Международный журнал информационных технологий и энергоэффективности

Том 8 Номер 4 (30)

2023

Международный журнал информационных технологий и энергоэффективности
Т.8 №4(30) 2023 г.

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Цечоев М.Х., Шарыпова Т.Н. Киберугрозы и меры их предотвращения на предприятии // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 5–8

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

КИБЕРУГРОЗЫ И МЕРЫ ИХ ПРЕДОТВРАЩЕНИЯ НА ПРЕДПРИЯТИИ

[1]Цечоев М.Х., Шарыпова Т.Н.
Ростовский государственный экономический университет (РИНХ), Ростов-на-Дону, Россия (344000, г. Ростов-на-Дону, пер. Островского, 62), e-mail: [1]tcechoev02@inbox.ru

Статья представляет собой обзор основных видов киберугроз, которые могут стать причиной серьезных проблем для компаний и частных лиц. В статье рассматриваются такие типы киберугроз, как вредоносный код, фишинг, DDoS-атаки, вредоносное ПО. Кроме того, в статье предлагается ряд мер по защите от киберугроз, включая использование антивирусных программ, установку брандмауэров, регулярное обновление программного обеспечения и обучение сотрудников правилам безопасности в сети. Также в статье подробно рассматриваются киберугрозы, связанные с облачными хранилищами и устройствами Интернета вещей (IoT).

Ключевые слова: киберугрозы, вредоносный код, вредоносное ПО, DDoS-атаки, фишинг, меры по защите от киберугроз.

CYBER THREATS AND MEASURES TO PREVENT THEM AT THE ENTERPRISE

[1]Tsechoev M.H., Sharypova T.N.
Rostov State University of Economics (RINH), Rostov-on-Don, Russia (344000, Rostov-on-Don, lane. Ostrovsky, 62), e-mail: [1]tcechoev02@inbox.ru

The article is an overview of the main types of cyber threats that can cause serious problems for companies and individuals. The article discusses such types of cyber threats as malicious code, phishing, DDoS attacks, malware. In addition, the article suggests a number of measures to protect against cyber threats, including the use of antivirus programs, the installation of firewalls, regular software updates and training of employees in network security rules. The article also discusses in detail the cyber threats associated with cloud storage and Internet of Things (IoT) devices.

Keywords: cyber threats, malicious code, malware, DDoS attacks, phishing, measures to protect against cyber threats.

Киберпреступность представляет собой серьезную угрозу для организаций и отдельных лиц в 21 веке. Киберугрозы — это злоумышленные действия, которые используют компьютерные системы и сети, часто применяя вредоносное или другое вредоносное программное обеспечение для получения несанкционированного доступа или контроля над системой, что приводит к повреждению или нарушению работы данных, служб или сетей. За последние пять лет количество кибератак увеличилось более чем на 200%. В 2022 году из-за утечки данных было раскрыто более 4,1 миллиарда записей[1].

В кибератаках используются различные методы и приемы, в том числе вредоносный код, фишинг, вредоносное ПО, программы-вымогатели, социальная инженерия и атаки типа «отказ в обслуживании» (DoS) [2]:

1. Вредоносный код — это код, предназначенный для выполнения вредоносных действий, таких как кража конфиденциальной информации или отключение компьютерных систем.

2. Фишинг — это форма социальной инженерии, при которой злоумышленники рассылают электронные письма, пытаясь обманом заставить пользователей раскрыть конфиденциальную информацию.

3. Вредоносное ПО — это тип вредоносного программного обеспечения, предназначенного для проникновения в компьютерные системы и их повреждения.

4. Программа-вымогатель — это тип вредоносного ПО, которое шифрует файлы и требует оплаты в обмен на их разблокировку. Социальная инженерия — это использование обмана и манипуляций для получения конфиденциальной информации.

5. DoS-атака — это атака, при которой компьютер жертвы переполняется трафиком, лишая его возможности отвечать на законные запросы.

По мере того, как технологии становятся все более неотъемлемой частью ведения любого бизнеса, компании все чаще сталкиваются с рисками, связанными с киберугрозами. Киберпреступность вызывает все большую озабоченность у предприятий любого размера и может привести к разрушительным потерям денег, данных, лояльности клиентов и репутации. Компании должны предпринимать упреждающие действия, чтобы защитить свои системы и данные от злоумышленников.

Организациям необходимо начать с внедрения надежных мер безопасности, таких как надежные брандмауэры, антивирусное программное обеспечение и шифрование данных. Они также должны убедиться, что их сотрудники обучены передовым методам кибербезопасности, таким как избегание подозрительных электронных писем и веб-сайтов, а также понимание того, как выявлять потенциальные угрозы. Компании также должны использовать двухфакторную аутентификацию и регулярно обновлять свои исправления безопасности, чтобы обеспечить актуальность своих систем [5].

В дополнение к этим основным мерам организациям следует проводить регулярные аудиты безопасности и сканирование для обнаружения любых потенциальных уязвимостей. Им также следует рассмотреть возможность использования системы мониторинга и реагирования для постоянного мониторинга своих систем и быстрого реагирования на любые потенциальные угрозы. Компании также должны создать политику кибербезопасности, подробно описав шаги, которые они предпримут для защиты своих систем и данных, а также последствия любых нарушений.

В конечном счете предотвращение киберугроз требует сочетания упреждающих мер, обучения сотрудников и систем реагирования. Компании должны проявлять бдительность в своих усилиях по защите своих систем, данных и информации о клиентах от злоумышленников.

Рассмотрим подробнее киберугрозы, связанные с облачными хранилищами и устройствами Интернета вещей (IoT), которые представляют собой все более сложную среду кибербезопасности из-за большого количества потенциальных точек входа. По мере роста использования облачных хранилищ и устройств Интернета вещей в компаниях увеличивается вероятность того, что злоумышленники получат доступ к данным и устройствам [4].

Одной из основных киберугроз, связанных с облачными хранилищами и устройствами IoT, является утечка данных, которая происходит, когда неавторизованные пользователи

получают доступ к конфиденциальным данным, хранящимся в облаке. Утечка данных может быть вызвана различными злоумышленниками, включая хакеров, мошеннических инсайдеров, вредоносное ПО и незащищённые API. Доступ к данным в облаке через незащищённую конечную точку также может привести к раскрытию данных для злоумышленника.

Ещё одна проблема безопасности — использование ненадёжных паролей пользователями, которые получают доступ к облачным хранилищам и устройствам IoT. Слабый пароль можно легко угадать или подобрать методом грубой силы, что позволяет злоумышленникам получить доступ к данным. Кроме того, пользователи, которые непреднамеренно или злонамеренно повторно используют пароли для нескольких учетных записей, могут непреднамеренно предоставить злоумышленникам доступ к нескольким ресурсам.

Вредоносное ПО — это еще один тип киберугроз, которые можно использовать для нападения на облачные хранилища и устройства IoT[3]. Вредоносное ПО может заражать машины, предоставляя злоумышленникам доступ к данным, хранящимся на устройстве, или возможность удаленного управления устройством. Вредоносное ПО также может использоваться для создания бэкдоров в системе, позволяя злоумышленникам вернуться позже и получить доступ к данным.

Наконец, отсутствие исправлений может представлять значительный риск для облачных хранилищ и устройств IoT. По мере выявления новых уязвимостей к устройствам необходимо применять исправления, чтобы обеспечить безопасность системы. Отсутствие исправления для устройства может привести к нарушению безопасности, поскольку злоумышленники могут воспользоваться неисправленной уязвимостью.

Из проведенного исследования видно, что киберугрозы являются реальной проблемой и могут иметь серьезные последствия для отдельных лиц и предприятий. Для защиты от этих угроз важно использовать лучшие практики, такие как внедрение надежных мер аутентификации, регулярное обновление программного обеспечения, использование безопасных сетей и обучение персонала осведомленности о кибербезопасности. Кроме того, организации должны быть в курсе последних угроз и использовать соответствующие контрмеры.

Список литературы

1. Пустовая Е.И., Шарыпова Т.Н. Кибербезопасность в наше время. Инновация. Наука. Образования. 2020. № 24.
2. Лыженкова А.Н., Шарыпова Т.Н. Киберпреступления: понятие, классификация, юридическая ответственность, основные правила компьютерной безопасности.Инновация. Наука. Образования. 2021. № 26.
3. Евкина И.Е., Шарыпова Т.Н. Киберпреступность как угроза информационной безопасности. Инновации. Наука. Образование. 2021. № 36.
4. Решетова Виктория Александровна, Шарыпова Татьяна Николаевна. Вопросы противодействия киберпреступности. Инновации. Наука. Образование. 2022. №56. С. 60-64.
5. Шарыпова Т.Н., Селиванов С.А. Анализ угроз информационной безопасности и способы ее защиты. Наукосфера. 2021. № 1-1. С. 242-245.

References

1. Pustovaya E.I., Sharypova T.N. Cybersecurity in our time. Innovation. The science. Education. 2020. № 24.
2. Lyzhenkova A.N., Sharypova T.N. Cybercrime: concept, classification, legal responsibility, basic rules of computer security.Innovation. The science. Education. 2021. № 26.
3. Ivkina I.E., Sharypova T.N. Cybercrime as a threat to information security. Innovation. The science. Education. 2021. № 36.
4. Reshetova Victoria Alexandrovna, Sharypova Tatiana Nikolaevna.Issues of countering cybercrime. Innovation. The science. Education. 2022. No. 56. pp. 60-64.
5. Sharypova T.N., Selivanov S.A. ANALYSIS OF THREATS TO INFORMATION SECURITY AND WAYS TO PROTECT IT. The sciencosphere. 2021. No. 1-1. pp. 242-245.

Сычев Д.И. Методы машинного и глубокого обучения для систем обнаружения вторжений: обзор и анализ // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 9–17

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 62

МЕТОДЫ МАШИННОГО И ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ: ОБЗОР И АНАЛИЗ

Сычев Д.И.
Санкт-Петербургский государственный университет телекоммуникаций имени профессора М.А. Бонч-Бруевича, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков, 22, к. 1), e-mail: s.denis_2001@mail.ru

В современном мире, с развитием информационных технологий, исследования в области кибербезопасности играют все большую роль. Одной из важных систем в кибербезопасности, является система обнаружения вторжений (англ. *Intrusion Detection Systems - IDS*). IDS мониторит состояние программного и аппаратного обеспечения, работающего в сети. Несмотря на прошедшие десятки лет разработки, существующие IDS по прежнему сталкиваются с трудностями в точности определения вторжения, обнаружении новых атак и ложных срабатываний. Для решения вышеописанных проблем ведутся исследования в области разработки IDS, использующую методы машинного обучения. Машинное обучение может автоматически определять существенные различия между общими и аномальными данными с высокой точностью. Системы обнаружения вторжений можно разделить на 2 типа: на основе сигнатур и на основе аномалий. IDS на основе сигнатур опираются на предопределенные шаблоны или сигнатуры известных атак, в то время как IDS на основе аномалий выявляют аномальное поведение, отклоняющееся от нормальной сетевой активности.
Методы машинного обучения (ML) и глубокого обучения (DL) широко используются в IDS для повышения точности и эффективности обнаружения вторжений. В этом тексте мы рассмотрим таксономию методов ML и DL, используемых для IDS.

Ключевые слова: Системы обнаружения вторжений, Машинное обучение, Глубокое обучение, Сетевая безопасность.

MACHINE AND DEEP LEARNING METHODS FOR INTRUSION DETECTION SYSTEMS: OVERVIEW AND ANALYSIS

Sychev D.I.
St. Petersburg State University of Telecommunications named after Professor M.A. Bonch-Bruevich, St. Petersburg, Russia (193232, St. Petersburg, Bolshevikov Ave., 22, room 1), e-mail: s.denis_2001@mail.ru

In the modern world, with the development of information technology, research in the field of cybersecurity is playing an increasingly important role. One of the important systems in cybersecurity is the intrusion Detection System (English Intrusion Detection Systems - IDS). IDS monitors the status of the software and hardware running on the network. Despite the past decades of development, existing IDS still face difficulties in accurately detecting intrusion, detecting new attacks and false positives. To solve the problems described above, research is underway in the field of IDS development using machine learning methods. Machine learning can automatically detect significant differences between general and anomalous data with high accuracy. Intrusion detection systems can be divided into 2 types: signature-based and anomaly-based. Signature-based IDS rely on predefined patterns or

signatures of known attacks, while anomaly-based IDS detect abnormal behavior that deviates from normal network activity.

Machine learning (ML) and deep learning (DL) techniques are widely used in IDS to improve the accuracy and efficiency of intrusion detection. In this text, we will look at the taxonomy of ML and DL methods used for IDS.

Keywords: Intrusion detection systems, Machine learning, Deep learning, Network security.

Введение

Развитие сетевых устройств оказывает все большее влияние на современную жизнь, что делает кибербезопасность важной областью для исследований[1,2]. Основные методы борьбы с киберпреступностью в основном составляют антивирусное программное обеспечение, брандмауэры и системы обнаружения вторжений (IDS). Эти методы защищают устройства в сети от внутренних и внешних атак. Среди них IDS — это тип системы обнаружения, которая играет ключевую роль в обеспечении защиты и отслеживания состояния программного и аппаратного обеспечения, работающего в сети.

Первая система обнаружения вторжений была предложена в 1980 году [1]. С тех пор появилось много различных IDS продуктов. Тем не менее, многие IDS по-прежнему страдают от высокого уровня ложных срабатываний, генерируя множество предупреждений для мало опасных ситуаций, что увеличивает нагрузку на систему аналитики и может привести к тому, что серьезные вредоносные атаки будут проигнорированы. Еще одна проблема существующих IDS заключается в том, что они уязвимы к появляющимся новым типам атак. Поскольку сетевые системы продолжают развиваться и изменяться, злоумышленники регулярно разрабатывают новые варианты атак. Таким образом, в современном мире существует необходимость в IDS, способных обнаруживать ранее неизвестные атаки.

