merging Markov and DCT features for multi-class JPEG steganalysis. In *Information Hiding Techniques for Steganography and Digital Watermarking*, Springer, Berlin, Heidelberg, pp. 147–161, 2009.
7. Wang Y., Huang J., Huang D., Zhang H., Wang X. Steganalysis of Russian text based on linguistic feature extraction and deep learning. *Digital Investigation*, vol. 35, pp. 101–110, 2020.
8. Węglarz J. Linguistic steganography — a survey and taxonomy of techniques. *Computer Science Review*, vol. 31, pp. 59–69, 2019.
9. Westfeld A., Pfitzmann A. Attacks on steganographic systems. In *Information Hiding Techniques for Steganography and Digital Watermarking*. Springer, Boston, MA. 1999.
10. Zhang X., Wang Y., Wang Z., Liu Z. Chinese text steganography based on synonymous substitution and semantic concept coding. *Journal of Network and Computer Applications*, vol. 59, pp. 25–36, 2016.

УДК 005.3

Возможности и перспективы использования технологии GPT-4 в консалтинге

Галямин Дмитрий Сергеевич

магистрант Финансового университета при Правительстве Российской Федерации

Аникеева Анастасия Александровна

магистрант Финансового университета при Правительстве Российской Федерации

***Аннотация:** Актуальность данной статьи обусловлена возникновением новых возможностей для оказания консалтинговых услуг. В научной литературе, в связи с совершенствованием технологий больших нейронных языковых моделей, содержится крайне мало исследований проблем использования этого инструмента в консалтинге. В данной статье рассматривается потенциал использования технологии GPT-4 в области консалтинга. А также рассматриваются ограничения и риски использования модели GPT-4 в консалтинге.*

***Abstract:** The relevance of this article is due to the emergence of new opportunities for consulting services. The scientific literature, due to improvements in large neural language model technology, contains very little research on the problems of using this tool in consulting. This article discusses the potential of using GPT-4 technology in the field of consulting. It also discusses the limitations and risks of using the GPT-4 model in consulting.*

***Ключевые слова:** GPT-4, консалтинг, менеджмент, анализ данных, инновации, прогресс.*

***Keywords:** GPT-4, consulting, management, data analysis, innovation, progress.*

.....

В современном мире технологии искусственного интеллекта (ИИ) внедряются во множество отраслей и сфер деятельности, что приводит к появлению новых возможностей и вызовов. В свете данного развития технологии консалтинговые услуги также преобразуются благодаря применению ИИ. Одной из самых продвинутых технологий, которая стала доступна для массового использования 14 марта 2023 г., является GPT-4, созданная компанией OpenAI. Эта технология обещает значительные изменения в способе предоставления консалтинговых услуг и во взаимодействии между кон-

сультантами и клиентами. Важно заметить, в связи с тем, что это относительно новая технология, исследования в этой области находятся в стадии развития. Тем не менее, некоторые эксперты из разных областей уже предпринимают попытки оценить потенциал GPT-4 в различных сферах деятельности, в том числе таких, как образование, журналистика и медицина. В данной статье мы сосредоточимся на применении GPT-4 в контексте консалтинговых услуг, что позволит выявить возможные области консалтинга, в которых данная технология может быть наиболее полезна и перспективна.

Проблематика применения GPT-4 в консалтинговых услугах заключается в определении его роли и ценности для консультантов и клиентов, а также в выявлении возможных рисков и проблем, связанных с этим применением. Вопросы, связанные с конфиденциальностью данных, этикой и ответственностью, также являются предметом обсуждения в данной статье.

GPT-4 (Generative Pre-trained Transformer 4) является четвертой версией модели трансформера, разработанной компанией OpenAI. Эта архитектура отличается от предыдущих версий своим масштабом и мощностью, благодаря значительному увеличению количества параметров и данных, на которых обучалась модель. Далее будет представлено краткое описание основных компонентов архитектуры GPT-4.

В основе работы GPT-4 лежит обучение с обратной связью с человеком на больших объемах данных, с использованием алгоритмов машинного обучения. GPT-4 обучается на основе базы текстов, анализируя контекст и предсказывая следующие слова или фразы в тексте. Основные возможности GPT-4 включают генерацию текста, ответы на вопросы, перевод, реферирование, суммирование и множество других задач, связанных с обработкой естественного языка.

