REDS:

Телекоммуникационные устройства и системы

№4

2025

СОДЕРЖАНИЕ

АНАЛИЗ ЭФФЕКТИВНОСТИ ОПРЕДЕЛЕНИЯ ОТЛИЧИТЕЛЬНЫХ ОСОБЕННОСТЕЙ ПРИЗНАКОВ СЕТЕВЫХ АТАК

Архипов Никита Дмитриевич
магистр МТУСИ, группа М092402(75), Москва, Россия,
nikitaarkhipov2002@mail.ru

Савин Всеволод Артёмович
МТУСИ, аспирант группы АЭФ2401(15), Москва, Россия
savin.vsevolod@icloud.com

Тришина Светлана Викторовна
МТУСИ, ассистент кафедры СИТиС, Москва, Россия
trishina@rambler.ru

Гадасин Денис Вадимович
МТУСИ, доцент кафедры СИТиС, к.т.н., доцент, Москва, Россия
d.v.gadasin@mtuci.ru

Аннотация
Статья посвящена исследованию методов определения отличительных особенностей с использованием статистического анализа признаков для обнаружения аномалий в паттернах трафика. В статье приведен существующий подход к анализу и выявлению аномалий трафика, дан анализ актуальности темы использования статистического анализа на основании методов корреляции в трафике и исследуется, возможность использования этих методов для эффективного детектирования существующих и новых аномалий.

Ключевые слова
Обнаружение вторжений, область исследования, обнаружение аномалий, методы отбора признаков, статистические методы, метод корреляционного анализа, машинное обучение

Введение

Многие компании сейчас используют компьютерную сеть, и вынуждены для её управления нанимать персонал, следящий круглосуточно за её состоянием, проводя обслуживание и всегда должны быть готовы устранить возникшие проблемы. Обнаружение аномалий является одной из основных причин многих проблем, таких как отказы информационной системы, возможные потери данных или поломки системы, так и оборудования. Мониторинг за состоянием [1, 2], необходимая и важная часть любой компьютерной системы, требующая использования различных методов наблюдения и отслеживания событий. Однако, хоть и обнаружение аномалий не является чем-то из ряда вон выходящего, но чем быстрее её обнаружить, тем выше вероятность сохранить работоспособность и данные сети в безопасности [3]. В пример можно привести возникновение аномалии, с целью сокрытия целенаправленных действий, посылая ложные пакеты имеющие выраженные нехарактерные признаки, тем самым создавая искусственный шум в сети, давая в нужный момент возможность замаскировать реальные действия [4, 5]. Использование атаки “Дымовая завеса”, позволяет выиграть время для основного действия злоумышленников, пока сетевые специалисты отвлеченны от главной цели атаки. Использование модели машинного обучения позволяет уведомлять или блокировать аномальный трафик. Но получить достаточно времени, даже используя машинное обучение не всегда возможно. Не все модели машинного обучения предназначены для работы с данными сети и обработкой характеристик пакетов, особенно в режиме реального времени. Поэтому существуют разные подходы к выбору моделей и способов их обучения [6, 7].

Для обнаружения сетевых аномалий используют один из четырёх подходов к обучению модели:

- Неконтролируемое обучение
- Контролируемое обучение
- Полуконтролируемое обучение
- Ансамблевые обучение (методы)

Наиболее часто используемым подходом является неконтролируемое обучение, используя закономерности, модель обучается на основе немаркированных данных и выявляет аномалии на основе их

отклонения от изученной модели. Использование подхода выгодно при неопределённом нормальном поведением и несбалансированным наборе данных.

Результаты исследования

Исходя из работы [8], анализирующая разные подходы к обучению модели, существенным ограничением неконтролируемого обучения модели, является скорость обнаружения при работе с новыми данными, зависящая от мер близости и напрямую влияющая на частоту ложных тревог. Длительное время обработки пакетов является нерешённой на текущий момент времени для данного подхода к обучению.

В противоположность метода неконтролируемого обучения, используется метод контролируемого обучения. Используя маркированные данные с нормальными и аномальными примерами пакетов сетевых данных метод, обучается их разделению. Модель, обученная таким способом, позволяет выявлять и различать нормальные и аномальные шаблоны на основе маркированной информации [9]. Использование подхода выгодно в случае, четкого определения аномальных случаев и доступна репрезентативность выборки для обучения.

Учитывая работу [8], для обучения выгодно использовать контролируемое обучение, выполняющее требование минимального времени задержки, имея ввиду допустимую задержку при обработке в несколько пакетов и высокой точности обнаружения.

Основываясь на этих подходах, используют полуконтролируемые и ансамблевые подходы, сочетающие в себе сильные стороны как неконтролируемых, так и контролируемых методов. Полуконтролируемые подходы обучаются на маркированных примеров вместе с немаркированными данными для построения модели [10], эффективно обнаруживающая аномалии. Ансамблевые подходы, объединяя несколько моделей, позволяют достичь результатов точности обнаружения аномалий выше, чем по отдельности каждая из моделей [11, 12].

Целью обучения в задаче классификации пакетов, является максимально точное разделение пакетов на две группы, на обычные и аномальные. Но как определить отличительные способности.

Любой трафик изначально единый, однообразный. Но при изучении его свойств, пакеты с деструктивной способностью имеют отличительные черты. И главная задача определить эти пакеты для того, чтобы принять соответствующие контрмеры [13, 14]. Для этого необходимо изучить различные подходы к извлечению признаков. Одним из подходов к извлечению признаков является подход, базирующийся на статистическом анализе данных, находящихся в пакетах. Данный подход анализа данных включает этап исследования зависимостей, включающий, такие статистические методы исследования, как корреляционный, дисперсионный и регрессионный анализ [15].

Использование подхода статистического анализа хорошо показано на примере метода социологического исследования “Экзитпол”.

Exit poll (англ. выходной опрос) – метод, впервые использовавшийся в ходе выборов губернатора штата Кентукки, США в 1967 году [16]. Проверяя честность выборного процесса, исходя из логики с учётом полной анонимности, что избирателям нет смысла врать, был проведён опрос выходящих с избирательного участка граждан. Полученные данные коррелировались с настоящими итогами выборов, выполняя функцию экзитпола, и в дополнении давая досрочное информирование об итогах голосования.

Данный метод показывает, как с точки зрения статистики, используя меньший размер выборки, т.е. количество опрашиваемых граждан, получить достоверные итоги. Результаты опроса могут быть перенесены только с учетом определенной статистической ошибки, зависящей от объема выборки. Важно распределить людей по социально-демографическим признакам, позволяя создать модель исследуемого населения избирательного возраста электората. Основная задача экзитпола – предварительные итоги, структурированные, как можно быстрее. Данная задача стоит и в обучении модели, получить результат, не используя полную выборку данных, получив предварительные итоги с минимальной ошибкой.

Использование статистических методов в машинном обучении, позволяет выполнить отбор признаков, вносящие наибольший вклад в работу модели [17, 18]. Целью отбора признаков является исключение тех признаков, взаимосвязь с целевой переменной, либо отсутствует, либо недостаточна.

В данной работе [19] предлагается статистический метод выбора признаков на основе матрицы корреляции, рассчитанной между признаками для определения полезных, ненужных и шумных признаков. Использовался набор данных UNSW-NB 15 с обучением классификатора дерева решений на основе Adaboost. Матрица корреляции, показанная на рисунке 1, составлялась перед этапом обучения, и

содержит все признаки набора данных, требующих оценки важности. Данный набор данных выбран за свою сложность при обучении моделей и учитывая его эталонность для систем NIDS. Набор данных содержит признаки и метки классов сетевых пакетов, включая девять типов атак, а именно Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode и Worms.

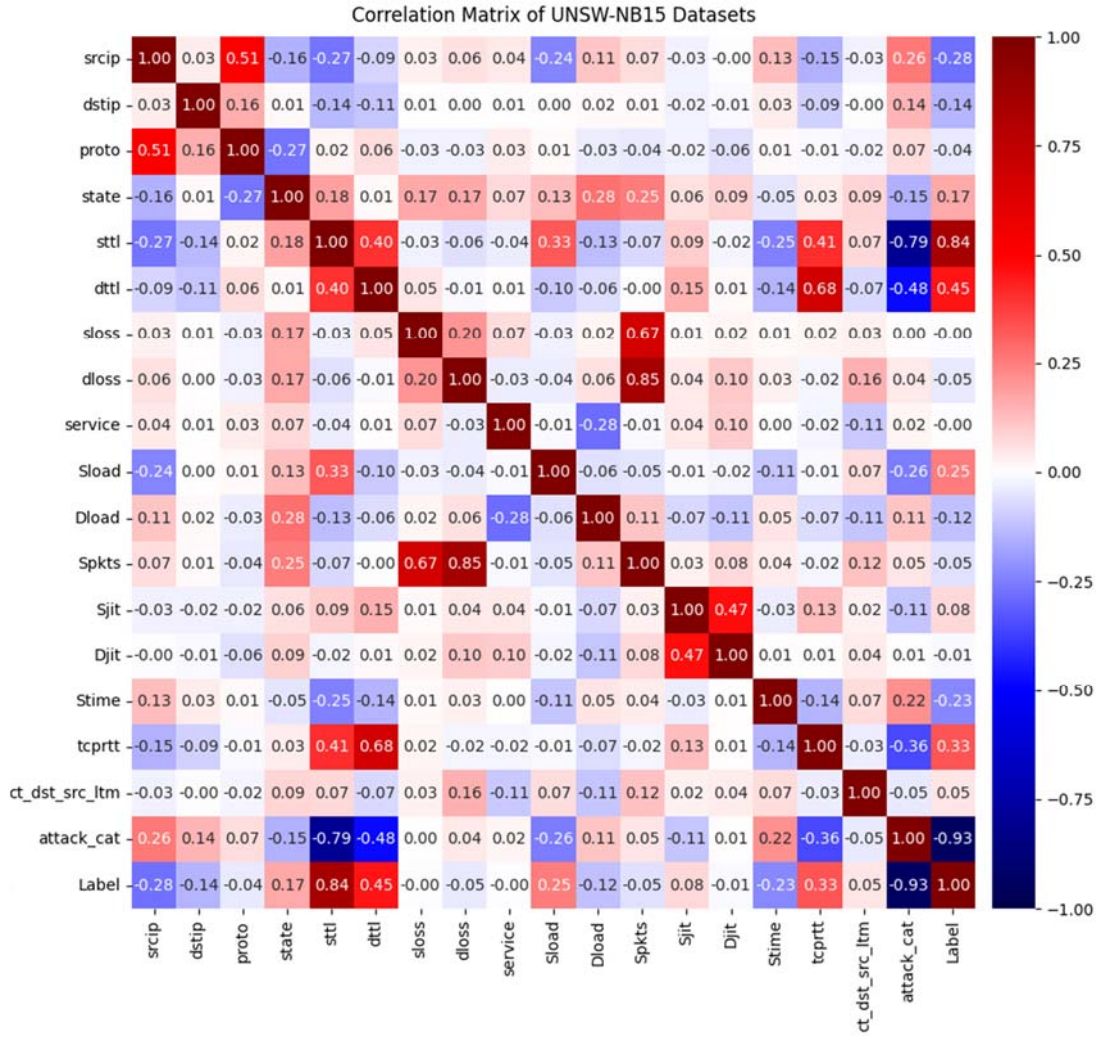

Рис. 1. Матрица корреляции признаков

Остановимся подробно на том, как матрица корреляции строится.

На рисунке №1 изображена матрица, преобразованная для удобства и наглядности в карту температурных значений, где градиентная шкала значений изображена справа. В матрице представлены значения расчёта линейной корреляции между признаками, используя коэффициент корреляции Пирсона, означающий степень взаимосвязанности переменных друг с другом и вычисляющийся по формуле 1.

Формула расчета коэффициента корреляции Пирсона:

$$r_{xy} = \frac{\sum\left(x_i - \bar{x}\right)\cdot\left(y_i - \bar{y}\right)}{\sqrt{\sum\left(x_i - \bar{x}\right)^2 \cdot \sum\left(y_i - \bar{y}\right)^2}}, \quad (1)$$

где x_i, y_i – элементы выборки; $\bar{x} = 1$ – среднее значение параметра x; $\bar{y} = 1$ – среднее значение параметра y.

Коэффициент корреляции Пирсона, статистическая мера определения силы связи между двумя признаками с использованием их относительных моментов. Диапазон значений коэффициентов корреляции Пирсона лежит в интервале от -1 до +1. Вычисление коэффициента на наборе данных происходит перебором каждого признака со всем набором признаков.

После составления матрицы корреляции, рассмотрим два этапа анализа и отбора признаков:

1. Нужно проанализировать корреляции всех признаков с целевым признаком, и оставить только сильно коррелирующие признаки.

2. Нужно проанализировать корреляции всех оставшихся признаков, и убрать все признаки, сильно коррелирующие между собой.

Коэффициенты, равные +1 и -1 в выборочной корреляции, соответствуют точкам двумерных данных, лежащих точно на прямой линии. Признак коэффициента корреляции со значением +1 показывает сильную положительную корреляцию, тогда как −1 представляет сильную отрицательную связь между признаками.