Чтобы решить вышеуказанные проблемы, начали разрабатываться IDS с использованием методов машинного обучения. Машинное обучение — это метод искусственного интеллекта, который может автоматически извлекать полезную информацию из больших наборов данных [2]. При наличии большого датасета, IDS на основе машинного обучения показывают могут показывать хороший результат в обнаружении проникновений, а за счет генерализации, справиться с некоторыми вариантами новых атак. Кроме того, IDS на основе машинного обучения не имеют сильной зависимости от предметной области, поэтому их легко спроектировать.

Ниже, представлена классификация методов машинного обучения и глубокого обучения для IDS. Выделены различные подходы на основе алгоритмов, источников данных и архитектур. Таким образом, предоставлен четкий и структурированный обзор последних достижений в области обнаружения вторжений с использованием машинного и глубокого обучения. Эта таксономия будет полезна как для исследователей, так и для практиков, которые стремятся лучше понять сильные и слабые стороны различных подходов и выбрать наиболее подходящий метод для конкретного использования.

1. Обзор систем обнаружения вторжений

Системы обнаружения вторжений могут быть разделены на две основные категории: сетевые IDS (NIDS) и хост-ориентированные IDS (HIDS). NIDS анализируют сетевой трафик, чтобы обнаруживать аномалии и атаки, в то время как HIDS сосредоточены на мониторинге отдельных хостов, таких как серверы или рабочие станции[3].

Традиционные подходы к обнаружению вторжений включают использование сигнатурных и правиловых методов. Сигнатурные методы заключаются в сравнении сетевого трафика с известными шаблонами атак, называемыми сигнатурами. Если сетевой трафик соответствует определенной сигнатуре, IDS генерирует предупреждение о возможной атаке. Правиловые методы основаны на анализе сетевого трафика или системных событий с использованием заранее определенных правил, которые указывают на подозрительную активность.

Традиционные методы обнаружения вторжений имеют несколько ограничений:

- Ложные срабатывания: Сигнатурные и правиловые методы склонны к ложным срабатываниям, когда допустимое поведение или сетевой трафик ошибочно определяются как атака[3,4]. Это может привести к перегрузке системы предупреждений и ухудшению эффективности работы специалистов по безопасности.
- Обнаружение атак "нулевого дня": Традиционные IDS слабо справляются с обнаружением атак "нулевого дня", которые представляют собой новые или ранее неизвестные угрозы, не имеющие сигнатур или явных признаков. Это создает слепые пятна в обнаружении и оставляет системы уязвимыми перед новыми атаками.
- Ресурсоемкость: Поддержка актуальной базы сигнатур и правил для традиционных IDS требует постоянного обновления и значительных ресурсов на поддержание эффективности системы. Кроме того, обработка больших объемов сетевого трафика может вызвать задержки и замедления в работе IDS.
- Отсутствие адаптивности: Традиционные методы обнаружения вторжений статичны и не способны адаптироваться к изменяющимся сценариям угроз или условиям сетевого трафика.

Для преодоления ограничений традиционных подходов к обнаружению вторжений, активно применяются методы машинного обучения и глубокого обучения. Эти методы способны автоматически обучаться на основе данных, выявлять закономерности и адаптироваться к новым сценариям угроз. Таким образом, ML и DL методы могут снизить количество ложных срабатываний, обеспечить обнаружение атак "нулевого дня" и улучшить адаптивность системы к изменяющимся условиям[5].

Машинное обучение и глубокое обучение в IDS применяются для решения различных задач, таких как классификация трафика, аномалий и атак, а также для анализа поведения сетевых узлов

2. Методы машинного обучения для IDS

Среди наиболее распространенных подходов к машинному обучению в системах обнаружения вторжений можно выделить обучение с учителем. В данном методе, модель обучается на основе размеченных заранее данных, содержащих примеры нормального поведения и возможных атак[6]. Целью обучения является настройка модели таким образом, чтобы она смогла классифицировать наблюдаемое поведение в системе как нормальное или аномальное. К популярным методам обучения с учителем, которые используются для IDS, относятся:

- **Метод логистической регрессии**: Это статистический метод для анализа набора данных, в котором одна или несколько независимых переменных используются для предсказания вероятности принадлежности наблюдения к одному из двух классов (например, нормальный или аномальный). Логистическая регрессия является простым и интерпретируемым подходом, однако для сложных и нелинейных зависимостей, она может быть менее эффективной.
- **Метод опорных векторов** (SVM): SVM – это мощный алгоритм классификации, который стремится найти оптимальную разделяющую гиперплоскость между двумя классами. SVM хорошо справляется с задачами, которые имеют большое количество признаков, и сложными зависимостями, но может быть ресурсоемким при больших объемах данных.
- **Дерево решений и ансамблевое обучение**: Дерево решений – это иерархические структуры, которые последовательно разделяют данные на основе определенных критериев. Ансамблевые методы, такие как метод случайного леса (Random Forest) и градиентный бустинг (Gradient Boosting), объединяют множество деревьев решений для улучшения производительности и устойчивости к переобучению. Деревья решений и ансамблевые методы характеризуются высокой точностью и интерпретируемостью, но могут столкнуться с проблемами масштабируемости при обработке больших данных.

Обучение без учителя используется в случаях, когда размеченные данные недоступны или их очень мало. Эти методы пытаются выявить аномалии или кластеры, опираясь на структуру и распределение данных. Некоторые популярные методы обучения без учителя для IDS включают:

- **K-средних**: Это итеративный алгоритм кластеризации, который разделяет данные на K кластеров на основе расстояния между точками данных. K-средних может использоваться для выявления групп аномального поведения или атак, но подвержен влиянию выбросов и чувствителен к исходному выбору центроидов кластеров.
- **DBSCAN** (Density-Based Spatial Clustering of Applications with Noise) – это алгоритм кластеризации, основанный на плотности, который группирует точки данных на основе их плотности и расстояния. DBSCAN хорошо справляется с аномалиями и может обнаруживать кластеры произвольной формы, но требует настройки гиперпараметров для определения плотности и расстояния.
- **Автоэнкодеры** – это нейронные сети, которые сначала сжимают данные в низкоразмерное представление (кодирование), а затем восстанавливают исходные данные из этого представления (декодирование). В контексте IDS, автоэнкодеры могут обучаться на нормализованных данных и использоваться для обнаружения аномалий, сравнивая восстановленные данные с исходными. Если разница между восстановленными и исходными данными велика, это может указывать на аномальное поведение или атаку.

3. Методы глубокого обучения для IDS

Глубокое обучение (Deep Learning, DL) – это подраздел машинного обучения, который использует нейронные сети с большим количеством слоев для обработки и анализа данных. Глубокое обучение может автоматически извлекать сложные признаки из сырых данных, что делает его особенно полезным для применения в системах обнаружения вторжений[6,7]. Одним из основных методов глубокого обучения, который используется в IDS является способ обучения Сверточной нейронной сети (Convolutional Neural Networks, CNN). CNN - это тип глубоких нейронных сетей, разработанный специально для обработки изображений и временных рядов. В контексте IDS, CNN могут использоваться для анализа сетевого трафика и системных журналов, автоматически извлекая признаки, связанные с атаками. CNN состоят из сверточных, пулинговых (субдискретизирующих) и полносвязных слоев, которые обрабатывают и объединяют признаки на разных уровнях абстракции[7]. Сверточные нейронные сети зарекомендовали себя как отличный инструмент для различных приложений и сетевых инструментов, однако, при использовании их с системами обнаружения вторжений, нужно учитывать ряд возможных подводных камней, которые могут появится при разработке:

- **Высокая вычислительная сложность**: CNN обычно состоят из нескольких уровней с многочисленными параметрами, что делает их обучение дорогостоящими в вычислительном отношении. Это может быть серьезным ограничением, особенно в при работе в реальном времени, где важны малая задержка и эффективная обработка.
- **Потребность в больших наборах размеченных данных**: Чтобы достичь высокой производительности, CNN требуют значительных объемов размеченных данных. Получение большого набора размеченных данных для обнаружения вторжений может быть затруднено из-за динамического характера киберугроз и сложности получения достоверных меток для сетевого трафика.
- **Чувствительность к входному представлению функций**: CNN предназначены для работы с сеткообразными структурами данных (например, изображениями). Применение их к IDS может потребовать преобразования данных сетевого трафика в подходящее представление, которое не всегда может быть простым или оптимальным.
- **Ограниченная интерпретируемость**: CNN часто считают моделями «черного ящика» из-за их сложной структуры и отсутствия интерпретируемости. Может быть трудно понять, почему CNN классифицировала конкретное сетевое событие как злонамеренное или неопасное, что может привести к недоверию со стороны экспертов по безопасности.

Также, среди популярных методов глубокого обучения, стоит рассмоетрть рекуррентные нейронные сети и автоэнкодер. Рекуррентные нейронные сети (Recurrent Neural Networks, RNN) – это класс глубоких нейронных сетей, специально разработанный для работы с последовательными данными, такими как временные ряды или текст. RNN обладают внутренней памятью и могут учитывать контекст и порядок событий при анализе данных. В IDS, RNN могут использоваться для обнаружения атак, основанных на аномальных последовательностях действий или сетевых запросов. Одним из распространенных вариантов RNN являются сети долгой краткосрочные памяти (LSTM) и еправляемый рекуррентный блок

(GRU), которые способны эффективно обрабатывать долгосрочные зависимости между событиями.

Как уже упоминалось в предыдущих разделах, автоэнкодеры являются нейронными сетями, которые сначала кодируют данные в компактное представление, а затем восстанавливают их из этого представления. Вариационные автоэнкодеры (VAE) – это расширение автоэнкодеров, которое вводит стохастический слой в кодирование, позволяя модели генерировать новые данные, похожие на обучающую выборку. И автоэнкодеры, и VAE могут использоваться в IDS для обнаружения аномалий и атак, основанныхна разнице между восстановленными данными и исходными данными, а также для создания репрезентативных эмбеддингов, которые могут использоваться в других моделях машинного обучения.

Методы глубокого обучения предлагают множество инновационных подходов для систем обнаружения вторжений. Они позволяют автоматически извлекать сложные признаки из данных, обеспечивая высокую точность и эффективность в обнаружении атак и аномалий. Однако эти методы требуют больших вычислительных ресурсов и обучающих данных для достижения оптимальной производительности. Важно выбирать подходящие методы глубокого обучения в зависимости от конкретной задачи IDS, доступных данных и вычислительных возможностей.

4. Проблемы и вызовы в применении ML и DL для IDS

Хотя машинное обучение и глубокое обучение предлагают множество преимуществ для систем обнаружения вторжений, их применение также связано с определенными проблемами и вызовами. В этом разделе мы рассмотрим некоторые общие ключевые аспекты, которые необходимо учитывать при использовании ML и DL в IDS.

Для эффективного обучения большинства моделей машинного и глубокого обучения требуются большие объемы размеченных данных. Однако в контексте IDS, сбор и разметка данных о вторжениях может быть трудоемким и дорогостоящим процессом. Это может привести к использованию небольших или несбалансированных обучающих наборов данных, что ухудшает качество обучения моделей и их способность обнаруживать атаки[8]. Так же, в современном мире злоумышленники постоянно разрабатывают новые и изменяющиеся стратегии атак, чтобы обойти системы обнаружения вторжений. Это требует от IDS с использованием ML и DL умения быстро адаптироваться к новым видам атак и обеспечивать надежное обнаружение. Однако обновление и повторное обучение моделей может быть ресурсоемким процессом, особенно в случае сложных архитектур глубокого обучения.

Модели глубокого обучения, требуют больших вычислительных ресурсов для обучения и инференции. Такие ресурсы, как графические процессоры (GPU) и специализированные аппаратные ускорители, могут быть дорогостоящими и недоступными для некоторых организаций. В результате, выбор подходящих моделей и оптимизация вычислительных процессов становятся критически важными для успешного использования ML и DL в IDS. Модели машинного обучения и, в особенности, глубокого обучения часто называют "черными ящиками" из-за их сложности и отсутствия интерпретируемости. Это может создать трудности для понимания и объяснения причин, по которым модель считает определенное поведение аномальным или атакующим. В результате, это может привести к ошибкам и недоверию со стороны пользователей и экспертов в области безопасности.

Использование ML и DL в IDS может потребовать сбора и обработки большого количества сетевых данных и журналов, которые могут содержать конфиденциальную и чувствительную информацию. Защита этих данных от утечек и злоупотреблений является важным аспектом применения ML и DL в системах обнаружения вторжений. Это может потребовать разработки дополнительных методов защиты данных и обеспечения соблюдения принципов конфиденциальности и соответствия законодательству.

Применение методов машинного и глубокого обучения для IDS представляет собой мощный инструмент в борьбе с киберугрозами, однако его успешная реализация связана с рядом проблем и вызовов. Здравый учет этих аспектов и разработка стратегий является важным аспектом, на который кампаниям, разрабатывающие IDS, стоит уделить внимание.

Вывод

В этой статье мы рассмотрели основы систем обнаружения вторжений (IDS) и их развитие с течением времени. Мы подробно обсудили применение методов машинного обучения и глубокого обучения в контексте IDS, а также рассмотрели некоторые из вызовов и проблем, связанных с их использованием. Машинное обучение и глубокое обучение предлагают значительные преимущества для повышения эффективности и точности систем обнаружения вторжений, позволяя адаптироваться к изменяющимся атакам и автоматически извлекать сложные признаки из данных. Однако успешное внедрение этих технологий требует учета ряда проблем и вызовов, таких как недостаток размеченных данных, вычислительные ресурсы, уязвимость к противодействию и манипуляциям, а также проблемы конфиденциальности и безопасности данных.