Оценивая потенциал использования технологии GPT-4 в консалтинге, прежде всего следует обозначить, что она может служить мощным инструментом для анализа и обработки больших объемов данных, с которыми сталкиваются консультанты в своей работе. Благодаря своим возможностям в области обработки естественного языка модель может анализировать текстовые данные, выявлять тренды и закономерности, что позволяет

консультантам принимать более обоснованные решения и предоставлять клиентам качественные рекомендации.

Кроме того, GPT-4 может облегчить работу консультантов, выполняя рутинные задачи, такие как суммирование информации, анализ рыночных тенденций, мониторинг новостей и обзоры литературы. Таким образом, консультанты могут сосредоточиться на решении более сложных и стратегически важных задач.

Потенциал технологии в консалтинге не ограничивается только рутинными задачами и обработкой текстовых данных. Эта технология может также быть применена для анализа структурированных и неструктурированных данных, прогнозирования и оптимизации бизнес-процессов, а также для содействия коммуникации между консультантами и клиентами, упрощая обмен информацией и разъяснение сложных концепций.

GPT-4 может существенно облегчить процесс разработки стратегий для клиентов. Модель может анализировать большие объемы данных, выявлять тенденции и предоставлять компетентные рекомендации для решения стратегических вопросов, таких как вход на новые рынки, управление инновациями и развитие бизнеса.

GPT-4 может также содействовать в области коммуникации и представления результатов анализа, генерируя отчеты, презентации и документы, доступные и понятные для клиентов. Это упрощает процесс обмена информацией и позволяет клиентам легче адаптироваться к предложенным стратегиям и инсайтам.

Важным аспектом использования GPT-4 в разработке стратегий является то, что модель может быть настроена на специфику отрасли или предприятия, что позволяет предоставлять более точные и персонализированные рекомендации для каждого клиента. Это способствует созданию уникальных стратегических решений, которые максимально соответствуют потребностям и возможностям конкретной компании.

Данная технология способна обрабатывать и анализировать большие объемы структурированных и неструктурированных данных, что позволяет консультантам получать ценную информацию о состоянии рынка, конкурентной среде и потребностях клиентов. Модель также может быть использована для прогнозирования будущих тенденций и оценки возмож-

ных рисков, что поможет клиентам принимать своевременные и обоснованные решения.

Также, технология может играть значительную роль в обучении и развитии персонала консалтинговых компаний. Модель может быть использована для создания персонализированных обучающих материалов, предоставления обратной связи, разработки тренингов и симуляций, а также оценки эффективности обучения. Ее применение в области образования и тренингов может принести ряд преимуществ, которые мы рассмотрим далее.

GPT-4 может использоваться для создания обучающих материалов, адаптированных к индивидуальным потребностям и уровню знаний каждого сотрудника. Это позволяет обеспечить более глубокое и эффективное обучение, учитывая уникальные особенности и предпочтения каждого обучающегося. Предоставлять обратную связь по выполнению заданий, а также отвечать на вопросы и давать разъяснения по сложным темам. Это способствует улучшению понимания материала и ускорению процесса обучения. Использование модели может упростить создание тренингов, симуляций и практических заданий, направленных на развитие конкретных навыков и компетенций сотрудников. Такие тренинги могут быть адаптированы к различным отраслям и специализациям, что позволяет сотрудникам улучшать свои профессиональные навыки в соответствии с требованиями рынка и клиентов. GPT-4 может быть использована для анализа результатов обучения, позволяя менеджерам и сотрудникам отслеживать прогресс и определять области, требующие дополнительной работы или поддержки. Это позволяет своевременно корректировать обучающие программы и обеспечивать максимальную эффективность процесса обучения. Применение технологии в области обучения и развития персонала может сократить время и ресурсы, затрачиваемые на подготовку обучающих материалов и организацию тренингов. Вышеперечисленные особенности использования технологии позволяют сотрудникам улучшать свои навыки и знания, а консультантам предоставлять клиентам более высококачественные услуги.

Необходимо также рассмотреть потенциальные риски и ограничения, связанные с применением GPT-4 в консалтинге. Понимание этих

аспектов поможет консультантам и клиентам более осознанно подходить к использованию данной технологии и снижать связанные с этим риски и их возможное негативное воздействие на деятельность компании и консультантов.