1. Проанализируем корреляции всех признаков с целевым признаком

В данном случае для выбора признака, он должен иметь сильную положительную корреляцию или сильную отрицательную корреляцию с целевым признаком. Сильная связь с целевым признаком означает его важность и полезность в обнаружении аномалий, поэтому такие признаки нужно оставить для обучения модели. Целевой признак, нужен при обучении модели с использованием контролируемого обучения, с учётом того, что данные датасета обучения содержат признак уже распознанных аномалий. В наборе данных UNSW-NB 15 целевой признак – “Label”, содержащий булево значение “0” – означая нормальный пакет и “1” - означая аномальный пакет.

2. Проанализируем корреляции всех оставшихся признаков между собой

В данном случае для выбора признака, он должен не иметь корреляции или иметь слабую корреляцию с другим признаком. Данный анализ не даёт прямого увеличения точности модели, но он позволяет её упростить, за счёт уменьшения количества признаков, предотвращая быстрое переобучение и позволяя использовать больше циклов при обучении, не доводя до переобучения, давая возможность увеличить точность.

Таблица 1

Признаки и причины для удаления

Имя признака	**Описание**	**Причина удаления**
srcip	IP адрес источника	Признак имеет сильную положительную корреляцию с признаком: proto – Протокол транзакции = 0.509643 Признак имеет достаточную корреляцию с целевым признаком -0.278830, но его требуется убрать, т.к. в реальности он не позволяет обнаружить аномалии. Анализируя его сильную корреляцию с признаком proto 0,5, имеющий корреляцию с целевым признаком -0.043, можно сделать вывод, данный признак является шумовым. Из-за особенностей датасета признак имеет достаточную корреляцию, и в данном случае не нужно учитывать его во внимание.
sport	Порт источника	Признак имеет слабую корреляцию с целевым признаком -0.060932
dstip	IP адрес назначения	Признак имеет слабую корреляцию с целевым признаком -0.142560 Его требуется убрать, т.к. он не позволяет обнаружить аномалии из-за особенностей датасета. Признак, так же имеет корреляцию с шумовым признаком proto 0.16, притом больше, чем с целевым признаком 0.14.
dsport	Номер порта назначения	Признак имеет слабую с целевым признаком = 0.049502
proto	Протокол передачи данных	Признак имеет сильную положительную корреляцию с признаком: srcip = 0.509643 И слабую с целевым признаком = -0.043151
state	Состояние пакета, относящиеся к протоколу (например, ACC, CLO, CON, ECO и др.)	Признак имеет сильную корреляцию с признаками: proto – Протокол транзакции = -0.271855 Dload = 0.279864 Spkts = 0.252161 И недостаточную корреляцию с целевым признаком = 0.169682
sloss	Количество пакетов, переданных повторно или потерянных источником	Признак имеет слабую корреляцию с целевым признаком = -0.002303

dloss	Количество пакетов, переданных повторно или потерянных на стороне назначения	Признак имеет сильную положительную корреляцию с признаками: Spkts = 0.848731 Dpkts = 0.992938 И слабую с целевым признаком = -0.046677
service	Тип сервиса (например, http, ftp, smtp, ssh, dns, ftp-data, irc или "-" при малом использовании сервиса)	Признак имеет сильную отрицательную корреляцию с признаком: Dload = -0.284793 И слабую с целевым признаком = -0.004414
Spkts	Количество переданных пакетов от источника к назначению	dloss = 0.848731 Dpkts = 0.892398 И слабую с целевым признаком = -0.054768
Dpkts	Количество переданных пакетов от назначения к источнику	dloss = 0.992938 Spkts = 0.892398 И слабую с целевым признаком = -0.055334
Sjit	Джиттер источника (в мс)	Djit = 0.473038 И слабую с целевым признаком = 0.075497
Djit	Джиттер назначения (в мс)	Sjit = 0.473038 И слабую с целевым признаком = -0.011419
ct_dst_src_ltm	Количество соединений с одним и тем же адресом источника и назначения за последние 100 соединений	Признак имеет слабую корреляцию с целевым признаком = 0.053946
attack_cat	Категории атаки Fuzzers, Analysis, Backdoors и другие	Признак используется при многозадачном обучении, имеющим свои проблемы и сложности. В работе использовался один целевой признак “Label”

Исходя из этих этапов, в случае отсутствия корреляции между признаками и сильной связи признаков с целевой переменной, будет получен набор данных, содержащий самые эффективные признаки [20] с точки зрения статистической линейной зависимости.

Рассмотрев все признаки, нужно найти и выбрать, используя матрицу корреляции, нужные для удаления, где либо нет корреляции с целевым признаком “Label”, либо они имеют сильную корреляцию друг с другом. После анализа корреляционной матрицы нужно удалить признаки, указанные в таблице 1. Значения корреляции в таблице №1 были взяты из той же матрицы корреляции, не преобразованной в карту температурных значений.

В таблице 1 на первом этапе при анализе взаимосвязей с целевой переменной, были убраны такие переменные, как sport, dsport, proto, sloss, dloss, service, Spkts, Dpkts, Sjit, Djit, ct_dst_src_ltm.

На рисунке 2, показана выборка признаков неудовлетворяющих на первом этапе отбора, в виде массива корреляции исключенных признаков с целевым признаком “Label”, для наглядной проверки.

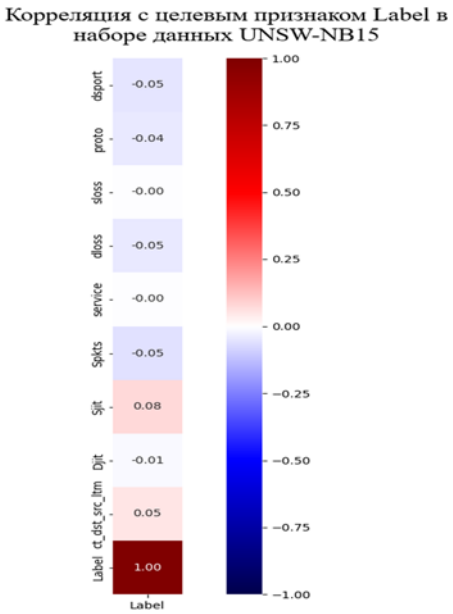

Рис. 2. Массив корреляции признаков с целевым признаком на первом этапе отбора

На втором этапе анализа корреляции всех оставшихся признаков, сильно коррелирующие между собой, были убраны такие переменные, как srcip, state.

На рисунке 3, показана выборка признаков неудовлетворяющих на втором этапе отбора, в виде матрицы корреляции исключенных признаков с зависящими от них шумными признаками и целевым признаком “Label”, для наглядной проверки.

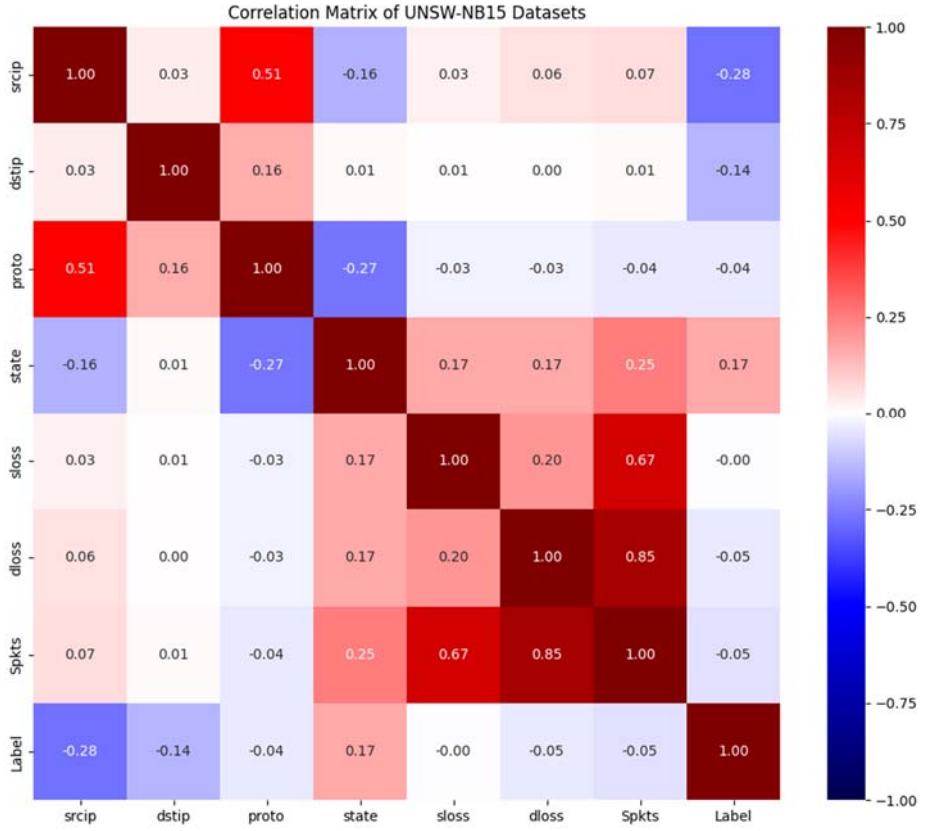

Рис. 3. Матрица корреляции исключённых признаков на втором этапе отборе

Признак srcip был удалён, из-за корреляции со шумовым признаком proto 0.51, и слабой корреляцией с целевым признаком -0.28.

Признак state был удалён, из-за корреляции с шумовыми признаками srcip -0.16, proto -0.27, sloss 0.17, dloss 0.17, Spkts 0.25 из-за корреляции большей, чем с целевым признаком 0.17.

Признаки, сильно коррелирующие друг с другом, и были удалены, поскольку они не добавляли существенной разницы и только увеличивали сложность модели. Матрица корреляции после отбора признаков, которая использовалась для обучения модели показана на рисунке 4.

Для примера, оценим оставшиеся признаки. Из самых наглядных и высоко коррелированных с целевым признаком, являются sttl - Время жизни пакета от источника к месту назначения и dttl - Время жизни пакета от места назначения к источнику. Признаки отвечают за время жизни пакета. По мере того, как сетевой пакет перемещается от источника, с указанием требуемого количесва sttl, т.е максимального количества прохождений маршрутизаторов до места назначения, где каждый маршрутизатор на пути уменьшает dttl на 1, по началу равный sttl, прежде чем переслать его на следующий участок. Как только dttl достигает 0, маршрутизатор отбрасывает пакет, отправляя обратно источнику сообщение ICMP о том, что время пакета превышено.

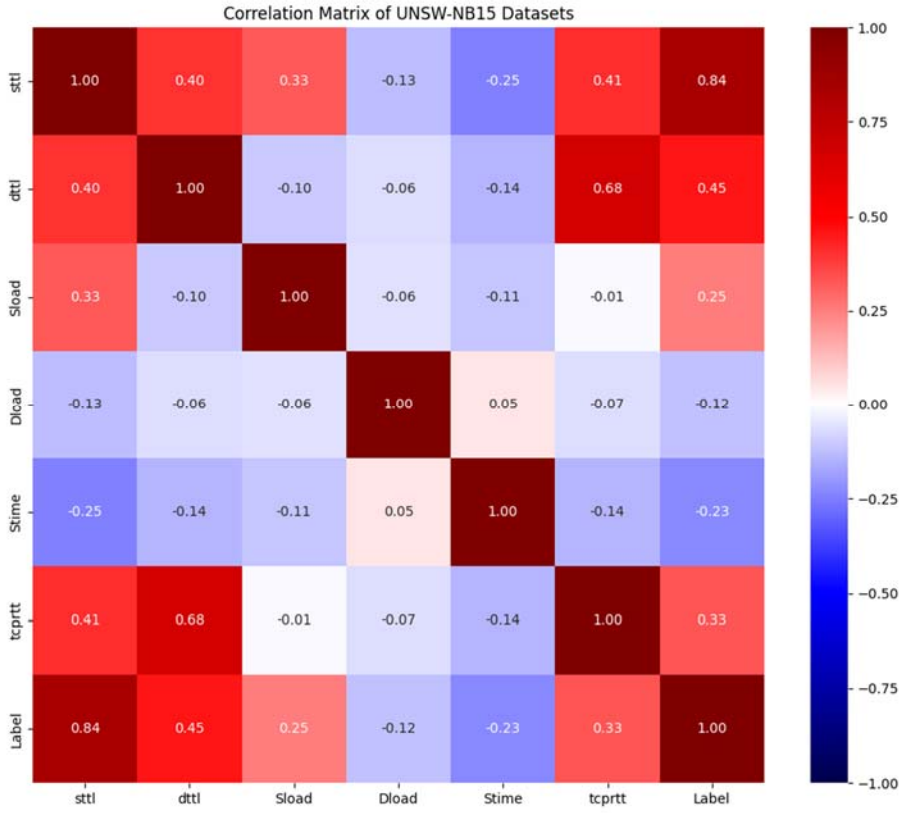

Рис. 4. Матрица корреляции после отбора признаков

Для соединения через глобальную сеть, по стандарту RFC 791 [21], должен быть указан параметр TTL, составляющий обычно от 64 до 128:

- Для систем Linux, MAC OSX, **Unix**-подобных и Android – 64
- Для системы Windows и некоторых маршрутизаторов Cisco – 128
- Максимальное возможное значение – 255

Аномальные пакеты специально конструируют и посылают с максимальным значением признака sttl и dttl, позволяя пробраться во внутреннюю сеть и максимально долго удерживать сессию, давая возможность исследовать всю подсеть компьютерной сети, пока значение признака dttl не достигнет 0.