Интеграция машинного и глубокого обучения в системы обнаружения вторжений представляет собой значительный шаг вперед в борьбе с киберугрозами. Однако для успешного применения этих подходов необходимо тщательно учесть ряд проблем и вызовов, а также разработать адекватные стратегии и решения для преодоления потенциальных препятствий на пути к обеспечению надежной и эффективной кибербезопасности. Сотрудничество между исследователями, специалистами в области безопасности и разработчиками программного обеспечения является ключевым фактором для достижения этих целей и создания новых, инновационных решений для борьбы с киберпреступностью. Важно продолжать исследования и разработки, направленные на повышение эффективности IDS и устойчивости к различным видам атак, чтобы обеспечить безопасность и защиту киберпространства в будущем.

Список литературы

1. Гельфанд А. М. и др. Области применения аналитики больших данных в критических информационных инфраструктурах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 438-440.
2. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.

3. Ковалев И. А., Косов Н. А. Состязательные атаки в нейронных сетях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 490-492.
4. Тимофеев Р. С., Косов Н. А. Сравнение методов обучения сверточных нейронных сетей //Актуальные научные исследования в современном мире. – 2021. – №. 6-1. – С. 97-102.
5. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике //Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
6. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.
7. Цветков А. Ю., Рузманов Е. Ю. Рассмотрение тестирования на проникновение в задачах защиты информации //ББК 3 П27. – 2021. – С. 55.
8. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2021. – №. 2. – С. 31-35.
9. Гельфанд А. М., Гвоздев Ю. В., Штеренберг С. И. Исследования недостатков языков высокоуровнего программирования для осуществления скрытого вложения в исполнимые файлы //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2015. – С. 295-297.
10. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с.
11. Зимин А. Е., Косов Н. А. Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). – 2017. – С. 343-348.

References

1. Gelfand A. M. et al. Applications of big data analytics in critical information infrastructures // Actual problems of infotelecommunications in science and education (APINO 2022). - 2022. - . pp. 438-440.
2. Budarny G. S. et al. Variety of security violations and typical attacks on the operating system // Actual problems of infotelecommunications in science and education (APINO 2022). - 2022. - pp. 406-411.
3. Kovalev I. A., Kosov N. A. Competitive attacks in neural networks // Actual problems of infotelecommunications in science and education (APINO 2021). - 2021. - pp. 490-492.
4. Timofeev R. S., Kosov N. A. Comparison of training methods for convolutional neural networks // Actual scientific research in the modern world. – 2021. – no. 6-1. - pp. 97-102.
5. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. - 2021. - pp. 33-37.

6. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise // Actual problems of infotelecommunications in science and education (APINO 2021). - 2021. - pp. 653-657.
7. Tsvetkov A. Yu., Ruzmanov E. Yu. Consideration of penetration testing for information protection //BBK 3 P27. - 2021. - pp. 55.
8. Shemyakin S. N. et al. Using graph theory to model the security of cloud systems // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and technical sciences. – 2021. – no. 2. - pp. 31-35.
9. Gelfand A. M., Gvozdev Yu. V., Shterenberg S. I. Investigation of the shortcomings of high-level programming languages for the implementation of hidden attachments to executable files // Actual problems of infotelecommunications in science and education. - 2015. - S. 295-297.
10. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A. V. Krasov, A. Yu. Tsvetkov. Volume Part 1. - St. Petersburg: St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich, 2015. – p.63.
11. Zimin A. E., Kosov N. A. Ensuring information security in the process of creating and using computer programs // Actual problems of infotelecommunications in science and education (APINO 2017). - 2017. - pp. 343-348.

Галимянов А.Ф., Галимянов Р.А. Дробные дифференциальные уравнения для прогнозирования в педагогических системах // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 18–21

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.032.26

ДРОБНЫЕ ДИФФЕРЕНЦИАЛЬНЫЕ УРАВНЕНИЯ ДЛЯ ПРОГНОЗИРОВАНИЯ В ПЕДАГОГИЧЕСКИХ СИСТЕМАХ

[1]Галимянов А.Ф., **[2]Галимянов Р.А.**
ФГБОУ ВО «Казанский (Приволжский) федеральный университет», Казань, Россия (420008, Республика Татарстан, г Казань, ул Кремлевская, д. 18, к. 1) e-mail: anis_59@mail.ru;
[2]ФГБОУ ВО «Казанский государственный энергетический университет", Казань, Россия (420066 Республика Татарстан, г.Казань ул.Красносельская, 51, корп. Д), e-mail: grinat@icloud.com

Для моделирования педагогических процессов и прогнозирования, а также влияния отдельных параметров на педагогический результат предлагается использовать искусственные нейронные сети. В этих целях предлагается использовать нейронную сеть с обратным шагом. Для моделирования этой сети предложено дробно-дифференциальное уравнение с дробным производным Капуто.

Ключевые слова: Нейронные сети, архитектура с обратной связью, дробно-дифференциальные уравнения.

FRACTIONAL DIFFERENTIAL EQUATIONS FOR FORECASTING IN PEDAGOGICAL SYSTEMS

[1]Galimyanov A.F. , [2]Galimyanov R.A.
Kazan (Volga Region) Federal University, Kazan, Russia,
(420008, Republic of Tatarstan, Kazan, Kremlevskaya str., 18, k. 1) e-mail: anis_59@mail. ru;
[2]Kazan State Power Engineering University, Kazan, Russia
(420066 Republic of Tatarstan, Kazan, Krasnoselskaya str., 51, building D), e-mail: grinat@icloud.com

Artificial neural networks are proposed to be used for modeling pedagogical processes and forecasting, as well as the influence of individual parameters on the pedagogical result. For this purpose, it is proposed to use a neural network with a reverse step. To model this network, a fractional differential equation with fractional Caputo derivatives is proposed.

Keywords: Neural networks, feedback architecture, fractional differential equations.

Прогнозирование в педагогических системах, исследование и предсказание влияния самых различных параметров на результаты педагогического процесса является весьма важным условием для правильной организации учебного и воспитательного процесса. В настоящее время принятие всесторонне обоснованных дидактических решений требует современных методов анализа и применения новых прогностических моделей. Учитывая, что в педагогический процесс влияют самые разные факторы, отобрать из них наиболее важные и изменять их в сторону оптимизации без продуктивной переработки потоков данных в

упорядоченную систему не применяя современных методов обработки невозможно. В настоящее время самым продуктивным методом обработки данных являются компьютерные интеллектуальные системы, основанные на искусственных нейронных сетях.

Использование нейронных сетей в самых разных компьютерных приложениях, в том числе и для прогнозирования, берет свое начало от попытки воспроизвести работу биологических нейронных систем, их способностей обучаться и исправлятоь свои ошибки. Но здесь следует иметь в виду, что слово “обучаться” в этом случае употребляется не в педагогическом смысле, а в смысе “тренировки” искусственной системы, когда изменением его параметров происходит процесс улучшения ее функциональных возможностей.

Биологический нейрон состоит из тела клетки (cell body), или еще называют его сома (soma), а также двух типов внешних древоподобных отростков - аксона (axon) и дендритов (dendrites). Само же тело клетки включает в себя ядро (nucleus), где содержится информация о наследственных свойствах, и плазму. Плазма обладает молекулярными средствами для производства материалов, необходимых для нервной клетки. Получает же сигналы нейрон от других нейронов через приемники – дендриты, а далее передает сигналы, обработанные или сгенерированные им самим по аксону, в конце которого имеются волокна (strands). На окончаниях этих волокон находятся синапсы (synapses). Через них данный импульс (сигнал) достигает других нейронов, которые вследствие этого тоже могут возбуждаться. Но рассматриваемый нейрон возбуждается только тогда, когда суммарный уровень всех сигналов (импульсов), которые в него приходят, превышает критический уровень, который называется порог активации. По другому говоря, каждому входу нейрона сопоставляются некоторые численные коэффициенты, называемые весами. Они могут принимать как положительные, так и отрицательные значения. Когда они положительны, синапс оказывает возбуждающее, когда отрицательны, замедляющее, то есть тормозящее действие, или действие возбуждающего синапса моделируется положительным значением веса, а действие тормозящего синапса – отрицательным значением.

Концепция искусственных нейронных сетей состоит в том, что нейроны моделируются простви автоматами, а вся функциональность определяется связями между нейронами. У искусственного нейрона также имеется входная группа (снапсы), а также аксон (выходная связь). Выходной сигнал посылается другим элементам по взвешенным связям.

Отличие любых нейронных сетей состоит в том, что они содержат большое количество нейронов и поэтому любая нейронная сеть является весьма высокоустойчивой к помехам, поэтому отдельные сбои, а также погрешности не оказывают существенного влияния на общие результаты функционирования, то есть на результаты работы. Поэтомму они практически незаменимы для обработки параметров педагогического процесса и для прогнозирования.

Очень большое значение имеет так называемая архитектура связей нейронных сетей. По ним нейронные сети разделяются на два класса: сети прямого распространения, где связи не имеют петель возврата, и сети обратного распространения, ил рекуррентные сети, которые имеют обратные связи между нейронами.

В последнее время нелинейные системы дробного порядка начали изучаться не только благодаря успешному их применению при моделировании физических явлений, таких как хаос, колебания, импульсы, диффузи, но и также благодаря их успешному и все более широкому примениению ихв самых различных областях, напрмер, химия, биология,

электроника и.т.д. Мы предлагаем применять данные системы для исследования и моделирования педагогических процессов. Эти процессы мы можем рассматривать как хаотические нелинейные системы. Они являются очень сложными из-за нерегулярного и непредсказуемого поведения. Их примечательной особенностью является то, что они являются очень чувствительными к начальным условиям. В таких системах также возможны неожиданные колебания, которые могут даже разрушить стабильность системы. Поэтому возникает необходимость их эффективного подавления. Поэтому были разработаны разные методы стабилизации нелинейных хаотических систем, в которых сосредоточено управление хаосом дробного порядка [1].

Технология управления нейронной сетью представляет собой интеллектуальный метод управления нелинейными ситстемами с неопределенностями. Идея метода заключается в аппроксимации неизвестных нелинейных функций с использованием нейронных сетей с радиальными базисными функциями (RBFNNS), которые представляют собой тип нейронной структуры, сформированной путем вычисления некоторых векторов регулируемых параметров и некоторых конкретных непрерывных функций. Данный метод является популярным, так как он облегчает управление нелинейными системами, в которых данные неточны или являются слишком сложными для математического моделирования. Поэтому он обеспечивает доступный способ для проектов управления и в значистельной степени применим в области разработки систем управления.

Метод обратного шага является эффективным при обработке неопределенностей нелинейных систем целого порядка. Но у него имеются недостатки, в том числе и неустранимые, которые отмечены в [1]. По аналогии с этой работой, в настоящей статье предлагается применить данный подход для педагогических систем.

Для полноты введем определения [3]

Определение 1. Пусть $0 < \alpha < 1$. Для заданной функции $f: [0, \infty] \to R$ ее интеграл порядка α (Римана-Лиувилля) определяется следующим образом:

$$ {}_0I_x^\alpha f(x) = \frac{1}{\Gamma(\alpha)} \int_0^x \frac{f(t)}{(x-t)^{1-\alpha}} dt $$

здесь $\Gamma(\alpha)$ – гамма-функция Эйлера.

Определение 2. Пусть $\alpha \geq 0$. Для заданной функции $f: [0, \infty] \to R$ ее производная Капуто порядка α определяется следующим образом:

$$ {}_0^C D_x^\alpha f(x) = \frac{1}{\Gamma(n-\alpha)} \int_0^x \frac{f^{(n)}(t)}{(x-t)^{\alpha+1-n}} dt, \alpha \geq 0, x > 0, \alpha \in [n-1, n), n = 1,2, \dots $$

По аналогии с [1] введем уравнение моделирования педагогической системы следующим образом:

$$ {}_0^C D_t^\alpha x(t) = -x(t) + x^2(t) + u(t) $$

здесь $0 < \alpha < 1, x(t)$ – переменная состояния, $u(t)$ – входная переменная.