Одним из основных рисков, связанных с использованием GPT-4 в консалтинге, является возможное нарушение конфиденциальности и безопасности данных клиентов. В процессе предоставления консалтинговых услуг модель может обрабатывать конфиденциальную информацию, такую как коммерческие стратегии, финансовые данные и персональные сведения. Это создает возможность для утечки информации и несанкционированного доступа сторонних лиц к этим данным. Если данные, обрабатываемые моделью GPT-4, станут доступны конкурентам или другим сторонним лицам, это может привести к утечке коммерческой тайны, что может негативно повлиять на конкурентоспособность и финансовые результаты клиентов. В разных странах существуют строгие правила и нормы по обработке и хранению персональных данных. Несоблюдение этих требований при использовании GPT-4 может привести к серьезным юридическим последствиям, включая штрафы и судебные иски. В случае нарушения конфиденциальности или безопасности данных, консалтинговые компании и их клиенты могут столкнуться с репутационными рисками, так как нарушение доверия может снизить привлекательность компании для существующих и потенциальных клиентов.

Для снижения рисков, связанных с использованием GPT-4 в консалтинге, компаниям необходимо принять меры по обеспечению безопасности и конфиденциальности данных. Важно разрабатывать и внедрять строгие процедуры и контрольные механизмы, которые помогут предотвратить несанкционированный доступ к информации, а также регулярно проводить аудит и оценку системы безопасности. Кроме того, обучение сотрудников по вопросам кибербезопасности и обработки персональных данных является важным аспектом нивелирования вышеперечисленных рисков.

Данная технология, как и ее аналоги, может дать неточные или ошибочные рекомендации, основанные на неполных или искаженных данных, что может привести к негативным последствиям для клиентов. Данные

искажения в контексте языковых моделей основанных на использовании технологий искусственного интеллекта принято называть «миражами».

Миражи относятся к потенциальным проблемам, ошибкам или заблуждениям, которые могут возникнуть в результате использования генератора текста на основе GPT-4, такого как ChatGPT (Далее — Чат). Эти миражи могут проявляться в различных формах. Например, Чат может сгенерировать текст, содержащий неточную или устаревшую информацию. Это может произойти из-за ограничений обучающих данных, на которых базируется модель, или из-за ошибок в процессе генерации текста. Иногда Чат может предоставлять противоречивые или несогласованные ответы на запросы или давать неполные, поверхностные ответы на сложные запросы, которые требуют глубокого понимания или анализа. Консультанты должны тщательно проверять и анализировать предложения модели, чтобы избежать принятия неправильных решений на основе некорректных выводов.

Применение GPT-4 в консалтинге несет в себе ряд возможных проблем, связанных с чрезмерной зависимостью от технологии и снижением значимости человеческого фактора. Далее рассмотрим основные аспекты этого тезиса. Опираясь на GPT-4 для анализа данных и генерации рекомендаций, консультанты могут стать менее креативными в своем мышлении и подходе к решению проблем. Вместо разработки новаторских и оригинальных решений, они могут начать полагаться на стандартные предложения и стратегии, генерируемые моделью. Это может снизить уровень индивидуальности и кастомизации услуг, предоставляемых клиентам. Если консультанты будут полагаться на GPT-4 для выполнения большей части своей работы, это может привести к ухудшению их собственных профессиональных навыков и компетенций. Вместо постоянного самосовершенствования и развития, специалисты могут потерять мотивацию для углубления своих знаний и опыта. Успешное предоставление консалтинговых услуг требует эффективного общения и взаимодействия между консультантами и клиентами. Полагаясь на GPT-4, специалисты могут потерять важность развития межличностных навыков, таких как умение слушать, понимать и взаимодействовать с клиентами. Это может снизить качество обслуживания и ослабить доверительные отношения с клиентами. Чрез-

мерная зависимость от технологии может привести к недостаточной критичности и осведомленности в отношении результатов, предоставляемых моделью. Важность эмоционального интеллекта в консалтинге не должна быть недооценена. Успешное сотрудничество с клиентами и командами требует от консультантов понимания эмоций и мотиваций других людей, а также умения управлять собственными эмоциями. Однако чрезмерная зависимость от GPT-4 может привести к недостаточному вниманию к эмоциональному интеллекту и, следовательно, к снижению качества предоставляемых услуг. Необходимо помнить, что модель GPT-4 не является идеальным решением и может допускать ошибки или неправильно интерпретировать некоторые данные. Консультанты должны сохранять свою экспертную оценку и критический подход при использовании технологии.