Эти два признака хорошо коррелируют с целевой переменной “Label”, и слабо коррелируют между собой, представляя наиболее удачные критерии обнаружения аномалии, в данном случае атаку “Exploits” из набора данных, где значение dttl становится больше sttl, что противоречит логике прохождения пакетов через маршрутизаторы или неправильно сконфигурированную компьютерную сеть из-за атаки, ошибки маршрутизации и т.д.

Таблица 2

Результат точности модели после обучения при тестировании

Technique	Dataset	Accuracy
Adaboost-based decision tree classifier	UNSW-NB15	99.3%

Предложенный метод обнаружения сетевых вторжений имеет высокую точность с набором данных UNSW-NB15, поскольку модель была обучена и протестирована на лучших дискриминирующих признаках.

Заключение

Использование таких средств мониторинга состояния системы, как модель машинного обучения позволяет вовремя уведомлять или заблокировать аномальный трафик. Но получить достаточный результат, даже используя машинное обучение не всегда возможно. Не все модели машинного обучения предназначены для обработки большого количества характеристик пакетов сети, особенно в режиме реального времени [22-28]. Для чего и существуют разные подходы к выбору моделей и способов к её упрощению. Был проведен анализ возможности использования этих методов для эффективного детектирования существующих и новых аномалий.

Использование статистического метода, такого как коэффициент корреляции Пирсона при обучении классификатора на основе дерева решений Adaboost позволила получить хорошие результаты точности, а именно 99.3%.

Литература

1. *Гадасин Д.В., Каледина А.В*. Использование современных средств мониторинга для анализа состояния IT-систем // Технологии информационного общества : Сборник трудов XIV Международной отраслевой научно-технической конференции, Москва, 18-19 марта 2020 г. М.: Издательский дом Медиа Паблишер, 2020. С. 267-269. EDN XAPWGD

2. Свидетельство о государственной регистрации программы для ЭВМ № 2023615007 Российская Федерация. Программное приложение «Анализатор актуальности угрозы» ("Threat Relevance Analyzer" – на английском языке) для определения актуальности угроз персональных данных при их обработке в информационных системах персональных данных : № 2023613955 : заявл. 27.02.2023 : опубл. 09.03.2023 / В. А. Докучаев, В. В. Маклачкова, Д. В. Гадасин [и др.] ; заявитель Общество с ограниченной ответственностью Фирма «ТЕЛЕСОФТ». EDN AOOMDG

3. *Гадасин Д.В., Каледина А.В*. Влияние аномальных событий на отдельные показатели QoS сети связи // Технологии информационного общества : Материалы XIII Международной отраслевой научно-технической конференции, Москва, 20-21 марта 2019 г. Том 2. М.: Издательский дом Медиа Паблишер", 2019. С. 19-21. EDN HBJVXH

4. *Gadasin D.V., Shvedov A.V., Vakurin I.S*. Determination of Semantic Proximity of Natural Language Terms for Subsequent Neural Network Training // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 – Conference Proceedings, Moscow, 15-17 марта 2022 г. Moscow, 2022. DOI 10.1109/IEEECONF53456.2022.9744290. EDN LASMDY

5. *Шведов А.В., Гадасин Д.В., Коровушкина В.М., Мелькова Е.К*. Интеллектуальное тестирование как способ повышения качества информационной системы // REDS: Телекоммуникационные устройства и системы. 2022. Т. 12, № 2. С. 43-52. EDN GOLZGE.]

6. *Гадасин Д.В., Шведов А.В., Пантелеева К.А*. Предобработка информации для систем машинного обучения // Актуальные проблемы и перспективы развития экономики : Труды XXI Международной научно-практической конференции, Симферополь-Гурзуф, 20-22 октября 2022 г. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. С. 268-269. EDN QVIOMF.

7. *Шульпина П.Д., Гадасин Д.В., Тремасова Л.А*. Взвешивание признаков как Предварительная обработка исходных наборов данных // Системы синхронизации, формирования и обработки сигналов. 2024. Т. 15, № 3. С. 40-47. EDN BIOWRB

8. *Swarnkar M., Hubballi N*. OCPAD: One class Naive Bayes classifier for payload-based anomaly detection / Expert Systems with Applications. 2016. 64, pp. 330-339. https://doi.org/10.1016/j.eswa.2016.07.036 (accessed on 16.12.2024)

9. Bhattacharyya DK, Kalita JK. Network anomaly detection: A machine learning perspective / CRC Press. 2013. URL: https://doi.org/10.1201/b15088 (accessed on 24.12.2024).

10. *Полякова А.Н., Кольцова А.В., Гадасин Д.В*. Место искусственного интеллекта в сетях хранения данных // Искусственный интеллект и цифровая экономика: взгляд студенчества : материалы I Всероссийской студенческой научно-практической конференции, Москва, 13 ноября 2019 г. / Министерство науки и высшего образования Российской Федерации, Государственный университет управления. М.: Государственный университет управления, 2020. С. 126-127. EDN PNJJGH

11. *Гадасин Д.В., Кривов Д.А*. Мониторинг трафика в сетях SDN // Телекоммуникационные и вычислительные системы – 2017 : Труды международной научно-технической конференции, Москва, 22 ноября 2017 г. М.: Горячая линия – Телеком", 2017. С. 88-89. EDN ZVITBZ

12. *Гадасин Д.В., Юдина А.А*. Сложные сети как симбиоз современных сетевых технологий и искусственного интеллекта // Технологии информационного общества : Сборник трудов XIV Международной отраслевой научно-технической конференции, Москва, 18-19 марта 2020 г. М.: Издательский дом Медиа Паблишер, 2020. С. 270-272. EDN FHRMNZ

13. *Zolotukhin P.A., Melkova E.K., Gadasin D.V., Korovushkina V.M*. Using Intelligent Testing as a Tool to Improve the Quality of Transport Information Systems // 2022 Systems of Signals Generating and Processing in the Field of on

Board Communications, SOSG 2022 – Conference Proceedings, Moscow, 15-17 марта 2022 г. Moscow, 2022. DOI 10.1109/IEEECONF53456.2022.9744348. EDN NOMJLX

14. Свидетельство о государственной регистрации программы для ЭВМ № 2018660142 Российская Федерация. Программное приложение "Сигнал-Ф1" для визуализации обнаружения компьютерных атак в СОА "Форпост" : № 2018617954 : заявл. 26.07.2018 : опубл. 16.08.2018 / В. А. Докучаев, В. В. Маклачкова, Д. В. Гадасин, А. В. Шведов ; заявитель Общество с ограниченной ответственностью Фирма «ТЕЛЕСОФТ» (ООО Фирма «ТЕЛЕСОФТ»). EDN TMNION.

15. *Ahmad I., Ul Haq Q.E., Imran M., Alassafi M.O., AlGhamdi R.A.* An Efficient Network Intrusion Detection and Classification System / Journal of Mathematics. 2022. 10(3). p. 530. https://doi.org/10.3390/math10030530 (accessed on 16.12.2024).

16. *Гадасин Д.В., Шведов А.В., Алексеева Е.А*. Информационная энтропия в стохастических сетях связи // Телекоммуникационные и вычислительные системы 2020 : Труды международной научно-технической конференции, Москва, 14-17 декабря 2020 г / Московский технический университет связи и информатики. М.: Горячая линия – Телеком", 2020. С. 108-116. EDN IOGLQH.

17. *Paskevich A.* What is the exit poll: how it works and whether it can be trusted. URL: https://news.obozrevatel.com/politics/chto-takoe-ekzitpol-kak-rabotaet-i-mozhno-li-doveryat.htm

18. *Гадасин Д.В*. Разработка методов и средств анализа однородных стохастических мегасетей и исследование их вероятностных характеристик : специальность 05.13.13 : автореферат диссертации на соискание ученой степени кандидата технических наук / Гадасин Денис Вадимович. Москва, 1998. 23 с. EDN ZKOAXH

19. *Докучаев В.А., Лопатина Е.В., Павлов С.В., Гадасин Д.В.* Качество передачи информации в корпоративных IP-сетях (часть 1). М.: Московский технический университет связи и информатики, Инсвязьиздат, 2010. 36 с. EDN ZGJSJH

20. *Шведов А.В., Яковенко Н.В., Коровушкина В.М., Гадасин Д.В.* Взаимосвязь параметров оценки надежности программного обеспечения // REDS: Телекоммуникационные устройства и системы. 2023. Т. 13, № 4. С. 20-29. EDN ASISTF

21. RFC 791 – Internet Protocol Specification. https://datatracker.ietf.org/doc/html/rfc791 (accessed on 12.01.2025).

22. *Гадасин Д.В., Шведов А.В., Кузин И.А.* Трехмерная реконструкции объекта по одному изображению с использованием глубоких свёрточных нейронных сетей // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16, № 7. С. 29-35. DOI: 10.36724/2072-8735-2022-16-7-29-35 EDN: YTLCNW

23. *Kalmykov N.S., Dokuchaev V.A.* Segment routing as a basis for software defined network // T-Comm. 2021. Т. 15. № 7. С. 50-54. EDN: LYVZCV

24. *Dokuchaev V.A., Maklachkova V.V., Statev V.Yu.* Classification of personal data security threats in information systems // T-Comm. 2020. Т. 14. № 1. С. 56-60. EDN: QOGYHH

25. *Докучаев В.А., Маклачкова В.В., Статьев В.Ю.* Цифровизация субъекта персональных данных // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 6. С. 27-32. EDN: XVWYJP

26. *Pavlov S.V., Dokuchaev V.A., Mytenkov S.S.* Model of a fuzzy dynamic decision support system // T-Comm. 2020. Т. 14. № 9. С. 43-47. EDN: VYFNLB

27. *Кузин И.А., Гадасин Д.В.* Модель контейнера данных для минимизации трафика при передаче субъективных характеристик объектов на изображении трехмерной сцены // Телекоммуникации и информационные технологии. 2021. Т. 8. № 2. С. 96-100. EDN: TYFFBH

28. *Назаров М.Д., Шведов А.В.* Корреляция атрибутов соглашения об уровне обслуживания с основными параметрами QoS в корпоративных сетях // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 73-79. EDN: VQHDTJ

ДИСТАНЦИОННОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ИСТОРИЯ, ТЕХНОЛОГИИ, СРАВНЕНИЕ

Белостоцкая Вероника Тарасовна
МТУСИ, студент, Москва, Россия
almas@dzhenia.ru

Панков Константин Николаевич
МТУСИ, доцент кафедры «Информационная безопасность», к.ф.-м.н., доцент, Москва, Россия
pankov_kn@mtuci.ru

Аннотация
Данная работа посвящена изучению дистанционного электронного голосования в Российской Федерации и мировой практике. Рассматриваются история внедрения, технические особенности и криптографические методы защиты данных. Также проведено сравнение систем ДЭГ России и Эстонии на основе их технической базы, прозрачности и восприятии обществом.

Ключевые слова
Дистанционное электронное голосование, ДЭГ, информационная безопасность, криптография, гомоморфное шифрование, блокчейн, электронная подпись, аутентификация, мировой опыт, история внедрения

Введение

Дистанционное электронное голосование (далее – ДЭГ) – это инновационная технология, которая позволяет гражданам принимать участие в голосовании без личного присутствия на избирательном участке. В наши дни, когда большинство сфер жизни охватила цифровизация, внедрение ДЭГ стало довольно логичным шагом со стороны государства.

Основной целью ДЭГ является повышение количества явок избирателей. Технология значительно упрощает процедуру голосования для людей с ограниченными возможностями, граждан, которые по каким-то причинам проживают за пределами своих избирательных участков, и людей, которые в силу обстоятельств не могут очно проголосовать. Однако несмотря на множество преимуществ, ДЭГ вызывает много дискуссий. Одна из них – это обеспечение гарантии открытости и справедливости процесса голосования, сохранение конфиденциальности данных избирателей, а также предотвращение киберугроз и случаев мошенничества [1], иначе говоря, повышение уровня информационной безопасности.

В Российской Федерации дистанционное электронное голосование начало развиваться в начале 2000-х годов, однако наибольшую популярность обрело в период пандемии COVID-19, т.к. обеспечивало минимальную контактность граждан. Первая масштабная попытка внедрения ДЭГ была предпринята в Москве, а затем технология распространилась на остальные регионы страны.

На сегодняшний день Россия активно применяет электронное голосование как на региональном, так и на федеральном уровне. Такой опыт привлекает внимание и позволяет проводить параллели с международными подходами, например, с Эстонией, которую ряд экспертов считает мировым лидером в области интернет-голосования.

В данной статье мы рассмотрим историю, особенности и современное состояние системы дистанционного электронного голосования в России и проведем сравнение с зарубежным опытом, в частности с эстонским.

История появления и развития дистанционного электронного голосования в России

Первый эксперимент с дистанционным электронным голосованием в России проводился 12 октября 2008 года в Тульской области в г. Новомосковске. Он проходил в одномандатном избирательном округе №3, где гражданам позволили выбрать депутата через интернет. Для реализации эксперимента создали специальную платформу, которая позволяла зарегистрированным пользователям проголосовать из любой точки, где есть доступ к сети [2].