Можно доказать, что если выходной сигнал управления сформулирован при помощи данного уравнения, законы адаптации разработаны по [1], ошибка отслеживания должна стремиться к достаточно малой окрестностит точки равновесия.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта "Цифровая модель формирования индивидуальной траектории профессионального развития

учителя на основе больших данных и нейросетей (на примере Республики Татарстан)", № 19-29-14082

Список литературы

1. Xue G, Lin F and Qin B (2020) Adaptive Neural Network Control of Chaotic Fractional-Order Permanent Magnet Synchronous Motors Using Backstepping Technique. Front. Phys. 8:106. doi: 10.3389/fphy.2020.00106
2. Galfmyanov A.F., Vorontsova V.L., Gorskaya T.Y., Approximate methods for the equations with fractional differential operator//Global Journal of Pure and Applied Mathematics. - 2015. - Vol.11, Is.6. - pp.5133-5144.
3. Самко С.Г., Kилбас А.А., Маричев О.Н., Интегралы и производные дробного порядка и некоторые их приложения. - Минск: Наука и техника, 1987. - 688с.
4. Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A.N., Kaiser L., Polosukhin I. (2017). Attention Is All You Need. NIPS.
5. Chen, Tian Qi and Rubanova, Yulia and Bettencourt, Jesse and Duvenaud, David K (2018) Neural Ordinary Differential Equations. Advances in Neural Information Processing Systems 31, 6571—6583 NIPS2018

References

1. Ua, Link F and In B (2020) Adaptive Neural Network Control of Chaotic Fractional-Order Permanent Magnet Synchronous Motors Using Backstepping Technique. Front. Phys. 8:106. doi: 10.3389/fphy.2020.00106
2. Galfmyanov A.F., Vorontsova V.L., Gorskaya T.Y., Approximate methods for the equations with fractional differential operator//Global Journal of Pure and Applied Mathematics. - 2015. - Vol.11, Is.6. - pp.5133-5144.
3. Caro S.G., Lglbas A.A., Marichev O.N., Integrals and derivatives of fractional order and some of their applications. - - Minsk: Science and Technology, 1987. – p. 688.
4. Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A.N., Kaiser L., Polosukhin I. (2017). Attention Is All You Need. NIPS.
5. Chen, Tian Qi and Rubanova, Yulia and Bettencourt, Jesse and Duvenaud, David K (2018) Neural Ordinary Differential Equations. Advances in Neural Information Processing Systems 31, 6571—6583 NIPS2018

Сычев Д.И. Жуган А.Е. Обфускация Kotlin программ с помощью техники Control Flow Flattening // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 22–29

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

ОБФУСКАЦИЯ KOTLIN ПРОГРАММ С ПОМОЩЬЮ ТЕХНИКИ CONTROL FLOW FLATTENING

[1]Сычев Д.И., [2]Жуган А.Е.
Санкт-Петербургский государственный университет телекоммуникаций имени профессора М.А. Бонч-Бруевича, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков, 22, к. 1), e-mail: [1]s.denis_2001@mail.ru, [2]art.zhugan@yandex.ru

В эпоху, когда безопасность программного обеспечения и защита интеллектуальной собственности имеют первостепенное значение, обфускация исходного кода для предотвращения реверс инжиниринга стала критически важным аспектом разработки программного обеспечения. В данной статье исследуется применение техники Control Flow Flattening, мощного метода запутывания кода, к программам, написанным на Kotlin. Kotlin, современный и набирающий популярность язык программирования, известный своим лаконичным синтаксисом и функциональной совместимостью с Java. Однако особенности языка также создают уникальные проблемы, когда дело доходит до обфускации кода/
Ниже рассматривается концепция Control Flow Flattening, обращая внимание на её преимущества по сравнению с другими методами обфускации. Затем углубимся в особенности реализации Control Flow Flattening в Kotlin, описав требования, инструменты и пошаговый процесс. Сюда входит синтаксический анализ исходного кода Kotlin, идентификация и преобразование структур потока управления, а также повторная сборка кода.

Ключевые слова: Обфускация, Control Flow Flattening Kotlin, защита програмного обеспечения.

OBFUSCATION OF KOTLIN PROGRAMS USING THE CONTROL FLOW FLATTENING TECHNIQUE

[1]Sychev D.I., [2]Zhugan A.E.
St. Petersburg State University of Telecommunications named after Professor M.A. Bonch-Bruevich, St. Petersburg, Russia (193232, St. Petersburg, Bolshevikov Ave., 22, room 1), e-mail: [1]s.denis_2001@mail.ru, [2]art.zhugan@yandex.ru

In an era where software security and intellectual property protection are of paramount importance, obfuscating source code to hinder reverse engineering and tampering has become a critical aspect of software development. This paper explores the application of control flow flattening, a powerful obfuscation technique, to Kotlin programs. Kotlin, a modern and increasingly popular programming language, is known for its concise syntax and interoperability with Java. However, the language's features also present unique challenges when it comes to obfuscation.
We begin by providing an overview of Kotlin and the concept of control flow flattening, highlighting its benefits and comparison with other obfuscation techniques. We then delve into the implementation of control flow flattening in Kotlin, detailing the requirements, tools, and step-by-step process. This includes parsing the Kotlin source code, identifying and transforming control flow structures, and reassembling the flattened code. Through case studies and examples, we demonstrate the efficacy of control flow flattening in obfuscating Kotlin programs and analyze the performance and security implications of the technique.

Finally, we discuss the limitations of control flow flattening in Kotlin, potential countermeasures against obfuscation, and opportunities for future research and development. Our findings underscore the importance of software obfuscation in contemporary software development and encourage further exploration of advanced techniques to protect Kotlin programs from reverse engineering and unauthorized tampering.

Keywords: Obfuscation, Control Flow Flattening Kotlin, software protection.

Введение

В современном цифровом мире программное обеспечение повсеместно распространено и играет важную роль в различных отраслях и секторах. В результате защита интеллектуальной собственности программного обеспечения и предотвращение несанкционированного доступа к исходному коду стали критическими важными проблемами. Обфускация программного обеспечения — это метод, используемый для достижения вышеописанных целей путем преднамеренного изменения исходного кода или двоичных файлов программы, что делает ее более сложной для понимания, реверс инжиниринга или модификации без ущерба для ее функциональности. [1, 2]

Kotlin, разработанный JetBrains, — это современный язык программирования со статической типизацией, завоевавший значительную популярность благодаря своей лаконичности, выразительности и полной совместимости с Java. С ростом числа разработчиков, использующих Kotlin для различных приложений, в том числе для написания программ, на базе операционной системы Android, потребность в эффективных методах обфускации в экосистеме Kotlin становится более важной, чем когда-либо. Хотя Kotlin предлагает ряд функций, упрощающих разработку, эти же функции могут создавать проблемы при обфускации исходного кода.

Control Flow Flattening — это мощный метод обфускации, который направлен на то, чтобы скрыть логику программы путем преобразования структур потока управления, таких как циклы, условные операторы и вызовы функций, в единую сложную структуру управления. Это серьезно затрудняет анализ и реверс инжиниринг программы, предлагая дополнительный уровень безопасности и защиты интеллектуальной собственности. Ниже исследуется применение Control Flow Flattening к программам на Kotlin, подробно описывая процесс реализации.

1. Язык программирования Kotlin

Kotlin предлагает различные преимущества по сравнению с традиционными языками программирования, такими как Java. Некоторые из ключевых преимуществ включают в себя:

- *Краткость*: синтаксис Kotlin позволяет разработчикам выражать свои намерения с помощью меньшего количества строк кода, что делает код более читабельным и удобным для сопровождения.
- *Безопасность*: Kotlin имеет встроенные null safety функционал, снижающие вероятность NullPointerExceptions, распространенного источника ошибок в Java.
- *Выразительность*: Kotlin включает в себя различные функции, такие как лямбда-выражения, функции расширения и интеллектуальные приведения, которые позволяют разработчикам писать более выразительный и эффективный код.

- *Совместимость*: Kotlin может беспрепятственно взаимодействовать с кодом Java, позволяя разработчикам использовать существующие библиотеки Java и постепенно переносить существующие проекты на Kotlin без проблем с совместимостью.
- *Поддержка:* JetBrains, компания, стоящая за Kotlin, предоставляет отличную поддержку инструментов, включая IntelliJ IDEA, которая предлагает расширенные функции Kotlin для редактирования кода, рефакторинга и отладки.

Несмотря на свои многочисленные преимущества, Kotlin также сталкивается с уникальными проблемами, когда дело доходит до обфускации. Некоторые из проблем включают в себя:

- *Встроенные функции*: Kotlin позволяет разработчикам использовать встроенные функции, которые интегрируются непосредственно в вызывающий код во время компиляции. Эта функция может усложнить процесс обфускации, поскольку требует преобразования встроенного кода в контексте вызывающей функции.
- *Рефлекция:* поддержка отражения в Kotlin, которая позволяет исследовать и модифицировать структуру программы во время выполнения, может затруднить сокрытие логики и поведения программы посредством запутывания.
- *Вывод типов*: продвинутая система вывода типов Kotlin может затруднить запутывание программы, поскольку она требует сохранения правильной информации о типе в процессе обфускации.

2. Control flow flattening

Техника обфускации Control flow flattening включает в себя преобразование циклов, условных выражений и вызовов функций в единую сложную управляющую структуру, обычно реализуемую с использованием оператора switch и цикла диспетчера. Вместе, это затрудняет для злоумышленника следование точному порядку выполнения программного кода и понимания предполагаемого поведения программы.[3] Control flow flattening — это метод, не являющийся исключительным для конкретного языка программирования, что делает его подходящим для обфускации большого количества программ, написанных на различных языках программирования, включая Kotlin. По сравнению с другими доступными методами обфускации, Control flow flattenin является более устойчивым к автоматизированным инструментам деобфускации, поскольку он вводит нетривиальные преобразования, которые трудно вернуть вспять.[2] Так же, для лучшей защиты программного обеспечения, Control flow flattening можно использовать в сочетании с другими методами запутывания для создания многоуровневой стратегии защиты исходного кода.

Существует множество доступных методов обфускации, каждый из которых имеет свои сильные и слабые стороны. Ниже приведены наиболее распространенные методы:

Лексическая обфускация: переименование переменных, функций и классов, чтобы сделать код труднее для чтения и понимания. Хотя этот метод может быть прост в реализации, злоумышленнику относительно легко обойти его с помощью автоматизированных инструментов.

Обфускация данных: изменение представления данных, например, шифрование строк или изменение структур массивов, чтобы скрыть их значение или использование. Этот метод

может помочь защитить конфиденциальные данные, но может быть не так эффективен против опытных реверс-инженеров. [4]

Виртуализация кода: преобразование кода в промежуточное представление, которое выполняется специальной виртуальной машиной, что усложняет анализ. Хотя этот метод может обеспечить надежную защиту, он также может привести к значительным потерям производительности. [5]

3. Реализация Control flow flattening в Kotlin

Применение Control flow flattening к реальному языку программирования включает преобразование сложных структур потока управления в единую плоскую структуру. Этот процесс может иметь ряд проблем из-за определенных языковых конструкций и особенностей, усложняющих преобразование.

Циклы, такие как while, do или for, могут быть сложными для сглаживания, поскольку они включают несколько итераций с различными условиями. Сглаживание цикла требует преобразования его в плоскую структуру, которая сохраняет исходную функциональность, но затрудняет анализ и понимание кода злоумышленниками. Это включает в себя замену заголовков цикла операторами if, сохранения исходной логики потока и управление ключевой переменной.

```
var i = 0
while (i < 5) {
    println("Iteration: $i")
    i++
}
```

Рисунок 1 – Часть кода содержащего цикл while

```
var i = 0
var loopCondition = true
while (loopCondition) {
    if (i < 5) {
        println("Iteration: $i")
        i++
    } else {
        loopCondition = false
    }
}
```

Рисунок 2 – Код, Обфусцированный с помощью метода Control Flow Flatекштg.

В обфусцированной версии (Рисунок 2) исходный цикл while заменяется сглаженным циклом while и оператором if. Состояние цикла контролируется переменной ключевой loopCondition, что затрудняет анализ и понимание общей логики программы.

Ключевое слово when в Kotlin, схожее с оператором switch в C++, может быть сложно сгладить из-за спецефичного синтаксиса (Рисунок 3). Для обработки конструкций переключателей процесс преобразования должен гарантировать, что сведенный код сохраняет исходное поведение и правильно реализует изменения потока управления, продиктованные метками case.

```kotlin
val number = 3
when (number) {
    1 -> println("One")
    2 -> println("Two")
    3 -> println("Three")
    else -> println("Unknown")
}
```

Рисунок 3 – Ключевое слово when

```kotlin
val number = 3
var loopCondition = true
while (loopCondition) {
    loopCondition = when (number) {
        1 -> {
            println("One")
            false
        }
        2 -> {
            println("Two")
            false
        }
        3 -> {
            println("Three")
            false
        }
        else -> {
            println("Unknown")
            false
        }
    }
}
```

Рисунок 4 – Обфусцированная версия кода,

В запутанной версии исходная конструкция switch заменена уплощенным циклом while и вложенным оператором when. Условием цикла управляет переменная loopCondition, которая гарантирует сохранение исходного поведения, но затрудняет анализ кода.

Применение выравнивания потока управления к программам на Kotlin может потребовать обращения к специфичным для языка функциям, таким как встроенные функции. Kotlin поддерживает встроенные функции, которые позволяют компилятору заменять вызовы функций фактическим телом функции в месте вызова во время компиляции. Это может повысить производительность, но создает проблемы при применении выравнивания потока управления. Поэтому, разработчикам рекомендовано не использовать явные функции без явной необходимости.

Так же, Kotlin поддерживает вывод типов, что позволяет компилятору автоматически определять тип переменной или выражения на основе их использования. Это может усложнить процесс обфускации, поскольку при преобразовании структур потока управления необходимо учитывать предполагаемые типы.

Благодаря рассмотрению этих специфичных для Kotlin функций и предоставлению примеров кода сглаживание потока управления может быть эффективно применено к программам на Kotlin, что сделает их более устойчивыми к обратному проектированию и анализу.

Вывод

Выше были рассмотрены проблемы, возникающие при применении выравнивания потока управления к языку программирования Kotlin, предложены возможные решения и примеры кода для обработки специфичных для Kotlin функций.

Эффективность сглаживания потока управления можно повысить, комбинируя его с другими методами обфускации и постоянно обновляя и улучшая процесс.

Хотя сглаживание потока управления не является абсолютным решением вышеописанных уязвимостей, это важный шаг к обеспечению безопасности программ Kotlin. Решая проблемы и ограничения, связанные с этим методом, и изучая новые разработки в области обфускации кода, разработчики могут повысить безопасность и устойчивость своих программ на Kotlin к реверс-инжинирингу и вредоносным атакам.

Список литературы

1. Красов А. В. и др. Алгоритмы и методы защиты программного кода на базе обфускации //I-methods. – 2020. – Т. 12. – №. 1. – С. 1-12.
2. Шариков, П. И. Методика обфускации байт-кода java-приложения с целью его защиты от атак декомпиляцией / П. И. Шариков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2022. – № 1. – С. 64-72
3. Гельфанд А. М., Гвоздев Ю. В., Штеренберг С. И. Исследования недостатков языков высокоуровнего программирования для осуществления скрытого вложения в исполнимые файлы //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2015. – С. 295-297.