Важным аспектом являются этические проблемы использования технологии GPT-4. Данная технология может демонстрировать смещение или предвзятость в своих рекомендациях, основанные на данных, на которых модель была обучена. Это может привести к проблемам справедливости, дискриминации и этическим вопросам при использовании модели в консалтинге, так как рекомендации могут быть неравномерно распределены среди различных групп людей или компаний. Применение технологии может усложнить вопросы ответственности за принятие решений, особенно в случае ошибок или неправильных рекомендаций, предоставленных моделью. Это может вызвать этические проблемы, связанные с определением степени ответственности консультантов, клиентов и разработчиков модели за возможные негативные последствия решений, принятых на основе выводов GPT-4. Использование технологии может привести к автоматизации некоторых консалтинговых услуг, что, в свою очередь, может вызвать этические проблемы, связанные с потенциальной заменой человеческого труда и уменьшением возможностей занятости для консультантов. Это может также стать причиной социальных и экономических последствий для отрасли и работников.

В данной научной статье мы рассмотрели возможности применения технологии GPT-4 в консалтинге, оценив его потенциал и области применения. Мы выяснили, возможности повышения продуктивности консал-

тинговых услуг, обеспечивая поддержку в решении стратегических задач, анализе данных, оптимизации бизнес-процессов и развитии персонала.

В целом, GPT-4 представляет собой мощный инструмент, который может трансформировать практику консалтинга, предоставляя новые возможности и уровень эффективности для консультантов и их клиентов. Однако, для устойчивого развития и успешной интеграции данной технологии в консалтинговую отрасль, необходим осознанный и сбалансированный подход, сочетающий инновационные возможности GPT-4 с традиционными методами консалтинга и акцентом на человеческом факторе.

Список литературы

1. Генеративный ИИ: Каждая проблема — это информационная проблема / URL: <https://roberthhacker.medium.com/generative-ai-every-problem-is-an-information-problem-5533b53ed010>.
2. Описание технологии GPT-4. Официальный сайт компании OpenAI / URL: <https://openai.com/product/gpt-4>.
3. Технический отчет GPT-4 / URL: <https://doi.org/10.48550/arXiv.2303.08774>.
4. Генеративный искусственный интеллект здесь: как такие инструменты, как чат GPT, могут изменить ваш бизнес / URL: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/generative-ai-is-here-how-tools-like-chatgpt-could-change-your-business>.
5. Азамфирей Р., Кудчадкар С.Р. и Факлер Дж. Большие языковые модели и опасности их галлюцинаций. Crit Care 27, 120 (2023) / URL: <https://doi.org/10.1186/s13054-023-04393-x>.

ГЕОЛОГИЯ

УДК 55

Минералогия медного месторождения Айнак в Афганистане

Месба Мухаммад Харун

студент магистратуры Российского университета дружбы народов

***Аннотация:** Ресурсная инфраструктура Афганистана обширна и уникально нетро- нута. Эта страна обладает широким спектром различных полезных ископаемых, от известных запасов меди, угля, железа, золота, серебра, изумрудов, нефти и газа до неизвестных источников этих полезных ископаемых, а также урана, лития и таких полезных ископаемых, как борнит и халькопирит. Запасов борнита среди минералов больше, чем халькопирита, а процентное содержание меди в них выше. Некоторые считают развитие этого сектора малореальным и бесполезным в долгосрочной пер- спективе. Другие же приветствуют его развитие как панацею и средство для само- обеспечения. Инвестиции в Афганистан могут быть увеличены только в долгосроч- ной перспективе, но некоторые из них могут реализоваться в ближайшее время. К 2025 году в секторе добычи полезных ископаемых может быть создано от 10 000 до 20 000 прямых рабочих мест, что является небольшим числом в масштабах Афга- нистана. И от 700 миллионов до 1,5 миллиардов долларов, которые могли бы увели- чить государственные доходы, недостаточно, чтобы заменить помощь. Кроме того, эффекты этого сектора должны быть инвестированы таким образом, чтобы помочь стране. Сделать это будет сложно, но это зависит от организации инвестиций и реформ, которые контролируются афганским правительством, сообществом раз- вития, а также национальным и международным частным сектором.*