В результате исследования были выявлены как положительные аспекты, так и отрицательные, среди которых была необходимость усовершенствования обеспечения анонимности избирателя и усиление

защиты данных. Однако, несмотря на выявленные недочеты, этот опыт был важным этапом для дальнейшего внедрения ДЭГ в Российской Федерации.

В период 2011 – 2019 годов активно разрабатывались нормативно-правовые акты и совершенствовались технологии для внедрения дистанционного электронного голосования. В 2011 году ЦИК (центральная избирательная комиссия) предоставила отчет, в котором сообщались перспективы развития ДЭГ, а также такие аспекты как обеспечение кибербезопасности, защита личных данных избирателей и борьба с фальсификациями.

С 2014 года велась работа по разработке единой платформы для проведения голосования. В это время технологии начали испытываться в рамках пилотных проектов, и активно обсуждались методы контроля за процессом голосования.

Полноценный эксперимент по внедрению ДЭГ в России был проведен в Москве на выборах депутатов в Московскую городскую думу. Это был первый масштабный тест системы, применённой в реальных условиях. Несмотря на зафиксированные уязвимости в шифровании и критику со стороны общественных организаций, проект получил положительные отзывы от пользователей, что дало толчок к дальнейшему развитию технологии.

В 2020 году, в период пандемии COVID-19, необходимость в ДЭГ значительно увеличилась и началось его широкое внедрение. В сентябре того же года ДЭГ было впервые использовано на выборах в Государственную думу и региональные органы власти в таких регионах, как Москва и Нижегородская область. Это событие стало важным в истории развития такого вида голосования в России.

Основные характеристики системы включали идентификацию избирателей через портал «Госуслуги», использование современных криптографических алгоритмов для защиты голосов и внедрение технологии блокчейн (метод безопасного хранения и передачи данных в виде цепочки блоков, которые соединяются между собой с помощью уникальных ключей, при этом каждый блок содержит информацию о предыдущем) для обеспечения безопасности данных [3].

В 2021 году внедрение ДЭГ значительно расширилось, и система стала доступна в семи регионах, что позволило провести дополнительные тесты с участием большего числа пользователей. Тогда же ЦИК России определила порядок и добавила новые меры для обеспечения еще большей прозрачности и безопасности избирательного процесса.

ДЭГ в наши дни продолжает стремительно развиваться. В 2022 году оно было внедрено в шестнадцати регионах, а в 2023 году – уже в двадцати семи. В 2024 году ДЭГ было впервые применено на выборах президента Российской Федерации в двадцати девяти регионах, что говорит нам о расширении применения и стремлении интегрировать её в избирательный процесс на более широком уровне.

Архитектура дистанционного электронное голосование в Российской Федерации

Система ДЭГ в России включает в себя несколько основных этапов, начиная от регистрации пользователей и заканчивая подсчётом голосов.

Сначала избиратель должен пройти регистрацию на портале «Госуслуги», при этом учетная запить должна быть подтвержденной. Это необходимо для того, чтобы принимать участие в голосовании могли только те граждане, которые имеют право голосовать. Затем, в установленные сроки, избиратель должен подать заявление на участие в дистанционном электронном голосовании там же. После проверки данных и подтверждения заявления об участии, гражданин получает доступ к электронному бюллетеню в день голосования.

В день выборов избиратель авторизуется в личном кабинете на платформе для голосования, проходя идентификацию через свою учётную запись. После этого ему предоставляется доступ к электронному избирательному бюллетеню, в котором он может выбрать понравившегося кандидата или партию. После того как выбор сделан, избиратель подтверждает его, отправляя голос в систему. Стоит отметить, что выбор можно поменять до того, как подтвердить его.

Одна из важных задач проведения ДЭГ – обеспечение безопасности данных и анонимности избирателя при голосовании. Для этого проводится шифрование данных, при помощи специальных криптографических алгоритмов. Это гарантирует тайну голосования. Для предотвращения фальсификаций и обеспечения прозрачности используется блокчейн-технология, которая записывает каждый голос в виде цепочки блоков. Эта система исключает возможность изменения или подделки голосов, обеспечивая сохранность и прозрачность всего процесса голосования.

После того, как завершится процесс голосования граждан, начинается расшифровка и подсчет голосов. Все данные подвергаются криптографической верификации, что исключает вероятность ошибок. В системе блокчейн каждый голос записывается и может быть проверен с помощью

криптографических ключей, что обеспечивает полную прозрачность подсчёта. Итоги выборов публикуются на официальных ресурсах.

Основные криптографические технологии в ДЭГ в России

Для обеспечения безопасности, конфиденциальности и прозрачности ДЭГ в России используются инновационные криптографические методики [4]. Рассмотрим ключевые составляющие данных подходов.

1. Гомоморфное шифрование

Гомоморфное шифрование [5] представляет собой один из ключевых элементов системы ДЭГ в России. Эта технология позволяет осуществлять вычисления с зашифрованными данными без их предварительной расшифровки. Это означает, что подсчёт голосов может проводиться без раскрытия их содержания, что гарантирует полную конфиденциальность избирателей.

К примеру, во время голосования каждый голос шифруется непосредственно на устройстве избирателя и остаётся зашифрованным на всех этапах: передачи, хранения и подсчёта. Расшифровке подлежат только окончательные результаты, что полностью исключает вмешательство в процесс обработки голосов.

2. Блокчейн-технология

В российских системах ДЭГ блокчейн активно используется [6] для повышения прозрачности процесса и гарантии неизменности информации. Основной принцип работы этой технологии заключается в хранении голосов в виде последовательных элементов (блоков), связанных друг с другом криптографическими методами [7].

Распределённая структура блокчейна исключает возможность изменения или удаления данных без согласия большинства участников сети. Это обеспечивает устойчивость системы к внешним вмешательствам и внутренним манипуляциям.

Кроме того, технология блокчейн позволяет осуществлять независимую проверку процесса голосования, поскольку каждая запись в системе остаётся доступной для анализа, но данные о личности избирателей защищены и сохраняют анонимность.

3. Электронная подпись

Электронная подпись (ЭП) играет ключевую роль в процессе идентификации избирателей и защиты их данных. Она позволяет подтвердить подлинность отправленного голоса и предотвратить подмену или искажение информации.

Алгоритм применения ЭП в системах ДЭГ включает следующие этапы:

- Избиратель подписывает свой голос с помощью индивидуального криптографического ключа.
- На сервере проводится проверка подписи с использованием открытого ключа, что подтверждает корректность и достоверность голоса.

Этот механизм предотвращает возможность голосования от имени другого человека и обеспечивает законность каждого бюллетеня.

Отметим, что в условиях квантовой угрозы [8] необходимо предусмотреть возможность усиления существующих схем ЭП с использованием квантовых [9] и постквантовых алгоритмов [10]

4. Двухуровневая аутентификация и защита каналов передачи данных

Для предотвращения несанкционированного доступа к системе ДЭГ и обеспечения безопасности передаваемой информации применяются следующие методы:

- Двухуровневая аутентификация, которая заключается в том, что избиратели подтверждают свою личность с использованием двух различных факторов, таких как одноразовый код или биометрические параметры.
- Шифрование каналов связи, которое заключается в том, что информация о голосовании передаётся через защищённые коммуникационные каналы, основанные на протоколах TLS/SSL, что предотвращает её перехват или изменение.

Эти меры помогают существенно снизить вероятность утечки информации и атак на систему.

Заметим, что для используемых криптографических технологий ДЭГ в случае применения нестандартизированных в Российской Федерации алгоритмов является актуальной задача проведения тестирования, верификации и валидации. Данная задача для систем распределенного реестра или блокчейн систем была предложена в [11] и развита в [12]. Также актуальна задача, связанная с защитой персональных данных [13].

Мировая практика применения дистанционного электронного голосования

По всему миру ДЭГ приобретает всё большую и большую популярность. Государства по-разному подходят к внедрению этой технологии, при этом учитывая свои национальные особенности. Однако опыт применения таких систем показывает как их потенциал, так и риски.

Эстония стала пионером [14] в применении дистанционного голосования на государственном уровне. Начиная с 2005 года, граждане могут голосовать онлайн, используя ID-карты или мобильные идентификаторы, что позволяет обеспечивать высокий уровень безопасности данных.

К особенностям эстонском системы можно отнести:

- Повторное голосование, которое заключается в том, что граждане могут менять своё решение до завершения периода голосования.
- Прозрачность, которая заключается в том, что внедрены механизмы общественного контроля, включая доступ к результатам аудита.

К 2021 году около 46,9% избирателей в Эстонии пользовались интернет-голосованием. Это демонстрирует, что грамотная технологическая база и доверие граждан могут обеспечить успешное функционирование системы электронного голосования.

Швейцария начала экспериментировать с ДЭГ в 2003 году, ориентируясь на граждан, проживающих за рубежом. Однако в 2019 году расширение системы было приостановлено из-за выявленных уязвимостей.

Германия начала использовать электронное голосование в 2005 году, но уже в 2009 году Федеральный конституционный суд запретил его, при этом отметив недостаточную прозрачность и невозможность контроля со стороны обычных граждан. В результате страна вернулась к бумажным бюллетеням, подчёркивая важность доверия к избирательному процессу.

В США электронное голосование через интернет используется ограниченно, в основном для военнослужащих и граждан, находящихся за границей. Несмотря на удобство, система сталкивается с препятствиями:

- Опасения кибератак.
- Низкий уровень доверия к технологии в условиях политической поляризации.

Нидерланды, которые начали использовать электронные системы голосования в 1990-х годах, в 2007 году отказались от них после выявления слабой защиты. Общественные протесты и независимые исследования показали уязвимость системы, что стало причиной возвращения к бумажным бюллетеням.

Франция начала использовать дистанционное голосование в 2003 году для граждан, проживающих за границей. Однако в 2017 году система была приостановлена из-за угрозы кибератак, что акцентировало внимание на необходимости более надёжной защиты.

Сравнение системы дистанционного электронного голосования в Российской Федерации и в Эстонии

Эстония и России – яркие примеры стран, которые активно внедряют системы ДЭГ. Однако подходы, технические решения и степень общественного доверия существенно различаются.

Эстония стала первой страной, которая реализовала систему интернет-голосования на национальном уровне. Впервые ДЭГ опробовали на выборах в 2005 году, и с тех пор его используют на всех уровнях выборных процессов.

В России внедрение системы ДЭГ началось существенно позже — первые испытания стартовали в широком формате в 2019 году, а в 2021 году она была задействована на выборах в Государственную Думу. В отличие от Эстонии, где дистанционное электронное голосование доступно всем гражданам, Россия пока сосредоточилась на проведении пробных проектов.

Эстония базируется на развитой национальной цифровой инфраструктуре, включающей ID-карты с микрочипами, мобильные идентификаторы и платформу X-Road, которая обеспечивает взаимодействие между государственными базами данных. Для защиты информации и обеспечения прозрачности избирательного процесса применяются технологии блокчейн. Здесь граждане могут голосовать с любого устройства, подключённого к интернету.

В России система функционирует на основе учётных записей пользователей на государственном портале «Госуслуги». С 2021 года началось использование блокчейн-технологий, что значительно

укрепило меры безопасности. Однако, в отличие от Эстонии, российская система доступна исключительно в регионах, где применяются технологии дистанционного электронного голосования.

Эстонская система гарантирует прозрачность благодаря возможности повторного голосования: если избиратель меняет своё решение, то учитывается только его последний выбор. После завершения выборов граждане могут убедиться, что их голос был засчитан, с помощью специального инструмента проверки. Систему регулярно тестируют независимые эксперты, а её программный код открыт для общественного анализа.

В России же применяется шифрование данных для обеспечения анонимности голосов. Итоги голосования подтверждаются публикацией хэш-значений, но полный процесс аудита доступен лишь ограниченному числу специалистов, что порождает вопросы о доступности общественного контроля за избирательной системой.

В Эстонии декларируется высокий уровень доверия граждан к системе ДЭГ. Это обусловлено прозрачностью процедур, высоким уровнем цифровой грамотности населения и многолетним опытом использования технологии. Стоит отметить, что в 2021 году около половины избирателей отдали свои голоса через интернет, что показывает широкое признание этой формы голосования.

В России общественное мнение о системе ДЭГ разделилось. Хотя многие отмечают удобство онлайн-голосования, сохраняются опасения относительно безопасности и объективности подсчёта голосов. Первоначальные этапы внедрения сопровождались техническими проблемами, что также сказалось на уровне доверия общества.

Заключение

Дистанционное электронное голосование (ДЭГ) представляет собой инновационный инструмент, способный существенно упростить процесс выборов, повысить его доступность и сократить организационные затраты. Рассмотрев опыт России и зарубежных стран, можно сделать вывод, что развитие этой технологии требует комплексного подхода, который включает обеспечение безопасности данных, прозрачности всех процедур и формирования доверия со стороны общества.

В России уже достигнуты значительные успехи в реализации ДЭГ: внедрение криптографических методов, таких как гомоморфное шифрование и блокчейн, которые позволяют защитить данные избирателей и предотвратить фальсификации. Однако остаются вызовы, связанные с киберугрозами, техническими сбоями и общественным восприятием системы.