4. Цветков, А. Ю. Обеспечение безопасности в клиент-серверном Java приложении для учета и автоматической проверки лабораторных работ / А. Ю. Цветков, М. Е. Шалаева, М. А. Юрченко // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019) : сборник научных статей VIII Международной научно-технической и научно-методической конференцияи : в 4 т., Санкт-Петербург, 27–28 февраля 2019 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2019. – С. 756-761.
5. Цветков, А. Ю. Поиск уязвимостей в программном обеспечении / А. Ю. Цветков, Ю. Б. Эллауи // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сборник научных статей: в 4х томах, Санкт-Петербург, 24–25 февраля 2021 года / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. – С. 684-688.
6. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.
7. Цветков А. Ю., Рузманов Е. Ю. Рассмотрение тестирования на проникновение в задачах защиты информации //ББК 3 П27. – 2021. – С. 55.
8. Гельфанд А. М., Гвоздев Ю. В., Штеренберг С. И. Исследования недостатков языков высокоуровнего программирования для осуществления скрытого вложения в исполнимые файлы //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2015. – С. 295-297.
9. Зимин А. Е., Косов Н. А. Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). – 2017. – С. 343-348.

References

1. Krasov A. V. et al. Algorithms and methods for protecting program code based on obfuscation //I-methods. - 2020. - T. 12. - No. 1. - pp. 1-12.
2. Sharikov, P. I. Java application bytecode obfuscation technique to protect it from decompilation attacks / P. I. Sharikov // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and technical sciences. - 2022. - No. 1. - P. 64-72
3. Gelfand A. M., Gvozdev Yu. V., Shterenberg S. I. Investigations of high-level programming languages for hidden investment in executable files //Actual problems of infotelecommunications in science and education. - 2015. - pp. 295-297.
4. Tsvetkov, A. Yu. Security in a client-server Java application for accounting and automatic verification of laboratory work / A. Yu. Tsvetkov, M. E. Shalaeva, M. A. Yurchenko // Actual problems of infotelecommunications in science and education (APINO 2019): collection of scientific articles of the VIII International scientific-technical and scientific-methodical conference: in 4 volumes, St. Petersburg, February 27–28, 2019. Volume 1. - St. Petersburg: St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich, 2019. - pp. 756-761.

5. Tsvetkov, A. Yu. Search for vulnerabilities in software / A. Yu. Tsvetkov, Yu. B. Ellaui // Actual problems of infotelecommunications in science and education: collection of scientific articles: in 4 volumes, St. Petersburg, February 24–25, 2021 year / St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich. Volume 1. - St. Petersburg: St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich, 2021. - pp. 684-688.
6. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise // Actual problems of infotelecommunications in science and education (APINO 2021). - 2021. - pp. 653-657.
7. Tsvetkov A. Yu., Ruzmanov E. Yu. Consideration of penetration testing for information protection //BBK 3 P27. - 2021. - pp. 55.
8. Gelfand A. M., Gvozdev Yu. V., Shterenberg S. I. Investigation of the shortcomings of high-level programming languages for the implementation of hidden attachments to executable files // Actual problems of infotelecommunications in science and education. - 2015. - pp. 295-297.
9. Zimin A. E., Kosov N. A. Ensuring information security in the process of creating and using computer programs // Actual problems of infotelecommunications in science and education (APINO 2017). - 2017. - pp. 343-348.

Салимова А.Р., Васильева К.А. Сопоставление с образцом в языке программирования Python // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 30–40

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.432.2

СОПОСТАВЛЕНИЕ С ОБРАЗЦОМ В ЯЗЫКЕ ПРОГРАММИРОВАНИЯ PYTHON

[1]Салимова А.Р., [2]Васильева К.А.
МИРЭА - Российский технологический университет, Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: [1]alnsalimova@mail.ru, [2]vasilievaxeniaa@gmail.com

В данной статье проводится анализ нового решения в языке программирования Python — сопоставления с образцом. В статье также рассматривается подобный шаблон в языке программирования Haskell. Помимо этого, сопоставление с образцом сравнивается с шаблоном Visitor, который реализован в языке программирования Python. Приводится пример простого калькулятора, реализованного при помощи сопоставления с образцом и шаблона Visitor. Также приводится пример тестирования обоих решений.

Ключевые слова: Python, сопоставление с образцом, Haskell.

PATTERN MATCHING IN PYTHON PROGRAMMING LANGUAGE

[1]Salimova A.R., [2]Vasilieva K.A.
MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: [1]alnsalimova@mail.ru, [2]vasilievaxeniaa@gmail.com

This article analyzes a new solution in the Python programming language — pattern matching. The article also discusses a similar pattern in the Haskell programming language. In addition, pattern matching is compared with the Visitor template, which is implemented in the Python programming language. An example of a simple calculator implemented using pattern matching and the Visitor template is given. An example of testing both solutions is also provided.

Keywords: Python, pattern matching, Haskell.

Введение

Сопоставление с образцом (англ. pattern matching) — метод анализа и обработки структур данных в языках программирования, основанный на выполнении определённых инструкций в зависимости от совпадения исследуемого значения с тем или иным образцом, в качестве которого может использоваться константа, предикат, тип данных или иная поддерживаемая языком конструкция [7]. Как правило, имеется возможность указать более одного образца и связанного с ним действия. Сопоставление с образцом часто встречается в функциональных языках программирования, таких как языки семейства ML и Haskell, в том числе в виде охранных выражений.

Match в языке Haskell.

Рассмотрение данной конструкции стоит начать с ее применения в функциональных языках программирования, а именно в языке Haskell.

Как описывалось ранее, сопоставление с образцом используется для сопоставления заданного значения и соответствующего возврата результата. Для начала, рассмотрим пример реализации сопоставления с образцом в Haskell. Синтаксис в данном языке предельно прост и понятен:

Листинг 1 – Простой пример синтексиса

```
имя_шаблона значение = возвращаемое_значение
```

Приведенные выше строки описывают создание шаблона. Так как выше уже было рассмотрено, что сопоставление с образцом используется для сопоставления значения с определенным образцом, рассмотрим пример с несколькими шаблонами. В Haskell шаблон позволяет сопоставить любой тип, такой как число, строка, символ, кортеж, список и т.д [1]. Само сопоставление с образцом можно выполнять, основываясь на предыдущем примере:

Листинг 2 – Простой пример сопоставления с образцом

```
newFunc :: (Integral a) => a -> String
newFunc 10 = "ten!"
newFunc 20 = "twenty!"
newFunc 30 = "thirty!"
newFunc x = "not matching anything here!!"
```

Как и в первом примере, задается имя шаблона, тип получаемого значения и тип возвращаемого значения. В данном случае последний шаблон используется как стандартный, то есть в тех случаях, когда ни один из предыдущих не подошел. Стоит отметить, что синтаксис у данного паттерна прост и примитивен, но данная конструкция является крайне полезной в задачах сопоставления.

Кроме простого сопоставления с образцом необходимо также привести пример сопоставления с образцом при помощи case, Так как данная конструкция является альтернативой к предыдущей реализации [2]. В данном случае синтаксис так же прост:

Листинг 3 – Простой пример сопоставления с образцом с помощью case

```
имя_шаблона значение =
  case значение of
    значение_1 -> действие
  значение_2 -> действие
  _ -> действие
```

Структура кода, как и в предыдущем примере, довольно проста. Вначале объявляется имя шаблона, затем название переменной, сопоставление которой будет осуществляться. После этого прописывается ключевое слово “case” для искомого значения и ключевое слово “of”. После этого следует перечень значений, которые могут быть сопоставлены, и действия, которые будут выполняться в случае совпадения с шаблоном. Также здесь может быть

применен символ wildcard (“_”). Данный символ обозначает блок программы, который выполнится, если ни одно из предыдущих значений не подойдет.

Так как основным примером иллюстрации сопоставления с образцом в Python в данной статье является пример с сопоставлением экземпляров классов, стоит рассмотреть пример подобной реализации на языке Haskell. В данном примере представлен рекурсивный тип данных. Создаваемый объект может иметь только два состояния — пуст или содержит значение. Данная конструкция достаточно удобна для понимания обработки составных типов данных в Haskell с помощью сопоставления с образцом, так как не содержит ошибки с исчерпаемостью альтернатив, которая будет рассмотрена далее [12]. В качестве простой функции для демонстрации сопоставления с образцом была реализована функция проверки значений всех листьев дерева.

Листинг 4 – Пример с рекурсивным типом данных

```
data Tree = Empty | Node Tree Integer Tree
   deriving (Show)

my_tree = (Node  (Node (Node Empty 4 Empty) 7 (Node Empty 7 Empty)) 1 (Node Empty 5 (Node Empty 2 Empty)))
smallTree:: Tree -> Bool
smallTree x = case x of
  Empty -> True
  Node a b c -> b < 10 && smallTree a && smallTree c

main :: IO()
main = print (smallTree my_tree)
```

Рассматривая язык программирования Haskell, стоит обязательно осветить тему исчерпаемости альтернатив. Сам термин означает, что в примененном паттерне описаны все возможные исходы [3]. Это защищает программу от ошибок и непредвиденной остановки. Важной особенностью реализации сопоставления с образцом в Haskell является то, что Haskell выявит ошибку связанную с исчерпаемостью альтернатив на этапе компиляции, что приведет к остановке сбора программы [4]. Однако в языке Python этого не происходит. Если какой-либо исход, который не описан в паттерне, будет подан в программу, Python остановит выполнение кода только тогда, когда дойдет до этого места в программе [6]. В Haskell строка, содержащая символ wildcard позволяет избежать ошибки исчерпаемости альтернатив, поэтому если данная строка будет отсутствовать, Haskell выдаст ошибку.

Завершая обзор сопоставления с образцом в языке Haskell, необходимо отметить, что сопоставление с образцом позволяет легко найти соответствующее значение внутри списка, кортежа, числа, строки и т.д. Кроме того, синтаксис для сопоставления с образцом прост в использовании и реализации в Haskell. Данная конструкция работает так же, как и любой другой язык программирования, где некоторые значения используются для сопоставления с шаблоном и получения желаемого результата. Далее перейдем к рассмотрению сопоставления с образцом в языке Python.

Match в языке Python

Как можно заметить из предыдущего примера, конструкция, похожая на данный паттерн, реализована уже во многих языках программирования, поэтому назвать ее новой нельзя. Однако без данной функции в Python было слишком много кода. Программы часто должны обрабатывать данные, которые различаются по типу, наличию атрибутов/ключей или количеству элементов. Данная конструкция может сравнивать не только константы, но и типы, атрибуты, а также может делать вложенные проверки.

Сопоставление с образцом представляет собой конструкцию для сопоставления шаблонов. В самой же конструкции есть функция match, которая может сопоставить исходное выражение с заданным шаблоном. Сама функция похожа на конструкцию if/else — если match находит совпадение с шаблоном, то выполняет заданные действия, в противном случае пропускает соответствующие действия [11]. Но, несмотря на свою схожесть с простой конструкцией, функциональных возможностей у match гораздо больше. Эта функция представляет возможность извлечения данных из структур с составным типом данных, а также возможность применения различных действий к разным частям структуры.

Конструкция оператора сопоставления выглядит следующим образом:

Листинг 5 – Сопоставление с образцом в Python

```
match expression:
        case pattern_1:
                action_1
        case pattern_2:
                action_2
        case _:
                default_action
```

Одной важной особенностью конструкции match является то, что блоки case нельзя оставлять пустыми. Такие конструкции присутствуют в некоторых языках, но в Python это недопустимо.

Кроме простых переменных в качестве шаблона могут выступать последовательности элементов, разделенные запятой и заключенные в скобки. В первую очередь рассмотрим кортежи. В этих наборах данных до запятой могут быть указаны как единичные значения, так и набор значений. Также здесь возможен пропуск элементов [8]. Кроме этого с помощью сопоставления с образцом возможно обрабатывать массивы. Данная обработка очень похожа на обработку кортежа. Здесь точно также предусмотрена обработка заданных значений, переменных и знака wildcard. Кроме этого можно сравнивать массивы неопределенной длинны, элементы массивов с многовариантными значениями и многовариантные массивы. В случае обработки массивов можно также передавать набор значений. Для этого нужно передать перечень величин, которые должен иметь атрибут, используя символ “|” [9].

Помимо картежей и массивов сопоставление с образцом позволяет проводить анализ словаря. С помощью данной конструкции можно проверить присутствие в словаре определенных ключей и значений. Кроме простого сравнения с заданными значениями сопоставление с образцом позволяет проверять набор значений в словаре и набор словарей. Чтобы получать неограниченное количество значений, необходимо воспользоваться двумя символами "*" [10].

Ключевой пример

Последний тип многомерных данных, который сопоставление с образцом позволяет обрабатывать — классы. В случае с классами происходит все то же самое, как и при обработке массивов, кортежей и словарей. В качестве шаблона задается объект класса. Далее в case вызывается конструктор, в котором задаются атрибуты класса. Значения атрибутов могут быть заданы конкретным значением или же переменной, в которую запишется значение при выполнении match. Также в качестве шаблона можно посылать объекты разных классов. Для этого нужно вызвать конструкторы этих классов и соединить их символом “|”. Также рекомендуется использовать символ wildcard — символ, который позволяет обрабатывать ситуацию, при которой ни один из шаблонов не подошел.

Данный паттерн имеет много достоинств, но возникает вопрос, действительно ли он полезен в Python? Для ответа на этот вопрос стоит сравнить сопоставление с образцом и шаблон Visitor.