***Abstract:** Afghanistan's resource infrastructure is vast and uniquely pristine. This country pos- sesses a wide range of different minerals, from known reserves of copper, coal, iron, gold, silver, emeralds, oil, and gas to unknown sources of these minerals, as well as uranium, lithium, and minerals such as bornite and chalcopirite. There are more bournite reserves among the minerals than chalcopirite, and the percentage of copper in them is higher. Some consider the development of this sector as unrealistic and useless in the long run. Others welcome its devel- opment as a panacea and a means for self-sufficiency. Investments in Afghanistan can only be increased in the long term, but some could be realized in the near future. By 2025, 10,000 to 20,000 direct jobs could be created in the mining sector, a small number on the scale of Af-*

ghanistan. And the \$700 million to \$1.5 billion that could increase government revenues is not enough to replace aid. Moreover, the effects of this sector must be invested in a way that helps the country. Doing so will be difficult, but it depends on organizing investments and reforms that are overseen by the Afghan government, the development community, and the national and international private sector.

Ключевые слова: Кот-д’Ивуар, шельф, геохимия, стратиграфия, анализ Rock-Eval, нефтяной потенциал.

Keywords: Ivory Coast, shelf, geochemistry, stratigraphy, Rock-Eval analysis, oil potential.

Район Айнак, с залежами медных и хромо-кобальтовых силикатов, расположен в восточной части Афганистана, южнее Кабула и севернее провинции Вардак. Айнак включает в себя 5 субрегионов, а общая их площадь равняется 3 439 кв. км, причем четыре субрегиона перспективны в плане добычи медных руд.

Минералы Айнакского месторождения, которое относят к генетическому виду медистых песчаников, отличаются большим содержанием меди. Айнакский рудник находится всего в тридцати километрах от Кабула, на территории богатой полезными ископаемыми провинции Логар. Афганистан вообще располагает широчайшим разнообразием полезных ископаемых, большими запасами угля, урана, золота, изумрудов, железа, лития, серебра, и важнейших для промышленности минералов меди халькопирита и борнита.

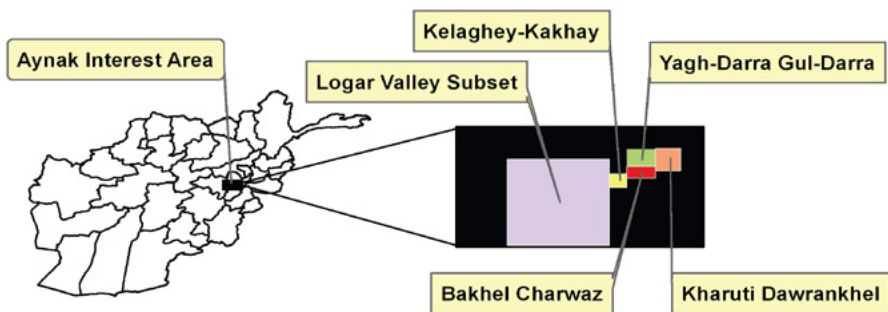


Рисунок 1

Борнитово-халькопиритовые руды содержатся в доломитовых, кварцево-биотитовых и мраморных сланцевых отложениях луйхарской свиты. Халькопиритовая руда более бедная, с содержанием меди 1% или менее, а борнитовую относят к богатым рудам, в ее составе всегда не менее 1,5% меди. В границах месторождения из неметаллических минералов чаще всего встречаются полевой шпат, а также кварц и доломиты. Распространены парагенетически связанные с халькопиритом включения пирита и пирротина. В породах борнита может присутствовать молибденит.

Главный минерал Айнакского месторождения — борнит, присутствующий в доломитовых, реже в мраморных слоях. Борнитовая руда включает от двух с половиной до пяти процентов борнита, в виде слоистых и линзовых вкраплений. Форма его зерен, внедренных в агрегаты хлорит-плагиоклаз-доломита, обычного доломита либо кварца не является правильной, она обычно крючкообразная, с извилистыми очертаниями (рисунок 2а).