Опыт Эстонии демонстрирует, что успешное внедрение электронного голосования возможно благодаря последовательной модернизации технологий и активной работе с гражданами. Этот пример подтверждает, что ДЭГ может стать эффективным инструментом цифровой демократии, если решить вопросы безопасности, правового регулирования и укрепления общественного доверия.

Также заметим, что для повышения уровня информационной безопасности систем ДЭГ нужно повышать криптографическую стойкость как классическую, так и квантовую для используемых криптографических систем и механизмов. Для этого, помимо прочего, должны быть проведены глубокие математические исследования (к примеру, как в [15-17]) для исследования различных характеристик [18 - 19] криптографических преобразований.

Таким образом, развитие дистанционного голосования – это важный шаг к цифровизации избирательных процессов, требующий постоянного совершенствования и ответственного подхода со стороны государства и общества.

Литература

1. *Борисов А.В*. Развитие электронного голосования // Журнал о выборах. 2011. № 4. С. 40. URL: http://cikrf.ru/about/library/journal/2011/n4/Borisov.pdf (дата обращения: 25.01.2025).

2. *Иванов А.В.* Эволюция дистанционного голосования в России: вызовы и перспективы // Российская юридическая наука. 2022. №3. С. 78-84.

3. *Волков В.Н., Смирнова Е.Л*. Цифровые технологии в избирательных процессах: мировой опыт и российская практика // Политика и общество. 2021. №2. С. 45-56.

4. *Пескова О.Ю., Фатеева С.В.* Электронное голосование: методы, риски и проблемы // Труды объединённой научной конференции "Интернет и современное общество". https://ojs.itmo.ru/index.php/IMS/article/view/245 (дата обращения: 25.01.2025).

5. *Babenko M.G., Golimblevskaia E.I., Shiriaev E.M.* Comparative Analysis of Homomorphic Encryption Algorithms Based on Learning with Errors // Proceedings of the Institute for System Programming of the RAS. 2020. Vol. 32, No. 2, pp. 37-52. DOI 10.15514/ISPRAS-2020-32(2)-4. EDN GHYJZY

6. *Угримова О.В*. Технология блокчейн в системах онлайн-голосования // rcoit.ru. URL: ссылка (дата обращения: 25.01.2025).

7. *Панков К.Н*. Использование криптографических средств для сквозных цифровых технологий на примере систем распределенного реестра // Технологии информационного общества : Материалы XII Международной отраслевой научно-технической конференции, Москва, 14-15 марта 2018 года. Том 1. М.: Издательский дом Медиа Паблишер, 2018. С. 365-366. EDN UUHHSM

8. Распоряжение Правительства РФ от 11 июля 2023 г. № 1856-р. Об утверждении Концепции регулирования отрасли квантовых коммуникаций в РФ до 2030 г. https://www.garant.ru/products/ipo/prime/doc/407297268/ (дата обращения: 25-01-2025).

9. *Панков К.Н., Миронов Ю.Б*. Применение квантовых методов в задачах защиты информации. М.: Горячая линия – Телеком, 2022. 212 с.

10. *Панков К.Н., Миронов Ю.Б*. Использование постквантовых алгоритмов в задачах защиты информации в телекоммуникационных системах. М.: Горячая линия – Телеком, 2023. 236 с. ISBN 978-5-9912-1015-7. EDN MTJUJL

11. *Pankov K.N*. Testing, Verification and Validation of Distributed Ledger Systems // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 19-20 марта 2020 г. Moscow: Institute of Electrical and Electronics Engineers Inc., 2020. P. 9078541. DOI 10.1109/IEEECONF48371.2020.9078541. EDN CITRFX

12. *Панков К.Н., Эйнман А.Д.* Сертификация систем распределенного реестра как инструмент обеспечения информационной безопасности // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11, № 2. С. 37-49. EDN CGQQYR

13. *Pankov K*. Enumeration of Boolean Mapping with Giv-en Cryptographic Properties for Personal Data Protec-tion in Blockchain Data Storage // Confer-ence of Open Innovations Association, FRUCT. 2019. No. 24, pp. 300-306. DOI 10.23919/FRUCT.2019.8711894. EDN BOVLMR

14. *Алексеев Р.А., Абрамов А.В*. Проблемы и перспективы применения электронного голосования и технологии избирательного блокчейна в России и за рубежом // Гражданин. Выборы. Власть. 2020. № 1(15). С. 9-21. EDN CUGOEQ

15. *Панков К.Н*. Локальная предельная теорема для распределения части вектора весов подфункций компонент случайного двоичного отображения // Математические вопросы криптографии. 2014. Т. 5, № 3. С. 49-80. EDN TFNXVD

16. *Pankov K.N*. Improved asymptotic estimates for the numbers of correlation-immune and k-resilient vectorial Boolean functions // Discrete Mathematics and Applications. 2019. Vol. 29, No. 3, pp. 195-213. DOI 10.1515/dma-2019-0018. EDN CFOLBU

17. *Kamlovskii O.V., Pankov K.N*. Some Classes of Balanced Functions over Finite Fields with a Small Value of the Linear Characteristic // Problems of Information Transmission. 2022. Vol. 58, No. 4, pp. 389-402. DOI 10.1134/s0032946022040093. EDN QSFFJO

18. *Панков К.Н*. Оценки скорости сходимости в предельных теоремах для совместных распределений части характеристик случайных двоичных отображений // Прикладная дискретная математика. 2012. № 4(18). С. 14-30. EDN PJPPCX

19. *Панков К.Н*. Оценки мощности классов отображений, применяемых в протоколах квантового распределения ключей / К. Н. Панков // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14, № 4. С. 4-18. DOI 10.36724/2409-5419-2022-14-4-4-18. EDN QKXSQK

РЕШЕНИЕ ПРОБЛЕМЫ ВОССТАНОВЛЕНИЯ ИНДЕКСОВ В OPEN DISTRO FOR ELASTICSEARCH ПОСЛЕ ПЕРЕЗАГРУЗКИ DOCKER-КОНТЕЙНЕРОВ

Малышев Максим Сергеевич
МТУСИ, студент группы БСТ2104, Москва, Россия
malysheff33ml@gmail.com

Гилимович Владимир Романович
МТУСИ, студент группы БСТ2104, Москва, Россия
gilimovich.v@icloud.com

Яковенко Наталья Викторовна
МТУСИ, старший преподаватель кафедры СИТиС, Москва, Россия
nv1906.iakovenko@yandex.ru

Гадасин Денис Вадимович
МТУСИ, доцент кафедры СИТиС, к.т.н., Москва, Россия
dengadiplom@mail.ru

Аннотация
В работе рассматриваются причины, которые могут привести к потери данных. Приводится инфраструктура предприятия, которая развернут в контейнерах. Системой мониторинга фиксируется сбой, который пытаются устранить на основании соответствующих политик. Ошибка не устраняется. Приводится детальный разбор ее составляющих, причина возникновения, прописываются рекомендации по усранению

Ключевые слова
Docker, контейнер, ошибка, сбой, устранение, восстановление индексов

Введение

В наши дни почти каждая сфера деятельности сталкивается с огромными объёмами сведений. Способность обрабатывать их быстро и надёжно существенно влияет на перспективы бизнеса. В противном случае можно упустить важные возможности или не успеть среагировать на внезапные изменения. Представьте масштаб: гигантские наборы сведений, поступающие с высокой скоростью, – и при всём этом нужно не просто аккумулировать информацию, но использовать её в процессе принятия управленческих решений.

В современных реалиях компаниям особенно важно:

- Систематизация: любое промедление в поиске нужной детали тормозит весь процесс.
- Мгновенный анализ: быстрая визуализация данных даёт возможность оперативно замечать тенденции.
- Заблаговременное оповещение: мониторинг и системы раннего предупреждения помогают своевременно реагировать на потенциальные риски.

Решение указанных сложностей возможно посредством Open Distro for Elasticsearch [1, 2]. Поскольку это полностью открытый продукт, организации могут избежать проблем, связанных с закрытыми лицензиями. В условиях неопределённой международной обстановки такое решение даёт компаниям свободу действий. Также мы воспользовались ещё одной технологией – контейнеризацией – для изолированного запуска наших сервисов Elasticsearch посредством Docker, так как он предоставляет удобные возможности для настройки и дальнейшего масштабирования. Но однажды все индексы и параметры Elasticsearch бесследно пропали из интерфейса системы после перезагрузки контейнеров. Этот опыт оказался весьма показательным: как выяснилось, без продуманной схемы хранения информации можно потерять критические данные.

В этой статье мы подробно расскажем о причинах, которые привели к потере данных, и о шагах, позволивших восстановить их. Кроме того, мы предложим проверенные приёмы организации хранения.

Анализ инфраструктуры

Компания "Никонора", специализирующаяся на решениях в области защиты и обработки данных, использует гибкую инфраструктуру, способную адаптироваться к требованиям клиентов. Часть архитектуры размещается в кластерах [3-6]. В рамках данной архитектуры использовались два горячих узла (hot-узла) для активной обработки и быстрого доступа к наиболее актуальным данным, а также два тёплых узла (warm-узла) для хранения менее востребованных архивных данных. Горячие узлы обеспечивают высокую производительность при текущих запросах, тогда как тёплые узлы служат для экономичного хранения больших объёмов данных, к которым обращаются реже.

Вся инфраструктура была развернута в Docker-контейнерах, что предоставляло возможность гибкого управления и масштабирования системы [7]. Каждый узел был смонтирован к отдельной директории на хост-машине, содержащей также настройки кластера:

Горячие узлы: /mnt/hot-1, /mnt/hot-2

Тёплые узлы: /mnt/warm-1, /mnt/warm-2

Логика взаимодействия на схеме:

Клиентские запросы (например, аналитические запросы, пользовательский поиск) поступают к «горячим» узлам (Hot-Node #1 и #2). Они обрабатывают наиболее актуальные данные для обеспечения высокой скорости работы.

Горячие узлы (Hot-Node #1 и #2), помимо обслуживания текущих запросов, могут при необходимости обращаться к «тёплым» узлам (Warm-Node #1 и #2) за архивными данными. Между горячими и тёплыми узлами может происходить репликация и обмен данными, а также миграция данных в зависимости от политики хранения.

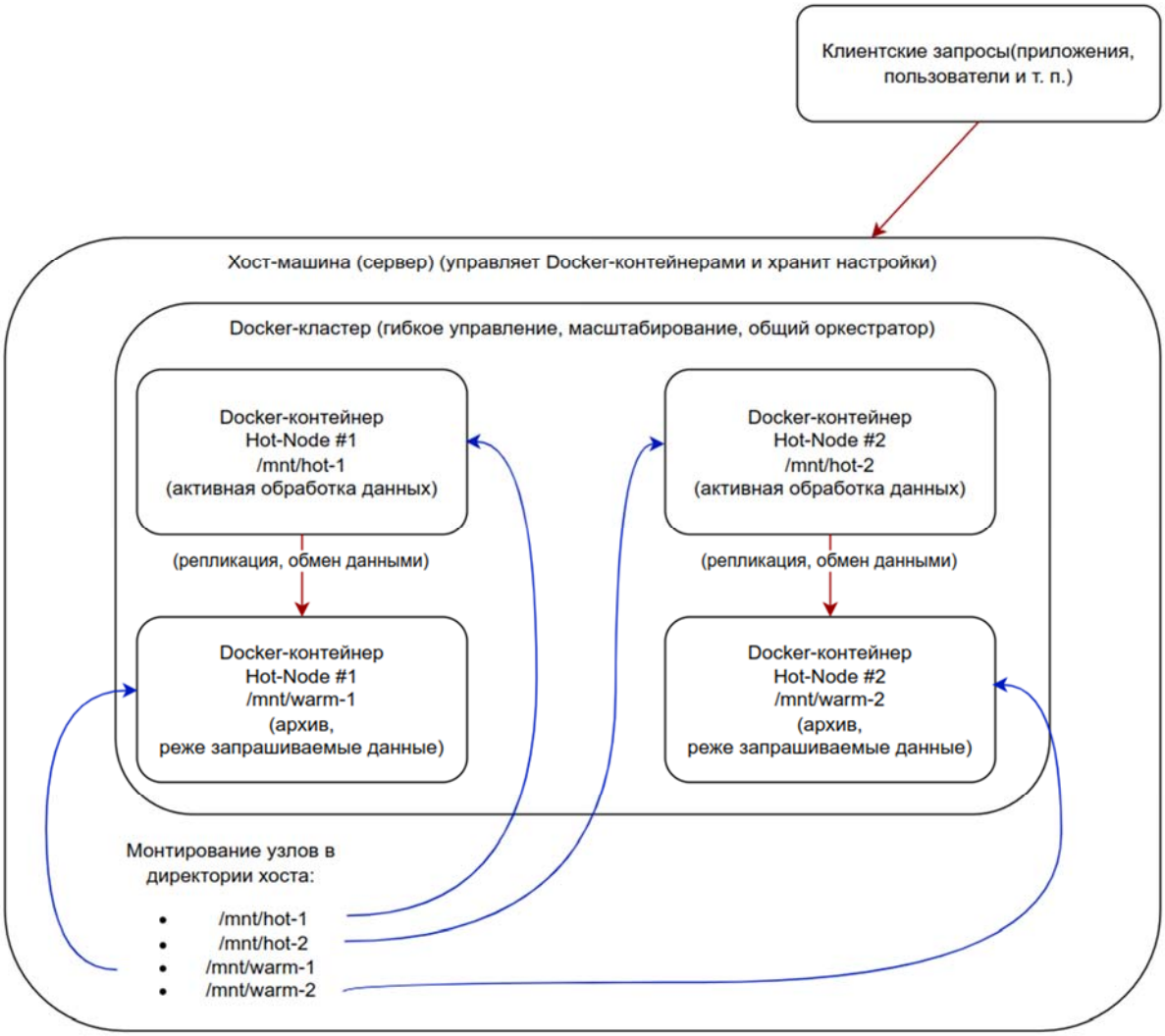

Рис. 1. Схема взаимодействия компонентов инфраструктуры

Тёплые узлы (Warm-Node #1 и #2) служат для экономичного хранения больших объёмов редко востребованных данных. Они также развёрнуты в Docker-контейнерах и смонтированы к соответствующим директориям на хост-машине.