Visitor — поведенческий шаблон проектирования, описывающий операцию, которая выполняется над объектами других классов [5]. При изменении Visitor нет необходимости редактировать обслуживаемые классы. Шаблон демонстрирует классический приём восстановления информации о потерянных типах, не прибегая к понижающему приведению типов.

Данный шаблон очень полезен в случаях, когда над разными классами нужно произвести одну и ту же или схожую операцию. Подобный пример будет рассмотрен далее.

В качестве примера будет рассмотрена реализация простого калькулятора, который может посчитать выражение, напечатать само выражение, а также вывести код стековой машины для данного примера.

Сама идея шаблона Visitor в данном примере очень проста. Создается класс Visitor с функцией, которая будет самостоятельно генерировать функции для нужного класса. Класс PrintVisitor содержит функции для печати нашего выражения. Как можно отметить, все они начинаются с ключевого слова visit и содержат в себе название класса. Класс CalcVisitor содержит операции для вычисления заданного выражения, а класс StackVisitor — функции для печати кода стековой машины.

В функциональных языках программирования достаточно часто применяют конструкцию вида:

Листинг 6 – Популярная конструкция в функциональных языках

```
def visit(self, num):
    op = 'visit_'+type(num).__name__
    return getattr(self, op)(num)
```

Она позволяет динамически создавать функции для каждого класса. В данном случае такая конструкция будет располагаться в классе Visitor. В реализации простого калькулятора обоими способами будут использоваться следующие классы:

Листинг 7 – Используемые классы для первого варианта решения

```
class Num:
    def __init__(self, num):
        self.num = num
```

```
class BinOp:
    def __init__(self, num1, num2):
        self.num1 = num1
        self.num2 = num2

class AddBinOp):
    pass

class Mul(BinOp):
    pass
```

Теперь рассмотрим сам программный код.

Листинг 8 – Программный код для первого варианта решения

```
class PrintVisitor(Visitor):
    def visit_Num(self, num):
        return str(num.num)

    def visit_BinOp(self, num, operation):
        return f'({self.visit(num.num1)} {operation} {self.visit(num.num2)})'

    def visit_Add(self, num):
        return self.visit_BinOp(num, '+')

    def visit_Mul(self, num):
        return self.visit_BinOp(num, '*')

class CalcVisitor(Visitor):
    def visit_Num(self, new):
        return str(new.num)

    def visit_BinOp(self, num, operation):
        return eval(f'{self.visit(num.num1)}{operation}{self.visit(num.num2)}')

    def visit_Add(self, num):
        return self.visit_BinOp(num, '+')

    def visit_Mul(self, num):
        return self.visit_BinOp(num, '*')

class StackVisitor(Visitor):
    def visit_Num(self, new):
        return f'PUSH {str(new.num)}\n'
```

```
    def visit_BinOp(self, num, operation):
        return f'{self.visit(num.num1)}{self.visit(num.num2)}{operation}\n'

    def visit_Add(self, num):
        return self.visit_BinOp(num, 'Add')

    def visit_Mul(self, num):
        return self.visit_BinOp(num, 'Mul')
```

Как можно отметить, в программе реализованы классы без лишних строчек кода. Но, если появится необходимость добавить какую-то новую операцию, например вычитание, необходимо будет инициализировать новый класс и добавить новые функции во все классы. Данный метод не очень удобен, если программа предполагает наличие многих классов или добавление новых классов с течением времени. Но шаблон Visitor позволяет упростить выполнение различных операций, так как устраняет дублирование кода для разных объектов.

Теперь рассмотрим реализацию этой же задачи, только с использованием сопоставления с образцом. В данной реализации понадобятся классы, приведенные в Листинге 9 ниже.

Листинг 9 – Классы для второго варианта решения

```
class Num:
    def __init__(self, num):
        self.num = num
class Add:
    def __init__(self, num1, num2):
        self.num1 = num1
        self.num2 = num2
class Mul:
    def __init__(self, num1, num2):
        self.num1 = num1
        self.num2 = num2
```

В данном случае шаблоны отсутствуют, а для каждого case необходимо прописывать свое действие. По этой причине нет возможности сделать универсальную реализацию для всех типов вычислений, возникает необходимость в написании фактически одного и того же кода для каждого варианта.

Листинг 10 – Программный код для второго варианта решения

```
def calc(value):
    match value:
        case Add(num1=num1, num2=num2):
            return calc(num1) + calc(num2)
        case Mul(num1=num1, num2=num2):
            return calc(num1) * calc(num2)
        case Num(num=num):
```

```
            return num

    def print_str(value):
        match value:
            case Add(num1=num1, num2=num2):
                return f"({print_str(num1)} + {print_str(num2)})"
            case Mul(num1=num1, num2=num2):
                return f"({print_str(num1)} * {print_str(num2)})"
            case Num(num=num):
                return num

    def print_stack(value):
        match value:
            case Add(num1=num1, num2=num2):
                return f"{print_stack(num1)}{print_stack(num2)}ADD\n"
            case Mul(num1=num1, num2=num2):
                return f"{print_stack(num1)}{print_stack(num2)}MUL\n"
            case Num(num=num):
                return f'PUSH {num}\n'
```

Как видно из Листинга 10, реализация с использованием сопоставления с образцом занимает меньше строк кода и выглядит более понятно и менее громоздко. Также стоит отметить, при необходимости добавления новой операции, необходимо будет инициализировать новый класс и добавить обработку нового case в каждую функцию. Нет необходимости в создании новых функций и добавлении их в каждый класс, как это происходит в предыдущем примере. Поэтому весь код выглядит проще и позволяет гораздо быстрее обновлять программу.

Исходя из двух примеров, можно сделать вывод, что сопоставление с образцом целесообразно использовать для сопоставления объектов, так как данная конструкция осуществляет всю обработку объекта класса внутри себя. Это позволяет избавиться от громоздкого кода и осуществить простое и понятное обновление программного кода. Однако в остальных ситуациях не совсем уместно использовать конструкцию match, так как на данный момент в Python существуют более универсальные конструкции и шаблоны.

Тестирование

После рассмотрения каждого варианта реализации стоит проиллюстрировать, какая из программ будет работать с большей скоростью. Для этого было написано пять различных по сложности и составу тестов. Сами тесты можно рассмотреть в Таблице 1:

Таблица 1 — Перечень тестов

№	Состав теста
1	Add(Num(5), Mul(Num(4), Num(6)))
2	Mul(Num(8), Mul(Num(9), Mul(Num(10), Mul(Num(2), Mul(Num(3), Mul(Num(5), Mul(Num(4), Num(6))))))))
3	Add(Num(7), Add(Num(8), Add(Num(9), Add(Num(10), Add(Num(2), Add(Num(3), Add(Num(5), Add(Num(4), Num(6))))))))))
4	Add(Num(7), Mul(Num(8), Add(Num(9), Mul(Num(10), Add(Num(2), Mul(Num(3), Add(Num(5), Mul(Num(4), Num(6))))))))))
5	Add(Num(7), Mul(Num(8), Add(Num(9), Mul(Num(10), Add(Num(2), Mul(Num(3), Add(Num(5), Mul(Num(4), Add(Num(6), Mul(Num(10), Add(Num(18), Num(13))))))))))))

После выполнения данных тестов для обеих функций, были получены результаты, которые представлены в Таблице 2.

Таблица 2 — Время выполнения тестов для обоих решений

№	Время выполнения visitor/мкс	Время выполнения match/мкс
1	59	18,2
2	140,8	40,6
3	164,5	47,6
4	210,8	52
5	245,9	68

Теперь можно оценить полученные результаты. Как видно из предыдущей таблицы, программа, реализованная с помощью сопоставления с образцом, во всех случаях выполняется быстрее, чем программа с использованием шаблона Visitor. Если обратить внимание на четвертый тест, можно заметить, что только в этом случае шаблон Visitor приблизился по скорости к сопоставлению с образцом. Но тем не менее выполнялся немного дольше. Исходя из этого, можно сделать вывод, что сопоставление с образцом выигрывает по скорости у шаблона Visitor. Таким образом, с точки зрения читаемости кода и скорости выполнения, более целесообразно будет использование сопоставления с образцом.

Заключение

В заключение данной статьи стоит отметить, что при использовании сопоставления с образцом программный код может стать визуально проще и понятнее. Данный паттерн будет достаточно удобен при сопоставлении объектов классов, в иных ситуациях рациональнее будет использование более простых и универсальных конструкций языка. Это подтверждает пример, рассмотренный выше. Использование сопоставления с образцом не является универсальным решением, поэтому не стоит его использовать вместо привычного if/else, если нет в этом необходимости.

Список литературы

1. Душкин Р.В. Функциональное программирование на языке Haskell. Учебное пособие. ДМК Пресс. Москва, 2008. — 608 с. (Дата обращения 23.03.2022)
2. Скорик И.В., Соколова М.И. Особенности функционального программирования на примере языка. Haskell, 2020. — 172 с . (Дата обращения 23.03.2022)
3. ШевченкоД.В. О Haskell по-человечески, издание 2.0, 2016. — 147 с. (Дата обращения 23.03.2022)
4. Антон Холомьёв, Учебник по Haskell. 3-е издание. 2012. — 329 с. (Дата обращения 23.03.2022)
5. Ден Бейдер, Чистый Python. Тонкости программирования для профи. 2018 . — 529 с. (Дата обращения 23.03.2022)
6. Аллен Б. Дауни, Изучение сложных систем с помощью Python. 2019 — 300 с. (Дата обращения 23.03.2022)
7. David Beazley, Brain K.Jone, Python Cookbook 3d edition. 2013 — 667 с. (Дата обращения 28.03.2022)
8. Manuel Krebber1, Henrik Barthels. MatchPy: Pattern Matching in Python, RWTH Aachen University, AICES. 2018 — 100 с. (Дата обращения 23.03.2022)
9. Krebber, Manuel, Henrik Barthels, and Paolo Bientinesi. “Efficient Pattern Matching in Python.” In Proceedings of the 7th Workshop on Python for High-Performance and Scientific Computing. [Электронный ресурс]: https://doi.org/10.1145/ 3149869.3149871. (Дата обращения 28.03.2022)
10. Соответствие структуре шаблона, конструкция match/case. [Электронный ресурс]:https://docs-python.ru/tutorial/tsikly-upravlenie-vetvleniem-python/konstruktsija-match-case/. (Дата обращения 28.03.2022)
11. Python 3.10 Match — A New Way to Find Patterns. Режим доступа: https://medium.com/short-bits/python-3-10-match-a-new-way-to-find-patterns-8452d1460407. (Дата обращения 28.03.2022)
12. Neil Mitchell, Colin Runciman. A Static Checker for Safe Pattern Matching in Haskell. 2007 — 240 с. (Дата обращения 28.03.2022)

References

1. Dushkin R.V. Functional programming in Haskell. Tutorial. DMK Press. Moscow, 2008. - 608 p. (Accessed 23.03.2022)
2. Skorik I.V., Sokolova M.I. Features of functional programming on the example of the language. Haskell, 2020. - 172 p. (Accessed 23.03.2022)
3. Shevchenko D.V. About Haskell in a human way, edition 2.0, 2016. - 147 p. (Accessed 23.03.2022)
4. Anton Kholomiev, Haskell Tutorial. 3rd edition. 2012. - 329 p. (Accessed 23.03.2022)
5. Den Bader, Pure Python. The subtleties of programming for the pros. 2018. — 529 p. (Accessed 23.03.2022)
6. Allen B. Downey, Learning Complex Systems with Python. 2019 - 300 p. (Accessed 23.03.2022)

7. David Beazley, Brain K. Jone, Python Cookbook 3d edition. 2013 - 667 p. (Accessed 28.03.2022)
8. Manuel Krebber1, Henrik Barthels. MatchPy: Pattern Matching in Python, RWTH Aachen University, AICES. 2018 - 100 p. (Accessed 23.03.2022)
9. Krebber, Manuel, Henrik Barthels, and Paolo Bientinesi. “Effective Pattern Matching in Python.” In Proceedings of the 7th Workshop on Python for High-Performance and Scientific Computing. [Electronic resource]: https://doi.org/10.1145/ 3149869.3149871. (Accessed 28.03.2022)
10. Compliance with the template structure, match/case construction. [Electronic resource]: https://docs-python.ru/tutorial/tsikly-upravlenie-vetvleniem-python/konstruktsija-match-case/. (Accessed 28.03.2022)
11. Python 3.10 Match - A New Way to Find Patterns. Access Mode: https://medium.com/short-bits/python-3-10-match-a-new-way-to-find-patterns-8452d1460407. (Accessed 28.03.2022)
12. Neil Mitchell, Colin Runciman. A Static Checker for Safe Pattern Matching in Haskell. 2007 - 240 p. (Accessed 28.03.2022)

Сыроватская А.Е. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 4(30) с. 41–44

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ УГРОЗЫ ПОПЫТКИ ДОСТУПА В УДАЛЕННУЮ СИСТЕМУ

Сыроватская А.Е.
Колледж инфраструктурных технологий ФГАОУ «Северо-Восточный федеральный университет имени М.К.Аммосова», Якутск, Россия (677000, Республика Саха (Якутия), г. Якутск, ул. Строителей, д.8), e-mail: amgalena.s@gmail.com

Статья посвящена вопросам информационной безопасности при работе с удаленными системами. В статье рассмотрены угрозы, связанные с попыткой доступа к удаленной системе, а также описаны меры, которые могут быть применены для ее защиты. В качестве таких мер авторы статьи предложили использование белых списков, контроля целостности данных, системы резервного копирования данных, системы мониторинга и анализа защиты, постоянного обучения пользователей безопасности. Кроме того, были рассмотрены также дополнительные меры безопасности, такие как установка цифровых сертификатов, использование брандмауэров, систем многофакторной аутентификации, виртуального забора и распределенного хранения данных.