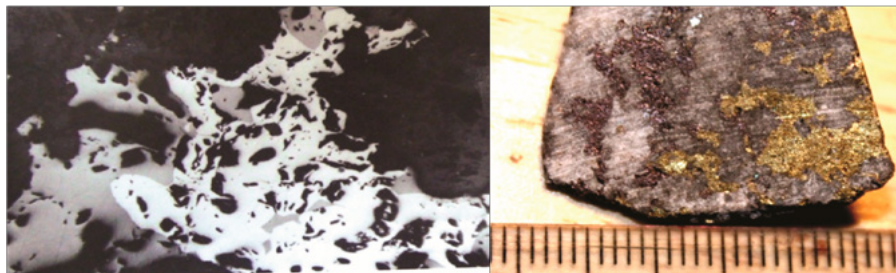
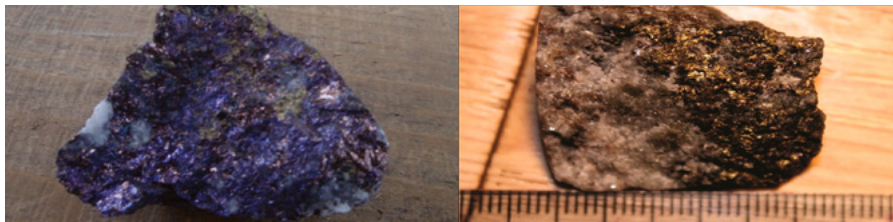


Рисунок 2. а) борнитовые и халькопиритовые прорастания (слева);
 б) борнитхалькопиритовый агрегат (справа).
 Борнит — серый, халькопирит — светлосерый, ув. 12.

Второй по распространенности минерал Айнакского месторождения — халькопирит, концентрация меди в нем сильно варьируется. В сланцевых песчаниках, доломитах и кварцитах он формирует либо линзовидные, либо равномерные включения и ветвящуюся сеть поперечных или слоистых жил в сланцах и других осадочных породах региона. Халькопирит выделяется оторочкой вокруг угловатых либо более округлых обломков, зачастую цементируясь с доломитом в гравиях либо песчаниках.



**Рисунок 3. а) кварц, содержащий азурит с халькопиритом;
б) кварц, содержащий халькопирит и борнит**

Минералы меди халькопирит, а также борнит имеют ведущее значение для формирования горных руд и пород. Их основу составляет минерал биотит, который также имеется и в мраморах (доломитовых). На Айнакском медном месторождении во множестве имеются минералы без включений металлов, например, мусковит, скаполит, гранит, тремолит, актинолит.

На участках трещиноватости встречается в основном халькозин, причем халькозинизацию борнита наблюдают вплоть до 460–560 метров вглубь от поверхности земли. Халькозин нередко срастается с борнитом, особенно ближе к срединной зоне борнитовых участков, замещая до 10–20 процентов его объема. Как правило, халькозин формирует прожилки либо оторочки в виде каймы в борните или халькопирите.

В малых количествах на участках халькопиритовых пород присутствует пирротин, развитый по преимуществу в слоях углистых сланцев и мраморов. Будучи парагенетически связанным с халькопиритом, минерал пирротин срастается с ним, формируя прямые либо извилистые границы.

Характерно, что в халькопиритовых породах всегда имеется пирит, хотя и в не очень больших количествах. При этом его количество заметно увеличивается в юго-восточной, юго-западной и северной зонах центрального участка Айнакского месторождения. Именно там вместо борнитовых руд преимущественно встречается халькопирит, а пирит, который там находят, сформирован в результате дисульфидизации пирротина в составе оторочек и прожилок халькопирита.

Минерал кобальтин на месторождении представлен рассеянными вкраплениями метакристаллов и очень мелких зерен неправильных очертаний размерами в сечении от 0,05 до 1,5 миллиметров, и крайне редко до

пяти миллиметров. Как правило, попадает в рудах халькопирита, в совсем малом объеме — в борнит-халькопиритовых. В рудах халькопирита присутствует и карролит, который выглядит как идиоморфные серо-белые включения с сиреневатым оттенком.

В южной стороне центральной зоны месторождения имеется шмальтин, связанный с кобальтином и халькопиритом в мелкие метакристаллы. В форме очень маленьких кристаллов (от 0,02 до 0,06 миллиметров) в халькопирите обнаруживают кобальтпентландит.

Герсдорфит обнаружен в аншлифах благодаря следующим признакам: светло-серый оттенок, идиоморфная форма включений, высокие отражательные свойства и изохронность. В краевых зонах зерен как борнита, так и халькопирита всегда имеется никель и кобальт, с одновременным присутствием там же кобальтина и зигенита.

В очень незначительном объеме в нижнем халькопиритовом участке встречается сфалерит в форме малых гнезд, узких прожилок и точечных вкраплений в халькопиритовой руде.

В рудах борнита центральной части месторождения распространен молибденит, особенно значительные его скопления обнаружены в зонах крупнозернистых руд, там молибденит представлен чешуйками по 1,5 миллиметра, срощенных с борнитом.