Хост-машина содержит все необходимые настройки кластера и управляет жизненным циклом Docker-контейнеров (запуск, остановка, масштабирование и т.д.). Каждый контейнер (узел) имеет доступ к своей физической директории (смонтированной папке /mnt/...), где хранит нужные данные и конфигурационные файлы.

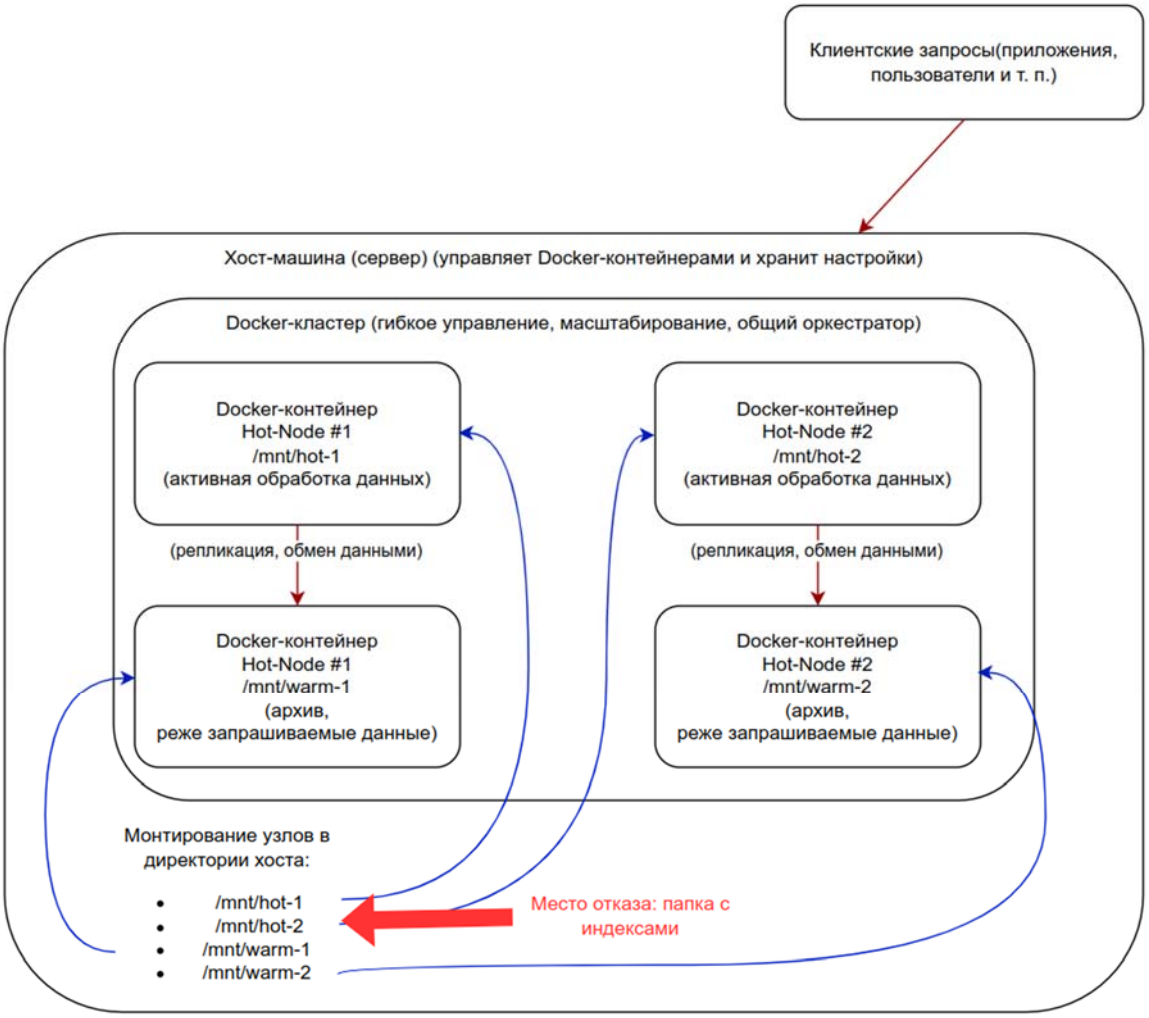

Рис. 2. Место отказа на схеме

Таким образом, на схеме видно:

Четыре узла (два горячих и два тёплых), каждый в своём Docker-контейнере.

Директории, смонтированные на хост-машине.

Основные связи: входящие запросы к горячим узлам, обмен данными между горячими и тёплыми, а также наличие общей инфраструктуры Docker.

В процессе восстановления команда компании Никонора разработала аргоритм действия представленый в таблице 1.

Система функционировала эффективно до момента внезапного сбоя. Система мониторинга компании оперативно зафиксировала проблему, и дежурный инженер незамедлительно приступил к её устранению, руководствуясь установленными процедурами. В процессе диагностики были проанализированы логи системы и проверена доступность всех узлов кластера [8-10].

После плановой перезагрузки системы и пересоздания Docker-контейнеров при попытке выполнения запросов к кластеру было обнаружено отсутствие всех индексов, что привело к тому, что система функционировала как новая, без каких-либо данных. В ходе проверки выяснилось, что папка с индексами была перемещена, что сделало её недоступной для кластера ElasticSearch. Это привело к полной потере данных при попытке работы с кластером.

Таблица 1

Алгоритм действий

Шаг	Описание	Результат
1	Анализ состояния системы: Проверить логи системы, доступность узлов и состояние папок с данными на диске.	Выявление причин потери индексов (например, перемещение папки индексов).
2	Возврат папки индексов: Переместить старую директорию индексов в соответствующее место на диске.	Восстановление доступности пользовательских индексов на горячих узлах.
3	Удаление системного индекса безопасности: Удалить индекс opendistro_security для устранения конфликта настроек безопасности.	Elasticsearch запускается без ошибок безопасности.
4	Очистка устаревших данных: Удалить конфликтующие или устаревшие настройки в папке индексов.	Устранение возможных причин сбоев при запуске Elasticsearch.
5	Проверка состояния узлов через API: Использовать API (_cat/indices, _dangling) для анализа состояния индексов.	Обнаружение "висящих" индексов (dangling indices).
6	Восстановление висящих индексов: Выполнить POST-запрос с параметром accept_data_loss=true для каждого dangling-индекса.	Регистрация "висящих" индексов в кластере.
7	Разработка автоматизации: Использовать Python-скрипт для автоматизированного восстановления всех индексов.	Упрощение и ускорение восстановления индексов на тёплых узлах.
8	Тестирование: Проверить работоспособность системы на тестовом стенде перед развертыванием изменений в продакшене.	Гарантия отсутствия ошибок и безопасное внедрение решений.

Компания предприняла меры по воссозданию аналогичных условий на тестовом стенде, провела тестирование различных вариантов решения, на основе разработнанного алгоритма, и выбрала наиболее эффективный метод для безболезненного восстановления функционирования системы.

Прежде чем приступить к восстановлению системы необходимо было провести перераспределение нагрузки на другие узлы, чтобы избежать еще больших потерь [11-14]. В качестве первого шага восстановления системы команда решила вернуть содержимое старой директории с индексами в новую. Для этого все индексы были скопированы из старой папки в новую с надеждой на то, что Elasticsearch автоматически их распознает и восстановит работоспособность. Однако после перезапуска Elasticsearch возникла следующая ошибка: «OpenDistro Security not initialized». Причиной данной ошибки стало использование Elasticsearch специальных системных индексов. Один из ключевых индексов, «opendistro_security», отвечает за хранение настроек безопасности, включая пользователей, роли и права доступа. Этот индекс зашифрован и привязан к конкретному узлу в кластере. Был сделан вывод, что простое копирование системного индекса без учета его зависимостей и специфических конфигураций привело к конфликту в работе Elasticsearch. Несмотря на то, что сам индекс безопасности не был поврежден, его некорректное перемещение вызвало сбой системы. Этот инцидент подчеркнул необходимость более детального и комплексного подхода при восстановлении системных компонентов.

```
{
  "cluster_name": "alertix-data",
  "status": "yellow",
  "timed_out": false,
  "number_of_nodes": 2,
  "number_of_data_nodes": 2,
  "active_primary_shards": 324,
  "active_shards": 339,
  "relocating_shards": 0,
  "initializing_shards": 4,
  "unassigned_shards": 305,
  "delayed_unassigned_shards": 0,
  "number_of_pending_tasks": 0,
  "number_of_in_flight_fetch": 0,
  "task_max_waiting_in_queue_millis": 0,
  "active_shards_percent_as_number": 52.31481481481482
}
```


Рис. 3. Демонстрация успешного запуска кластера

Понимая, что проблема была связана с системным индексом безопасности, команда предприняла следующие шаги для её устранения:

Индекс «opendistro_security» был удален из директории индексов. Это действие позволило устранить конфликты, связанные с настройками безопасности, обеспечив корректную работу Elasticsearch.

Были очищены дополнительные настройки в папке индексов, которые могли содержать устаревшие или конфликтующие данные. Данный шаг способствовал устранению потенциальных причин сбоев и обеспечению чистоты конфигурации.

После выполнения указанных мероприятий был произведен перезапуск Elasticsearch на горячих узлах. Сервис успешно запустился, и все пользовательские индексы были отображены корректно. Это подтвердило успешное решение проблемы на горячих узлах и восстановление нормальной работы системы.

Несмотря на успешное применение аналогичных действий на горячих узлах, на warm-узлах проблема не была решена. После перезапуска и выполнения тех же шагов индексы продолжали не отображаться при выполнении запросов к Elasticsearch. В ходе расследования было принято решение обратиться к API Elasticsearch для получения информации о состоянии узлов и доступных индексах.

С помощью запросов к API _cat/indices и _dangling было обнаружено, что перенесенные индексы распознаны как "висящие" (dangling indices). Это означает, что данные индексов физически присутствуют на диске узла, но кластер не регистрирует их и не включает в список доступных индексов. В результате информация об индексах не отображалась, несмотря на их наличие на уровне диска [15-17].

Для решения проблемы было принято решение автоматизировать процесс восстановления индексов на warm-узлах посредством разработки Python-скрипта. Скрипт выполнял следующие функции:

Собирал данные о «висящих» индексах, с помощью GET-запроса к API _dangling, получая список всех индексов, находящихся на диске, но не зарегистрированных в кластере.

Производил аутентификация для безопасного доступа к API Elasticsearch с помощью сертификатов admin.crt и admin.key.

Выполнял POST-запрос к API с параметром accept_data_loss=true, Для каждого идентификатора индекса (index_uuid), что позволило восстановить индекс.

Скрипт фиксировал информацию об успешном восстановлении или возникших ошибках, а также обрабатывал возможные исключения при работе с файлами.

После выполнения скрипта на warm-узлах все индексы были успешно восстановлены и стали доступны для поиска и обработки. Это позволило полностью восстановить работоспособность кластера и обеспечить доступ к данным.

Рис. 4. Повышение объема событий, после восстановления

Рекомендации

Для решения проблемы восстановления индексов в системе Elasticsearch необходимо следовать следующему алгоритму.

Сначала проводится диагностика: проверяется состояние узлов, анализируются системные логи и доступность данных на диске. Дополнительно используется API Elasticsearch (_cat/indices и _dangling) для анализа состояния индексов. Затем восстанавливаются горячие узлы: папка с пользовательскими индексами перемещается в нужное место, удаляется системный индекс opendistro_security для устранения конфликтов, очищаются устаревшие настройки, и узлы перезапускаются. Для тёплых узлов проводится обнаружение "висящих" индексов через API _dangling, после чего они регистрируются с использованием параметра accept_data_loss=true. После этого рекомендуется разработать автоматизацию, которая упростит и ускорит процесс восстановления индексов на всех узлах. Завершается процесс тестированием всех изменений на тестовом стенде перед внедрением в рабочую среду.

Дополнительно для повышения надёжности [18-20] и предотвращения подобных проблем в будущем рекомендуется:

Разработка специализированных процедур для разных типов узлов: создать отдельные процедуры восстановления для горячих и тёплых узлов, учитывающие их уникальные требования и особенности. Это обеспечит более эффективное и безопасное восстановление системы.