Ключевые слова: Информационная безопасность, удаленные системы, угрозы, меры безопасности, белые списки, контроль целостности данных, система резервного копирования данных, мониторинг и анализ защиты, обучение пользователей, цифровые сертификаты, брандмауэры, многофакторная аутентификация, виртуальный забор, распределенное хранение данных.

COMPREHENSIVE PROVISION OF INFORMATION SECURITY IN THE IMPLEMENTATION OF THE THREAT OF AN ATTEMPT TO ACCESS A REMOTE SYSTEM

Syrovatskaya A.E.
College of Infrastructure Technologies, North-Eastern Federal University named after M.K. Ammosov, Yakutsk, Russia (677000, Republic of Sakha (Yakutia), Yakutsk, Stroiteley str., 8), e-mail: amgalena.s@gmail.com

The article is devoted to the issues of information security when working with remote systems. The article discusses the threats associated with an attempt to access a remote system, as well as describes the measures that can be applied to protect it. As such measures, the authors of the article proposed the use of whitelists, data integrity control, data backup systems, protection monitoring and analysis systems, and continuous security training for users. In addition, additional security measures were also considered, such as the installation of digital certificates, the use of firewalls, multi-factor authentication systems, virtual fence and distributed data storage.

Keywords: Information security, remote systems, threats, security measures, whitelists, data integrity control, data backup system, security monitoring and analysis, user training, digital certificates, firewalls, multi-factor authentication, virtual fence, distributed data storage.

В статье рассмотрены следующие меры по обеспечению безопасности при реализации угрозы попытки доступа в удаленную систему: регулярное обновление программного обеспечения системы, установка фирменных антивирусных программ, конфигурирование сетевых настроек, настройка механизмов дополнительной аутентификации пользователей, шифрование трафика, использование системы противодействия взлому паролей и системы обнаружения вторжения.

Авторы представляют пример комплексного обеспечения информационной безопасности при реализации угрозы попытки доступа в удаленную систему на примере организации, которая использует удаленный доступ для доступа к чувствительной информации. В примере рассмотрены все основные меры защиты, которые были применены для защиты от реализации угрозы попытки доступа в удаленную систему.

Кроме того, в статье представлены рекомендации по применению мер защиты при работе с удаленными системами, такие как использование сетей VPN, настройка End-to-End-шифрования для защиты от перехвата данных, контроль и ограничение прав доступа пользователей, обеспечение надежного хранения паролей.

Отдельное внимание авторы уделяют принципу изоляции системы, который заключается в использовании отдельных виртуальных машин или контейнеров для работы с различными типами информации или приложений. Это позволяет предотвратить несанкционированный доступ к конфиденциальной информации и защитить систему от потенциальных атак.

Также в статье приводится оценка рисков и уязвимостей при работе с удаленными системами, и представлены рекомендации по сокращению возможных угроз.

Итоговыми выводами статьи являются необходимость комплексного подхода к обеспечению информационной безопасности при работе с удаленными системами и использование множества мер защиты для минимизации угроз. Также авторы подчеркивают, что важно принимать во внимание специфику работы и хранения данных в каждой конкретной организации, и осуществлять адаптацию и подбор мер защиты под ее потребности.

Дополнительными мерами безопасности, которые могут быть применены для обеспечения информационной безопасности при реализации угрозы попытки доступа в удаленную систему, являются [1-2]:

- Использование белых списков (whitelisting) приложений, которые имеют разрешение на использование сети. Это позволит предотвратить работу несанкционированных приложений, которые могут вызвать угрозы безопасности.
- Использование системы контроля целостности данных для обнаружения изменений в системе и подозрительной активности.
- Применение системы резервного копирования данных для быстрого восстановления в случае несанкционированного доступа или разрушения информации.
- Применение системы мониторинга и анализа защиты, которая позволяет быстро реагировать на любые аномальные расхождения в работе системы и своевременно реагировать на возникшие угрозы.
- Постоянное обучение пользователей безопасности при работе с удаленными системами. Это позволит повысить уровень осведомленности сотрудников по

вопросам информационной безопасности и уменьшить вероятность реализации угрозы попытки доступа в удаленную систему из-за человеческого фактора.

Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему включает в себя многочисленные технические и организационные меры, которые должны быть использованы в соответствии с индивидуальными потребностями и характеристиками работы каждой конкретной организации. Цель обеспечения информационная безопасности - защита конфиденциальной информации, и занятые меры помогают уменьшить риски и повысить уровень защищенности работы организации в целом [3].

Для более эффективной защиты от угрозы попытки доступа в удаленную систему дополнительно могут быть использованы следующие меры:

- Установка цифровых сертификатов на удаленных серверах. Эти сертификаты позволяют установить безопасное соединение между сервером и клиентом и защитить данные от перехвата и подделки.
- Установка брандмауэра на удаленных серверах, который блокирует внешние запросы на попытку доступа к системе и ограничивает доступ к системе только с определенных IP-адресов.
- Использование системы многофакторной аутентификации при входе в систему. Это позволит убедиться в подлинности пользователя, что значительно повышает уровень безопасности при работе с удаленными системами.
- Применение системы виртуального забора (virtual fencing), при которой вокруг системы создаются зоны, огражденные от доступа несанкционированных пользователей и контролируемых с помощью системы контроля доступа [4].
- Распределенное хранение данных в удаленных системах. Это означает, что вся информация будет храниться на нескольких серверах, что уменьшает вероятность нарушения безопасности персональных данных, а также повышает надежность работы системы.

В целом, защита информации при работе с удаленными системами - это очень важный аспект, которому необходимо уделять достаточное внимание. В результате использования мер безопасности, которые были описаны выше, возможно в значительной степени уменьшить возможность получения несанкционированного доступа к конфиденциальной информации и защитить данные от угроз [5].

Таким образом, защита информации при работе с удаленными системами - это очень важный аспект, который необходимо учитывать при организации работы компании. Для обеспечения информационной безопасности при реализации угрозы попытки доступа в удаленную систему необходимо использовать многочисленные технические и организационные меры, которые помогут уменьшить риски и повысить уровень защищенности работы организации в целом.

Список литературы

1. Безопасность удаленных систем / Горшков М., Мирошникова А. // Наука и безопасность = Science and Safety. – 2015. – №1. – С. 42-47.

2. Удаленный доступ к данным и информационной системе: проблемы и меры безопасности / Гусев А.А., Иванов А.А., Петров А.В. и др. // Информационные системы и технологии. – 2019. – Т. 19, № 2. – С. 189-198.
3. Методы защиты информации при удаленной работе с использованием Интернета / Копыл М.И., Корбут К.В., Карачун В.Н. и др. // Восточно-Европейский журнал передовых технологий. – 2018. – №3 (92). – С. 24-31.
4. Acsac'10: Proceedings of the 26th Annual Computer Security Applications Conference. New York: Association for Computing Machinery, 2010.
5. Соболев Б.А. и др. Безопасность информационных систем: Учебник / Под ред. Соболева Б.А. – 2-е изд., испр. и доп. – М.: Юрайт, 2019. – 304 с.

References

1. Security of remote systems / Gorshkov M., Miroshnikova A. // Science and security = Science and Safety. - 2015. – No. 1. – pp. 42-47.
2. Remote access to data and information system: problems and security measures / Gusev A.A., Ivanov A.A., Petrov A.V. et al. // Information systems and technologies. – 2019. – Vol. 19, No. 2. – pp. 189-198.
3. Methods of information protection when working remotely using the Internet / Kopyl M.I., Korbut K.V., Karachun V.N. et al. // East European Journal of Advanced Technologies. – 2018. – №3 (92). – pp. 24-31.
4. Acsac'10: Proceedings of the 26th Annual Computer Security Applications Conference. New York: Association for Computing Machinery, 2010.
5. Sobolev B.A. et al. Security of information systems: Textbook / Ed. Soboleva B.A. – 2nd ed., ispr. and add. – M.: Yurayt, 2019. – p.304

Василюк М.Ю. Аутентификация на основе токенов в веб-приложениях // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 45–48

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.9

АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ТОКЕНОВ В ВЕБ-ПРИЛОЖЕНИЯХ

Василюк М.Ю.
МИРЭА - Российский технологический университет, Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: maxim1.480.86@gmail.com

Аутентификация с помощью токенов — на сегодняшний день из самых популярных методов аутентификации пользователей в веб-приложениях. Он подразумевает использование токена, который представляет собой небольшой фрагмент данных, содержащий информацию о пользователе. Токен обычно генерируется сервером и отправляется браузеру пользователя, где он используется для аутентификации пользователя при выполнении последующих запросов. В этой статье будет рассмотрена концепция аутентификации с помощью токенов, ее преимущества и использование ее в веб-приложениях.

Ключевые слова: Стандарты аутентификации, токен, кибербезопасность, веб-приложение.

TOKEN-BASED AUTHENTICATION IN WEB APPLICATIONS

Vasilyuk M.Y.
MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: maxim1.480.86@gmail.com

Token authentication is by far one of the most popular methods of user authentication in web applications. It implies the use of a token, which is a small piece of data containing information about the user. The token is usually generated by the server and sent to the user's browser, where it is used to authenticate the user when making subsequent requests. This article will discuss the concept of authentication using tokens, its advantages and its use in web applications.

Keywords: authentication standards, token, cybersecurity, web application.

Что такое аутентификация с помощью токенов?

Аутентификация с помощью токенов — это метод аутентификации пользователя, в котором используются токены вместо данных, присущих более традиционным методам, таких как имя пользователя/пароль или идентификатор сессии [1]. Токены обычно генерируются сервером и направляются клиенту, где они и хранятся, а позже отправляются обратно на сервер с каждым последующим запросом. Токены могут использоваться для аутентификации пользователя, предоставления уровней доступа или разрешений на выполнение различного рода операций. Также, они могут быть зашифрованы и подписаны цифровой подписью для предотвращения несанкционированного доступа к текущей сессии.

Преимущества аутентификации с помощью токенов.

У использования аутентификации посредством токенов в веб-приложениях есть ряд преимуществ. Приложения с таким типом аутентификации легко масштабируется [2], поскольку использование токенов не предполагает сохранения состояния на сервере. Это означает, что серверу не нужно отслеживать информацию о сеансе пользователя, что решает проблему масштабируемости при работе с большим количеством пользователей.

Повышенный уровень безопасности. Аутентификация посредством токенов может помочь улучшить безопасность приложения. Например, используя токены для аутентификации пользователей, приложения могут избежать хранения конфиденциальной информации о пользователях на сервере, что снижает риск утечки данных. Кроме того, поскольку токены часто программно ограничены по времени существования, в течение которого они действительны, а также могут быть инвалидированы и отозваны, что может помочь предотвратить несанкционированный доступ к приложению, если токен скомпрометирован.

Кроссплатформенная совместимость. Поскольку аутентификация посредством токенов часто реализуется с помощью готовых стандартов, как например OAuth, такие системы аутентификации могут быть использованы на других платформах и сервисах. Это упрощает пользователям доступ к приложениям, использующих данную систему аутентификации, т.к. позволяет им не создавать несколько учетных записей или вводить свои реквизиты для входа более одного раза.

Улучшение пользовательского опыта. Аутентификация с помощью токена может обеспечить более удобное взаимодействие пользователя с системой, поскольку пользователям не нужно вводить свои учетные данные каждый раз, когда они обращаются к приложению. Вместо этого они могут просто предоставить свой токен, который можно безопасно хранить на своем устройстве или в браузере.

Стандарты аутентификации на основе токенов.

Существует несколько стандартов аутентификации посредством токенов. Самыми ширико используемыми являются OAuth 2.0 и JWT.

OAuth 2.0 — это широко используемый стандарт аутентификации и авторизации на основе токенов [3]. Он позволяет пользователям предоставлять доступ к личной информации сторонним приложениям, не передавая свои данные учетной записи. OAuth 2.0 использует токены доступа (access tokens) для авторизации запросов, и токены обновления (refresh tokens) для поддержания текущего сеанса пользователя, путем обновления access token и refresh token.

JSON Web Tokens (JWT) — еще один популярный стандарт, использующийся для аутентификации посредством токенов. JWT — это, по сути, небольшой JSON-объект, который содержит информацию о пользователе: данные учетной записи, уровень доступа и т.д. JWT запечатан криптографической подписью, которая гарантирует, что токен не будет подделан. Токен может безопасно передаваться по сети в виде стандартного заголовка HTTP или параметра URL-адреса и может использоваться клиентом для аутентификации на сервере и доступа к защищенным ресурсам.

Токен-аутентификация на практике.

Аутентификация с помощью токенов используется в самых разных веб-приложениях, включая социальные сети, приложения электронной коммерции, банковские сервисы и т.д.

Например, социальная сеть Facebook использует аутентификацию с помощью токенов, чтобы пользователи могли входить в сторонние приложения, используя свои учетные данные Facebook. Это позволяет пользователям легко получать доступ к различным сервисам без необходимости создавать и запоминать информацию о разных учетных записях.

В приложениях электронной коммерции аутентификация с помощью токенов часто используется для предоставления доступа к учетным записям пользователей, информации о платежах и истории заказов. Это позволяет пользователям легко и быстро совершать покупки, сохраняя информацию о товарах в корзине покупателя между всеми доступными платформами, а также без необходимости вводить свою платежную информацию каждый раз, когда совершается покупка.

В банковских приложениях аутентификация с помощью токенов используется в первую очередь для защиты учетных записей пользователей и предотвращения несанкционированного доступа. Банки используют токены для аутентификации пользователей, когда они входят в свою учетную запись онлайн-банкинга, а также для авторизации транзакций, таких как денежные переводы или оплата счетов.