Наряду с вышеперечисленными минералами на месторождении встречается немало других пород, вот лишь некоторые из них:

1. Мусковит;
2. Хлорит;
3. Скаполит;
4. Углистые вещества;
5. Амфиболы;
6. Турмалин;
7. Кальцит.

Айнакское месторождение относят к промышленно-генетическому виду залежей медистых песчаников, оно отличается высоким качеством минералов, крупномасштабностью залежей их слоев и немалыми запасами основных медных руд.

На текстуру и состав руд Айнака и вмещающих их сульфидных и мраморных пород повлиял, преимущественно, свойственный региону метаморфизм в сторону нижних амфиболитовых фаций. В местных породах с тонкими зернами, представленных мраморами, сланцами, кварцитами, наблюдается характерная слоистость осадочных пород и наблюдаемых в них сульфидных вкраплений, которые содержат микроостатки диагенетических форм, с многочисленными вкраплениями пирита. В отдельных образцах можно увидеть, что первичный пирит затем частично замещался халькопиритом. Регион, где расположено Айнакское медное месторождение и горные группы его центральной части, почти горизонтален, если сравнивать с западной зоной района Айнак. В центральной зоне месторождения минералы залегают практически горизонтально и малоградиентно, тогда как в западной зоне залежи высокоградиентные, под углом от 9 до 59 градусов.

Список литературы

1. AGS и BGS, 2005a информационный пакет Айнак, часть I введение. Афганистан: Геологическая служба и Британская геологическая. — URL: [11www.bgs.ac.uk/AfghanMinerals/DMA_tender_docs.htm](http://www.bgs.ac.uk/AfghanMinerals/DMA_tender_docs.htm) / (электронные ресурсы) (дата обращения: 22.03.2023).
2. Предварительный отчет о результатах геологической разведки медного месторождения Айнак в 1974–1976 гг.: английская версия Геологической службы Афганистана и Британской геологической службы. — URL: www.bgs.ac.uk/AfghanMinerals/DMA_tender_docs.htm / (электронные ресурсы) (дата обращения: 22.03.2023).
3. MOMP and AGS, 2014 Copper of Afghanistan, in Ministry of Mines and Petroleum and Afghanistan Geological Survey, Minerals in Afghanistan. — URL: https://www.bgs.ac.uk/AfghanMinerals/DMA_tender_docs.htm / (электронные ресурсы) (дата обращения: 22.03.2023).
4. Mucnez, P., and Corbella, M., 2012. Factors controlling the precipitation of copper and cobalt minerals in sedimenthosted ore deposits: Advances and restrictions: Journal of Geochemical Exploration, v. 118, p. 38–46. (дата обращения: 22.03.2023).

5. Brown, A.C., 1971. Zoning in the White Pine copper deposit, Ontonagon County, MI, USA: Economic Geology, v. 66, no. 4, p. 543–573. (дата обращения: 22.03.2023).

УДК 551

Методика планирования газодинамических исследований скважин на газоконденсатных месторождениях

Курманчук Никита Сергеевич

аспирант Тюменского индустриального университета

***Аннотация:** Данная научная статья посвящена методике планирования газодинамических исследований скважин на газоконденсатных месторождениях. В статье рассмотрены основные этапы планирования и проведения газодинамических исследований, а также описаны методы оценки характеристик скважин и интерпретации полученных данных.*

***Abstract:** This scientific article is devoted to the methodology of planning gas-dynamic studies of wells in gas-condensate fields. The article discusses the main stages of planning and conducting gas dynamic studies, as well as describing methods for assessing the characteristics of wells and the interpretation of the data obtained.*

***Ключевые слова:** гидравлические исследования скважин, планирование исследований газоконденсатного месторождения.*

***Keywords:** hydraulic well research, planning of gas condensate field research.*

.....

Разработка газоконденсатных месторождений является одной из важнейших отраслей нефтегазовой промышленности. Одним из ключевых аспектов этой деятельности является планирование газодинамических исследований скважин. Однако, в силу сложности геологической структуры и многообразия факторов, влияющих на процессы добычи газа и конденсата, этот процесс требует тщательной методики планирования.