Внедрение автоматизированных решений для управления индексами: разработать и интегрировать автоматизированные решения для управления и восстановления индексов. Это позволит снизить нагрузку на инженеров и повысить точность операций.

Усиление процессов тестирования и валидации: внедрить строгие процессы тестирования и проверки процедур восстановления на тестовых стендах перед их применением в рабочей среде. Это поможет заранее выявить и устранить возможные ошибки.

Улучшение системы мониторинга: расширить функциональность мониторинга для детального отслеживания состояния индексов и узлов. Это позволит быстрее обнаруживать проблемы и оперативно реагировать на них.

Повышение квалификации сотрудников: инвестировать в обучение и повышение квалификации сотрудников, ответственных за управление и восстановление системы. Это обеспечит более эффективное и компетентное реагирование на инциденты.

Заключение

Восстановление индексов в системе Elasticsearch после возникновения сбоя оказалось задачей высокой сложности, требующей не только глубокого понимания внутренней архитектуры системы. Благодаря детальному анализу проблемы и применению адекватных инструментов, нам удалось вернуть кластер в рабочее состояние без утраты данных.

Особое внимание было уделено тщательному тестированию всех этапов на тестовом стенде перед внедрением изменений в производственную среду. Это имело решающее значение, поскольку данные, хранящиеся в кластере, могут потребоваться для последующего расследования инцидентов. Любая утрата информации могла негативно сказаться на функционировании компании и усложнить процесс расследования.

Полученный опыт подчеркнул необходимость правильной настройки инфраструктуры, регулярного создания резервных копий и предварительного тестирования всех процедур. Мы надеемся, что наше решение окажется полезным для других специалистов, позволяя им избегать подобных проблем и эффективно восстанавливать системы при сбоях, минимизируя возможные риски и потери данных.

Литература

1. *Гормли К., Тонг З.* Elasticsearch: The Definitive Guide // O'Reilly Media. 2015. 724 с.

2. *Куц Р., Рогозински М.* Mastering Elasticsearch // Packt Publishing. 2015. 424 с.

3. *Гадасин Д.В., Золотарева П.Ю., Тремасова Л.А.* Влияние кластеризации при обработке сырых данных // Системы синхронизации, формирования и обработки сигналов. 2024. Т. 15, № 3. С. 10-19. EDN JQIPHX

4. *Мелькова Е.К., Шведов А.В., Тремасова Л.А., Гадасин Д.В.* Организация кластера исходя из функции принадлежности // Системы синхронизации, формирования и обработки сигналов. 2023. Т. 14, № 1. С. 30-39. EDN CNVIJU

5. *Тремасова Л.А., Первухина А.А., Гадасин Д.В.* Использование методов Косарайю и k-средних для формирования кластеров // Электросвязь. 2024. № 9. С. 47-55. DOI 10.34832/ELSV.2024.58.9.007. EDN DOZTZK

6. *Гадасин Д.В.* Построение бинарного дерева минимальной цены // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18, № 11. С. 38-44. DOI 10.36724/2072-8735-2024-18-11-38-44. EDN GMCEWG

7. *Георге Р., Лупу М., Кондра М.* Elasticsearch in Action // Manning Publications. 2015. 325 с.

8. *Гадасин Д.В., Малышев М.С., Гилимович В.Р.* Устранение сбоя работы системы средствами openvpn // Теория и практика экономики и предпринимательства: Труды XXI Международной научно-практической конференции, Симферополь – Гурзуф, 18-20 апреля 2024 г. Симферополь: ИП Зуева Т. В., 2024. С. 231-233. EDN SZSCNH

9. *Гадасин Д.В., Пантелеева К.А., Маклачков К.А.* Разработка единой точки входа сообщений о пользовательском негативном опыте взаимодействия с web-сервисами // Искусственный интеллект в автоматизированных системах управления и обработки данных : Сборник статей II Всероссийской научной конференции. В 5-ти томах, Москва, 27-28 апреля 2023 г. М.: Издательский дом КДУ, "Добросвет", 2024. С. 413-417. EDN ADRGFV

10. *Гадасин Д.В., Бессолицын А.Д., Гадасин Д.Д.* Оценка качества данных информационных систем // DSPA: Вопросы применения цифровой обработки сигналов. 2024. Т. 14, № 2. С. 4-12. EDN GYIWJU

11. *Гадасин Д.В., Вакурин И.С., Тремасова Л.А*. Алгоритм распределения данных между системами хранения на основе свойства самоподобия // Электросвязь. 2024. № 4. С. 44-50. DOI 10.34832/ELSV.2024.53.4.007. EDN BRSLCL

12. *Гадасин Д.В., Шведов А.В*. Применение транспортной задачи для балансировки нагрузки в условиях нечеткости исходных данных // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18, № 1. С. 13-20. DOI 10.36724/2072-8735-2024-18-1-13-20. EDN WKNPIX

13. *Tremasova L.A., Andriyanova A.K., Gadasin D.V., Gadasin D.D*. Modeling and Solving the Problem of Load Balancing in Data Transmission Networks Using the Stepping Stone Method // 2024 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russian Federation, 2024, pp. 1-7, doi: 10.1109/IEEECONF60226.2024.10496718.

14. *Shvedov A.V., Gadasin D.V., Klygina O.G., Tremasova L.A*. Optimization of Network Routing Using the Markov Decision Process and Hamiltonian Cycle // 2023 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russian Federation, 2023, pp. 1-4, doi:10.1109/IEEECONF56737.2023.10091989.

15. *Гадасин Д.В., Комкова М.Г., Пантелеева К.А., Гадасин Д.Д.* Связь между величиной энтропии и количеством информации при представлении предметной области разными лингвистическими единицами // DSPA: Вопросы применения цифровой обработки сигналов. 2023. Т. 13, № 2. С. 12-21. EDN WRHCSW

16. *Гадасин Д.В., Бессолицын А.Д*. Виды и методы структурирования данных из различных информационных систем: анализ и применение // Актуальные проблемы и перспективы развития экономики, Симферополь – Гурзуф, 12-14 октября 2023 г. Симферополь: ИП Зуева Т. В., 2023. С. 202-204. EDN UGZRXL

17. *Пантелеева К.А., Палибза С.А., Гадасин Д.В*. Принципы построения системы управления при возникновении сбоев в ит-инфраструктуре // REDS: Телекоммуникационные устройства и системы. 2024. Т. 14, № 2. С. 24-34. EDN MOYCNG

18. *Gadasin V.A., Gadasin D.V*. Reliability of large-scale communication networks with additive structure // Automation and Remote Control. 1997. Vol. 58, No. 1 Part 2, pp. 130-140. EDN KBCUTS

19. *Гадасин В.А., Гадасин Д.В.* Надежность двухполюсных сетей с аддитивной структурой II. Финальная вероятность связи // Автоматика и телемеханика. 1999. № 10. С. 164-179. EDN OKEMTZ

20. *Гадасин Д.В., Лисиненко Е.К., Юсифов Э.С., Савин В.А.* Оценка регрессионных моделей Исходя из показателей качества // Системы синхронизации, формирования и обработки сигналов. 2024. Т. 15, № 1. С. 4-16. EDN CSWKOE

КАК ЭФФЕКТИВНО ОБЩАТЬСЯ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Мугдусян Лусинэ Сержиковна
студент 3 курса магистратуры Московского технического университета связи и информатики, Москва, Россия
mugdusyan_lusine@mail.ru

Аннотация
В данной статье рассматриваются вопросы формулировки запросов (промптов) для эффективного взаимодействия с искусственным интеллектом. Описаны способы составления промптов для автоматизации и повышения продуктивности бизнес-процессов. Представлены примеры применения промптов в разных областях бизнеса. На основе анализа сделаны заключения о потенциале внедрения крупных языковых моделей в бизнес-процессы.

Ключевые слова
Промпт, промпт-инжиниринг, искусственный интеллект, большие языковые модели, автоматизация, анализ данных, формулирование запросов, машинное обучение, бизнес

Введение

В современном мире, где искусственный интеллект становится неотъемлемой частью жизни, умение формулировать запросы определяет, насколько эффективно вы сможете использовать эти технологии. Этот навык помогает как в повседневной жизни, так и в профессиональной деятельности, открывая перед пользователем новые горизонты возможностей [4]. В современной практике управления бизнесом как малые, так и крупные компании активно внедряют технологии искусственного интеллекта для оптимизации процессов принятия решений, повышения качества обслуживания клиентов и автоматизации рутинных операций. [2]. Увеличение масштабов использования искусственного интеллекта в различных отраслях обуславливает растущий спрос на специалистов в области промпт-инженерии, чья задача заключается в разработке и внедрении решений на основе искусственного интеллекта, направленных на достижение стратегических целей организаций.

Промпт-инжиниринг – это искусство взаимодействия с искусственным интеллектом, заключающийся в разработке структурированных и детализированных инструкций для решения разных задач. Этот метод позволяет достичь более точных и релевантных результатов при работе с большой языковой моделью.

Результаты исследования

Большая языковая модель (LLM – Large Language Model) – это система искусственного интеллекта, обученная на обширных массивах данных, способная генерировать ответы на пользовательские запросы. Функционирование таких моделей основывается на обработке входных данных (промптов), которые определяют характер и содержание выходных данных. LLM способны выполнять различные задачи, включая генерацию текста, переводы с разных языков. Качество результатов напрямую зависят от точности и детализации промптов. овременные LLM, такие как ChatGPT, Bard и другие, показывают высокую эффективность в решении сложных задач. Однако, успешное применение LLM требует глубокого понимания принципов промпт-инжиниринга, поскольку именно от качества входных инструкций зависит конечный результат работы модели.

Промпт – это любой запрос к LLM. Правильно сформулированный промпт – это основа успешного взаимодействия с искусственным интеллектом. Большинство моделей поддерживают промпты как на русском, так и на английском языке. Расплывчатые или неконкретные запросы могут привести к неточным или нерелевантным результатам.

Качество формулировки промпта влияет на эффективность работы специалиста, занимающегося разработкой промпта. Промпт может включать в себя ряд структурных элементов, среди которых:

1. Инструкция – представляет собой четко сформулированное задание или указание, которое требуется выполнить модели в рамках поставленной задачи.

2. Контекст – представляет собой дополнительные данные и информацию, которые могут быть

использованы для улучшения качества и релевантности ответов, генерируемых моделью.

3. Роль – модель поведения, соответствующая конкретному персонажу или статусу (например, роль может предполагать имитацию поведения эксперта для получения ответа на специализированный вопрос).

4. Входные данные – исходная информация или запрос, на основе которого мы осуществляем решение задачи или поиск ответа.

5. Индикатор вывода – параметр, определяющий формат или тип результирующих данных, а также стилистику представления ответа (например, формирование ответа в соответствии с требованиями научного стиля изложения).

Выбор элементов и структуры промпта определяется конкретной задачей, что дает возможность адаптировать его формат в зависимости от целей использования. LLM умеют решать несколько типов задач. Под каждый тип задач используется соответствующий промпт:

1. Открытые вопросы. Данный тип вопросов предполагает получение развернутого ответа, который может включать в себя объяснение, ссылку на фактические данные, выполнение вычислений и т.п. Вопросы такого рода часто начинаются с ключевых слов: "кто", "что", "где", "почему" и "каким образом".

2. Закрытые вопросы. Данный тип вопросов предполагает получение краткого и однозначного ответа без необходимости дополнительных или развернутых пояснений. Основные ключевые слова, характерные для данного типа вопросов: "выбрать", "дать ответ".

3. Генерация. Метод создания текстового контента, включая научные статьи, литературные произведения, новостные материалы. В качестве основных ключевых слов для генерации текста можно использовать: "придумать", "написать", "сочинить", "рассказать".

4. Мозговой штурм. Процесс создания идей и последующего отбора наиболее удачной. В качестве ключевых слов можно использовать: "предложить варианты", "сгенерировать идеи").

5. Чат. Это формат свободного общения с языковой моделью, где можно общаться с ней на различные темы, как с обычным собеседником.

6. Логические рассуждения и анализ. Промпты которые просят языковую модель проанализировать данные и предоставить четкий ответ. Ключевыми словами тут будут: "поясни", "аргументируй".

7. Редактирование текста. Такие промпты позволяют исправлять ошибки, расставлять заголовки, форматировать текст. Ключевые слова: "исправь ошибки", "отредактируй".

8. Классификация. Промпты используются для сортировки и анализа информации. Ключевые слова: "распредели", "отсортируй".

9. Перевод текста. Эти промпты используются для перевода текста с одного языка на другой. Ключевые слова: "переведи".

10. Обобщение. Данные промпты помогают выделить основные тезисы из текста и сократить его. Ключевые слова: "сократи", "суммаризируй".

11. Переписывание. Такие промпты помогают переписать текст или переформулировать вопросы. Ключевые слова: "перепиши", "измени формулировку".

12. Извлечение. Эти промпты помогают выделить нужные детали из текста. Ключевые слова: "найди", "выдели".

13. Генерация кода. Данные промпты помогают написать код на множестве языках программирования. Ключевые слова: "напиши код на".

Существует множество разных способов создания промптов, однако самыми популярными из них являются:

1. Подсказка: этот подход заключается в том, чтобы дать языковой модели несколько примеров (N-shot) ожидаемого результата перед тем, как запросить у нее генерацию собственного ответа. Такой метод можно применять для решения разнообразных задач, включая перевод текста, его сокращение или написание программного кода.

2. Цепочка подсказок (Chain-of-thought): этот подход заключается в разделении сложной задачи на несколько более простых и мелких шагов. Языковой модели даются указания выполнять эти шаги последовательно, причем результат каждого этапа становится входными данными для следующего. Такой метод может применяться для решения задач, таких как ответы на вопросы или анализ проблем.

3. Промптинг генераций знаний (Generated Knowledge Prompting): этот подход предполагает создание запросов, в которые добавляются дополнительные данные или знания, не входящие в изначальный набор обучения языковой модели. Такой способ позволяет улучшить точность и детализацию результатов, выдаваемых моделью.

4. Положительные и отрицательные промпты: этот подход включает применение как позитивных промптов (которые направляют LLM на создание определенных типов результатов), так и негативных (которые ограничивают LLM в генерации нежелательных типов данных). Такой метод позволяет управлять стилем и тоном выходных данных модели, а также предотвращать формирование вредоносного или оскорбительного контента.

5. Интерактивный контекстно-зависимый промпт: этот метод заключается в последовательном уточнении запроса на основе ответов, полученных от языковой модели. Такой подход позволяет улучшить понимание моделью сложных или неоднозначных запросов и помогает ей давать более точные и релевантные ответы.

6. Ролевой промптинг: этот подход предполагает, что языковая модель принимает на себя конкретную роль или идентичность при создании текста. Такой прием позволяет генерировать более творческие и интересные материалы, например, рассказы или сценарии.

Промпт для задания с несколькими вариантами ответов (MCQ): Данный подход предполагает, что языковой модели предлагается несколько вариантов ответа на один вопрос, а также дается указание выбрать верный ответ из предложенного списка.

Теперь рассмотрим базовые принципы формулировки промптов которые обеспечивают более точные и эффективные результаты.

1. Четкость и точность: Формулируйте ясные, лаконичные и конкретные указания, которые четко описывают поставленную задачу или ожидаемый результат. Промпт должен быть понятным и не допускать двусмысленностей, чтобы модель могла его правильно интерпретировать.

2. Постановка цели: четко сформулируйте, какую цель вы преследуете с помощью промпта. Это может быть генерация текстов в различных креативных форматах, перевод на иностранные языки, создание разнообразного творческого контента или предоставление подробных ответов на вопросы.

3. Функционал модели: Осознайте, на что способна языковая модель и какие у нее ограничения. Настраивайте запросы так, чтобы они учитывали сильные стороны модели, и старайтесь не давать задачи, которые выходят за пределы её возможностей.

4. Итерации и тестирование: Пробуйте разные варианты формулировок и подходов, чтобы достичь лучшего результата и получить нужные выходные данные. Регулярно тестируйте и дорабатывайте запрос, чтобы сделать его более эффективным.

5. Обратная связь и доработка: Учитывайте мнения пользователей и экспертов, чтобы улучшить промпт и сделать его более эффективным. Регулярно дорабатывайте промпт на основе полученных отзывов, чтобы гарантировать стабильное достижение нужных результатов.

Эти принципы закладывают прочную основу для создания эффективных промптов, которые могут направлять искусственный интеллект на получение желаемых результатов в широком диапазоне задач и приложений.

Рассмотрим примеры промптов для сотрудников из сферы информационных технологий.

1. Инструкция: определите приоритеты в списке функций продукта, учитывая интересы пользователей и цели бизнеса.

Контекст: у команды разработчиков есть перечень возможных функций, которые могут быть внедрены в продукт.

Входные данные: Список функций продукта, обратная связь от пользователей и аналитика использования существующих функций.

Индикатор результата: Ранжированный список функций продукта, упорядоченный по их значимости для пользователей и соответствию бизнес-задачам.

2. Инструкция: Разработайте профиль пользователя, который будет описывать целевую аудиторию нового продукта.

Контекст: Продукт – это программное приложение, созданное для помощи малому бизнесу в управлении финансами.

Входные данные: отсутствуют

Индикатор результата: Детальный профиль пользователя, включающий демографические данные, проблемы и поведенческие особенности целевой аудитории.

3. Инструкция: Создайте план разработки нового мобильного приложения, которое будет удовлетворять запросы пользователей, будет реализовано в установленные сроки и не выйдет за рамки бюджета.

Контекст: Приложение ориентировано на занятых профессионалов, которым необходимо удобное решение для управления задачами и поддержания организованности. Оно должно обладать простым и понятным интерфейсом, быть легким в использовании и поддерживать интеграцию с популярными

сервисами для повышения эффективности.

Входные данные: отсутствуют

Индикатор результата: План развития продукта с указанием сроков, стадий реализации и распределения ресурсов.

4. Инструкция: Изучи отзывы пользователей и определи основные проблемы и направления для улучшения.

Контекст: Разработчики собрали обратную связь от пользователей через опросы и формы для отзывов в приложении.

Входные данные: отзывы включающий комментарии, пожелания и информация о сбоях.

Индикатор результата: документ, в котором кратко изложены ключевые выводы анализа отзывов, включая понимание нужд пользователей, их проблем и болевых зон, которые нуждаются в доработке.

5. Инструкция: Создай план действий, направленный на облегчение адаптации клиентов и снижение уровня оттока (Customer Churn Rate).

Контекст: Компания сталкивается с большим процентом ухода новых клиентов.

Входные данные: Информация о методах и процедурах привлечения клиентов, уровне оттока и степени их удовлетворенности.

Индикатор результата: Разработанная стратегия, которая сделает процесс привлечения клиентов более эффективным и снизит их отток. План должен включать предложения по упрощению привлечения клиентов, усилению поддержки и увеличению их вовлеченности.

6. Инструкция: Выполни анализ конкурентов и выяви преимущества и недостатки продуктов и оказываемых услуг компании.

Контекст: Компания функционирует в условиях высокой конкуренции.

Входные данные: Данные о товарах, услугах, ценовой политике и маркетинговых подходах конкурентов.

Индикатор результата: Отчет по анализу конкурентов, содержащий основные выводы, учитывая преимущества и недостатки конкурентов, а также возможности для выделения компании на рынке.

7. Инструкция: Разработай стратегию для анализа эффективности внедрения нового продукта.

Контекст: Компания планирует внедрить на рынок новый продукт.

Входные данные: Задачи выпуска продукта, ключевые метрики маркетинга и информация об уровне удовлетворенности клиентов.

Индикатор результата: Стратегия анализа эффективности внедрения продукта, охватывающая основные метрики, способы сбора информации и процессы формирования отчетов.

Каждый из этих примеров демонстрирует, как искусственный интеллект помогает в решении задач, которые раньше требовали значительных усилий и времени.

В профессиональной среде промпт-инжиниринг становится ключом к повышению продуктивности. Рассмотрим основные сценарии применения искусственного интеллекта в бизнесе:

1. Автоматизация и аналитика. Запросы вроде "Создай отчёт о продажах за последний месяц" позволяют мгновенно получить анализ данных. Это экономит время сотрудников и освобождает их для выполнения более творческих задач.

2. Маркетинг и контент. Промпт "Придумай идеи для рекламной кампании экологического бренда" помогает генерировать креативные решения быстрее, чем традиционные методы мозгового штурма [6]. Искусственный интеллект также может предложить несколько вариантов стратегий продвижения.

3. Клиентская поддержка. Чат-боты, работающие на основе продуманных запросов, мгновенно решают проблемы клиентов. Это повышает удовлетворённость клиентов и снижает нагрузку на отделы поддержки.

4. Стратегическое планирование. Запрос "Проанализируй конкурентов в сфере доставки продуктов" помогает оценивать рынок, выявлять возможности и угрозы, что крайне важно для разработки стратегий роста компании.

5. Управление проектами. Искусственный интеллект способен облегчить создание детализированных планов проектов. Например, промпт "Создай проектный план для запуска нового продукта с указанием временных рамок и ресурсов" позволяет эффективно распределить задачи и сроки.

Использование преимуществ промпт-инжиниринга приносит огромные выгоды как для личного, так и для профессионального использования:

1. Экономия времени: Быстрое получение ответов и решений.

2. Креативность: Предложение неожиданных идей и подходов к решению задач.

3. Образование: Доступ к обширным знаниям в удобной и понятной форме.

4. Автоматизация: Упрощение рутинных процессов.

5. Гибкость и универсальность: Возможность адаптации промптов под любые цели.

6. Снижение стресса: Быстрое решение задач уменьшает уровень тревожности и улучшает организацию.

Эти преимущества делают промпт-инжиниринг инструментом, который трансформирует подход к работе и обучению.

Промпт-инжиниринг – это навык будущего, который уже сегодня помогает использовать технологии искусственного интеллекта на максимальной мощности. Правильно составленные запросы экономят время, для этого необходимо придерживаться следующих советов:

1. Демонстрируйте, а не просто объясняйте LLM: Добавляйте в свои запросы короткие примеры. Используйте инструкции, но обязательно дополняйте их примерами. Наиболее сложные команды предполагают динамическое включение нескольких примеров, которые соответствуют каждому конкретному запросу.

2. Экспериментируйте с формулировками своих запросов: со временем вы, вероятно, будете улучшать промпты — вносить дополнительные указания для нетипичных ситуаций, редактировать примеры, адаптировать контекст и т. д. Рекомендуется сохранять различные версии в процессе редактирования, чтобы при необходимости можно было легко вернуться к предыдущим вариантам, если изменения окажутся неудачными или захотите позже сравнить разные варианты.

3. Сохраняйте все важные результаты: вам будут нужны как удачные, так и неудачные примеры для тестирования. Это поможет поддерживать высокий уровень качества и исправлять ошибки. Также важно фиксировать версию промпта, которая использовалась для их создания.

4. Выберите подходящую модель для вашего запроса: Наблюдаемый общий прогресс заключается в переходе от OpenAI к множеству разработчиков, включая Anthropic, Cohere и Google. Применение нескольких моделей связано с определенными особенностями в плане затрат, скорости и возможного дублирования, однако для каждого конкретного запроса некоторые модели оказываются более эффективными, чем остальные. Как правило, команды работают с 2-3 поставщиками, хотя некоторые используют больше.

5. Контролируйте процесс использования: языковые модели не предназначены для принципа «установил и забыл». Клиенты сталкиваются со сложными ситуациями, модели претерпевают изменения, задержки могут внезапно возрасти, что в конечном итоге приводит к значительному изменению качества результата.

6. Создайте систему обратной связи: когда вы начинаете работать с технологиями машинного обучения, уделите внимание разработке механизмов обратной связи, которые можно внедрить в процесс взаимодействия с клиентами. Такие механизмы могут быть активными (например, поднятый или опущенный большой палец с комментарием) или пассивными (например, фиксация действий клиента, когда он применяет результат, сгенерированный языковой моделью или просит внести доработки). Периодически анализируйте данные из каждой категории, чтобы выявить возможности для улучшения.

Заключение

При работе с системами искусственного интеллекта решающую роль играет то, как мы формулируем наши вводные данные [3]. В отличие от обычных поисковых запросов или разговоров с человеком, здесь есть определенные аспекты, которые следует учитывать, чтобы добиться оптимальных результатов. Промпт-инжиниринг становится ключевым навыком в эпоху активного внедрения искусственного интеллекта и позволяет эффективно взаимодействовать с LLM для решения задач в различных сферах бизнеса, значительно повышая продуктивность и сокращая временные затраты.

Качество результатов, получаемых от LLM, напрямую зависит от чёткости и конкретности формулировок промптов, и требует от специалиста умения структурировать запросы. Использование LLM позволяет автоматизировать рутинные процессы в бизнесе, генерировать креативные идеи, анализировать большие данные что улучшает качество принимаемых решений [5].

В профессиональной бизнес-среде промпт-инжиниринг становится инструментом для стратегического планирования, анализа конкурентов и улучшения бизнес-процессов. Овладение специалистом навыков промпт-инжиниринга открывает новые возможности для личного и профессионального роста, делая взаимодействие с искусственным интеллектом более эффективным и результативным.

Литература

1. *Агамалиев Р.* От «Энигмы» до ChatGPT: эволюция искусственного интеллекта и российские бизнес-кейсы. Манн, Иванов и Фербер, 2024. С.20.

2. *Агравал А., Ганс Д., Голдфарб А*. Искусственный интеллект на службе бизнеса. Как машинное прогнозирование помогает принимать решения. Манн, Иванов и Фербер, 2019. 211 с.

3. *Боровская Е.В., Давыдова Н.А*. Основы искусственного интеллекта: учебное пособие для вузов. Лаборатория знаний, 2023. С. 114-116.

4. *Бутл Р*. Искусственный интеллект и экономика: Работа, богатство и благополучие в эпоху мыслящих машин. Альпина ПРО, 2023. С. 11

5. *Дейвенпорт Т.* Внедрение искусственного интеллекта в бизнес-практику: Преимущества и сложности. Интеллектуальная литература, 2019. С. 41-51.

6. *Евстафьев В.А., Тюков М.А.* Искусственный интеллект и нейросети: практика применения в рекламе: учебное пособие. Дашков и К, 2024. С. 24-32.