Основные проблемы планирования газодинамических исследований

Планирование газодинамических исследований скважин на газоконденсатных месторождениях требует учета множества факторов. Основными из них являются:

1. Сложность геологической структуры. Газоконденсатные месторождения могут иметь сложную геологическую структуру, что затрудняет определение характеристик скважин и оценку потенциала месторождения.
2. Многообразие факторов, влияющих на процессы добычи газа и конденсата. К таким факторам относятся: температура, давление, состав пластовых флюидов, технические параметры скважин и т.д.
3. Необходимость максимального использования информации, полученной при проведении предыдущих исследований. Использование данных, полученных на предыдущих стадиях разработки месторождения, позволяет сократить время и затраты на проведение газодинамических исследований.

Методика планирования газодинамических исследований

Для планирования газодинамических исследований скважин на газоконденсатных месторождениях можно использовать следующую методику:

- Анализ данных, полученных на предыдущих этапах разработки месторождения. Для этого необходимо проанализировать данные геологических исследований, результаты геофизических исследований, параметры скважин и другие данные, полученные на предыдущих этапах разработки месторождения.
- Оценка дебита скважин. Для оценки дебита скважин можно использовать различные методы, такие как тестирование скважин, анализ исторических данных и математические модели.
- Оценка давления в пласте. Для оценки давления в пласте можно использовать данные, полученные при бурении скважин, геофизические данные, данные о флюидодинамических свойствах пласта и другие параметры.

- Оценка состава пластовых флюидов. Для оценки состава пластовых флюидов можно использовать результаты лабораторных анализов, данных о составе пластовых флюидов на смежных месторождениях и другие данные.

Разработка плана газодинамических исследований. На основе данных, полученных на предыдущих этапах, можно разработать план газодинамических исследований. В этот план могут входить следующие мероприятия:

1. Тестирование скважин. Тестирование скважин позволяет оценить их производительность и другие характеристики, такие как давление и состав флюидов.
2. Измерение параметров скважин. Для измерения параметров скважин можно использовать различные методы, такие как датчики давления, температуры и другие датчики.
3. Моделирование процессов добычи газа и конденсата. Математические модели позволяют оценить процессы добычи газа и конденсата на месторождении и разработать оптимальную стратегию добычи.
4. Анализ результатов и корректировка плана исследований. Анализ результатов газодинамических исследований позволяет корректировать план исследований и принимать более точные решения относительно добычи газа и конденсата.

Заключение

Планирование газодинамических исследований является важной составляющей разработки газоконденсатных месторождений. Для успешной разработки месторождения необходимо учитывать множество факторов, таких как сложность геологической структуры, многообразие факторов, влияющих на процессы добычи, и многие другие. Эффективное использование газодинамических исследований позволяет повысить эффективность добычи, сократить затраты на разработку месторождений и улучшить экономические показатели проекта.

Однако следует отметить, что планирование газодинамических исследований является сложным и многогранным процессом, требующим большого количества знаний и опыта. Поэтому для разработки опти-

мального плана газодинамических исследований необходимо привлекать высококвалифицированных специалистов в области газодинамики, геологии и нефтегазовой промышленности.

Таким образом, газодинамические исследования являются ключевым элементом в разработке газоконденсатных месторождений, позволяющим определить оптимальную стратегию добычи и повысить эффективность проекта.

Список литературы

1. Дополнение к Единой технологической схеме разработки залежей углеводородного сырья Ачимовских отложений Уренгойского месторождения по лицензионному участку ООО «Газпром добыча Уренгой». Тюмень: ТюменНИИгипрогаз, 2015.
2. Газпром 086–2010 «Инструкция по комплексным исследованиям газовых и газоконденсатных скважин». М.: Газпром экспо, 2011.
3. Алиев З.С., Бердин Т.Г., Ли Г. С. Опыт исследования скважин нижнемеловых залежей Уренгойского месторождения. Обзорная информация: Разработка и эксплуатация газовых и газоконденсатных месторождений. М.: ИРЦ Газпром, 2002. 43 с.
4. Сафронов М.Ю., Ли Г.С., Стасенков И. В. Опыт строительства скважин в сложных горно-геологических условиях II участка Ачимовских отложений Уренгойского НГКМ. Материалы научно-практических конференций молодых ученых и специалистов ОАО «Газпром» — призеров 2011 года. М.: ООО «Газпром экспо», 2012. С. 5–10.

Журнал «Научный аспект №4 2023»

Эл. почта редакции: public@na-journal.ru

Подробнее на сайте: <https://na-journal.ru>