Заключение

Аутентификация с помощью токенов — это одновременно мощный и гибкий метод аутентификации пользователей в веб-приложениях. Он обладает существенными преимуществами по сравнению с традиционными методами аутентификации, в число которых входит масштабируемость, безопасность и гибкость. Стандарты аутентификации токенов, такие как OAuth 2.0 и веб-токены JSON (JWT), получили широкое распространение и предлагают разработчикам надежный набор инструментов для создания безопасных и масштабируемых приложений.

Поскольку количество веб-приложений продолжает расти, аутентификация с помощью токенов будет продолжать играть важную роль в обеспечении безопасности и конфиденциальности данных пользователей.

Список литературы

1. A secure Token-based Communication for Authentication and Authorization Servers // ResearchGate URL: https://www.researchgate.net/publication/309365153_A_Secure_Token-Based_Communication_for_Authentication_and_Authorization_Servers (дата обращения: 23.01.2023).
2. What is a Token? What are its Pros and Cons? // loginradius URL: https://www.loginradius.com/blog/identity/pros-cons-token-authentication/ (дата обращения: 02.02.2023).
3. OAuth 2.0 // OAuth 2.0 URL: https://oauth.net/2/ (дата обращения: 04.02.2023).
4. JSON Web Token (JWT) // RFC Editor URL: https://www.rfc-editor.org/rfc/rfc7519 (дата обращения: 05.02.2023).

References

1. A secure Token-based Communication for Authentication and Authorization Servers // ResearchGate URL: https://www.researchgate.net/publication/309365153_A_Secure_Token-

Based_Communication_for_Authentication_and_Authorization_Servers (accessed: 23.01.2023).
2. What is a Token? What are its Pros and Cons? loginradius URL: https://www.loginradius.com/blog/identity/pros-cons-token-authentication/ (accessed: 02.02.2023).
3. OAuth 2.0 // OAuth 2.0 URL: https://oauth.net/2/ (accessed: 04.02.2023).
4. JSON Web Token (JWT) // RFC Editor URL: https://www.rfc-editor.org/rfc/rfc7519 (accessed: 05.02.2023).

Свищёв А. В., Кравцова Е. Ю. Анализ архитектурных шаблонов проектирования для конструирования программного обеспечения // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 4(30) с. 49–54

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.415.2

АНАЛИЗ АРХИТЕКТУРНЫХ ШАБЛОНОВ ПРОЕКТИРОВАНИЯ ДЛЯ КОНСТРУИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

[1]Свищёв А. В., [2]Кравцова Е. Ю.
МИРЭА - Российский технологический университет, Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: [1]svicshyov@mirea.ru, [2]9067320378@mail.ru

Данная статья дает представление о том, как выбираются архитектурные шаблоны проектирования с точки зрения конструирования программного обеспечения. С учетом всех существующих архитектурных шаблонов может быть трудно решить, какой именно выбрать. Даже если архитектурный шаблон описывает, в каких обстоятельствах его следует применять, это не обязательно приводит к тому, что он применяется, когда появляется такая возможность. Это может быть связано с факторами, которые гораздо более очевидны в процессе разработки, такими как: время, капитал и сложность реализации.

Ключевые слова: Архитектурные шаблоны проектирования, конструирования программного обеспечения, проектирование архитектуры.

ANALYSIS OF ARCHITECTURAL DESIGN PATTERNS FOR SOFTWARE DESIGN

[1] Svishchev A. V., [2] Kravtsova E. Y.
MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: [1]svicshyov@mirea.ru, [2]9067320378@mail.ru

This article provides insight into how architectural design patterns are chosen from a software design perspective. With all the existing architectural patterns available, it can be difficult to decide which one to choose. Even if an architectural template describes in what circumstances it should be applied, this does not necessarily result in it being applied when the opportunity arises. This may be due to factors that are much more obvious in the development process, such as: time, capital, and implementation complexity.

Keywords: Architectural design patterns, software design, architecture design.

В последние десятилетия программное обеспечение стало повсеместным. Почти все современные инженерные системы включают в себя важные программные подсистемы; это включает системы в транспортном, финансовом, образовательном, здравоохранительном, юридическом, военном и деловом секторах. Наряду с увеличением полезности программного обеспечения, его возможностей, стоимости и размера наблюдается соответствующий рост методов, моделей, инструментов, показателей и стандартов, поддерживающих разработку программного обеспечения.

Конструирование программного обеспечения — это процесс преобразования пользовательских требований в некоторую подходящую форму, которая помогает разработчику в написании кода и реализации программного обеспечения.

Для оценки требований пользователя создается документ SRS (Спецификация требований к программному обеспечению), тогда как для кодирования и реализации необходимы более конкретные и подробные требования с точки зрения программного обеспечения. Результат этого процесса можно напрямую использовать в реализации на языках программирования.

Конструирование программного обеспечения с использованием архитектурных шаблонов проектирования происходит в несколько этапов. Архитектурные шаблоны представляют собой обобщенные решения для повторяющихся проблем, возникающих при проектировании архитектуры программного обеспечения. Эти шаблоны помогают разработчикам структурировать и организовать код, обеспечивая масштабируемость, гибкость и поддерживаемость. Вот основные этапы конструирования программного обеспечения с использованием архитектурных шаблонов:

1. Анализ требований: сначала необходимо проанализировать требования к программному обеспечению и определить ключевые функциональные и нефункциональные характеристики. Это поможет определить, какие архитектурные шаблоны могут быть наиболее подходящими для проекта.

2. Выбор архитектурных шаблонов: на основе анализа требований выберите подходящие архитектурные шаблоны для вашего проекта. Некоторые распространенные архитектурные шаблоны включают Model-View-Controller (MVC), Model-View-ViewModel (MVVM). Выбор шаблона зависит от типа приложения, технологий и ожидаемой нагрузки.

3. Проектирование архитектуры: С использованием выбранных архитектурных шаблонов разработайте архитектуру вашего программного обеспечения. Определите основные компоненты, их взаимосвязи и обязанности. Убедитесь, что архитектура соответствует требованиям проекта и обеспечивает гибкость для изменений и масштабирования.

4. Реализация компонентов: на этапе реализации начните создавать компоненты программного обеспечения в соответствии с выбранными архитектурными шаблонами. Следуйте принципам разделения обязанностей, инкапсуляции, модульности и повторного использования кода.

В разработке программного обеспечения выделяют три уровня проектирования результатов:

Архитектурный дизайн (Architectural Design). Архитектурный дизайн является высшей абстрактной версией системы. Он идентифицирует программное обеспечение как систему со многими компонентами, взаимодействующими друг с другом. На этом уровне дизайнеры получают представление о предлагаемой области решения.

Высокоуровневый дизайн (High-level Design). Высокоуровневый дизайн разбивает концепцию архитектурного дизайна «единая сущность-множество компонентов» на менее абстрактное представление подсистем и модулей и изображает их взаимодействие друг с другом. Высокоуровневое проектирование фокусируется на том, как система вместе со всеми

ее компонентами может быть реализована в виде модулей. Он распознает модульную структуру каждой подсистемы, а также их взаимосвязь и взаимодействие друг с другом.

Детальный дизайн (Detailed Design). Детальный дизайн касается части реализации того, что рассматривается как система и ее подсистемы в предыдущих двух проектах. Это более подробно относится к модулям и их реализациям. Он определяет логическую структуру каждого модуля и их интерфейсы для связи с другими модулями.

Разобрав уровни проектирования (конструирования) программного обеспечения следующим этапом, производится анализ существующих архитектурных шаблонов проектирования:

Архитектурный шаблон — это высокоуровневый проект того, как элементы или компоненты взаимосвязаны. Он может показывать предопределенные подсистемы, их обязанности и их отношения между собой. Архитектурный шаблон является способом абстрагирования элементов и компонентов, чтобы систему было легче понять, смоделировать и описать. Не нужно показывать, как спроектирован каждый элемент или компонент, только то, как он может быть использован и для какой цели. Это похоже на класс в объектно-ориентированном программировании с публичным интерфейсом, в то время как частный интерфейс не показывается для внешнего мира.

MVC (Model-View-Controller) — является самым ранним архитектурным шаблоном, состоящий из трёх компонентов:

Model — известен как самый низкий уровень, что является базовой бизнес-логикой и данными;

View — компоненты интерфейса для отображения данных. Использует шаблон Observer для обновления модели и отображения обновленной модели при необходимости;

Controller — это компонент обеспечивающий взаимосвязь между оболочкой (View) и моделью (Model). Сюда сначала направляется ввод, который обрабатывает запрос через модель и передает его обратно в представление.

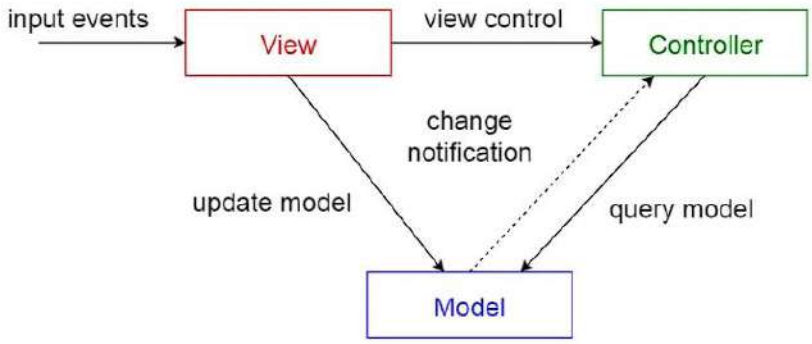


Рисунок 1 – MVC шаблон проектирования

Шаблон проектирования MVC позволяет разделить внешний и внутренний код на отдельные части, чтобы упростить обновление и масштабирование приложения без вмешательства или прерывания. Модель MVC также позволяет нескольким разработчикам одновременно работать над разными частями приложения. Однако существуют риски: представление модели для просмотра может вызвать проблемы с безопасностью и

производительностью. MVC распространен для веб-приложений, библиотек и пользовательских интерфейсов.

Pipe-filter pattern — шаблон, использующийся для структурирования систем, которые производят и обрабатывают поток данных. Каждый шаг обработки заключен в компонент фильтра . Данные для обработки передаются по каналам. Эти каналы можно использовать для буферизации или синхронизации.

Внедряют в рабочие процессы в биоинформатике. Последовательные фильтры выполняют лексический анализ, синтаксический анализ, семантический анализ и генерацию кода.

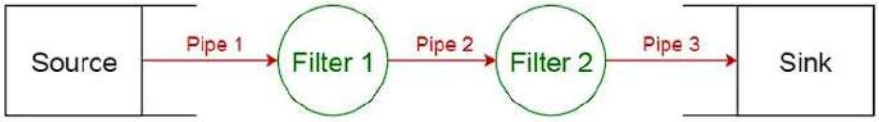


Рисунок 2 – Pipe-filter pattern шаблон проектирования

Данный шаблон позволяет разложить задачу, выполняющую сложную обработку, на ряд отдельных элементов, которые можно использовать повторно. Это может повысить производительность, масштабируемость и возможность повторного использования, позволяя независимо развертывать и масштабировать элементы задачи, выполняющие обработку.

Layered pattern (многоуровневая архитектура) — этот шаблон можно использовать для структурирования программ, которые можно разбить на группы подзадач, каждая из которых находится на определенном уровне абстракции. Каждый уровень предоставляет услуги следующему более высокому уровню.

- Уровень представления (также известный как уровень пользовательского интерфейса);
- Прикладной уровень (также известный как сервисный уровень);
- Уровень бизнес-логики (также известный как уровень домена);
- Уровень доступа к данным (также известный как уровень сохраняемости).

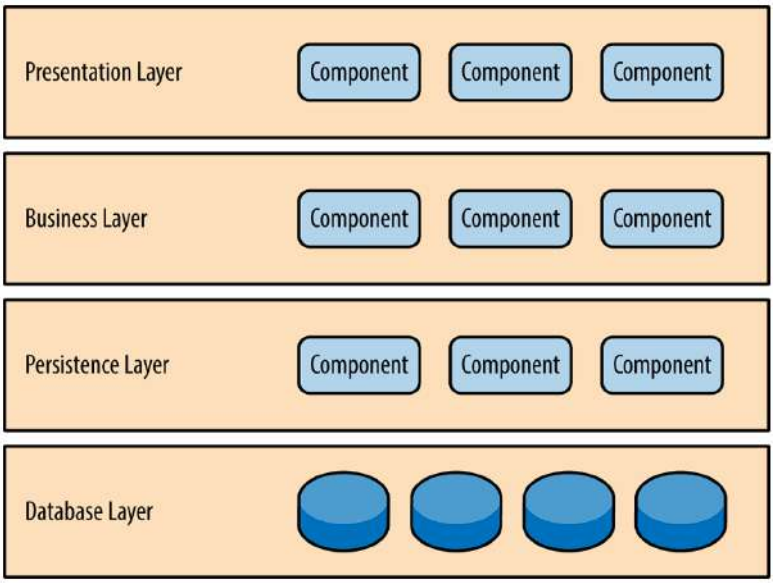


Рисунок 3 – Шаблон многоуровневой архитектуры

Одной из мощных особенностей шаблона многоуровневой архитектуры является разделение задач между компонентами. Компоненты внутри определенного уровня имеют дело только с логикой, относящейся к этому уровню. Например, компоненты на уровне представления имеют дело только с логикой представления, тогда как компоненты, находящиеся на бизнес-уровне, имеют дело только с бизнес-логикой. Этот тип классификации компонентов упрощает создание эффективных моделей ролей и ответственности в вашей архитектуре, а также упрощает разработку, тестирование, управление и обслуживание приложений с использованием этого архитектурного шаблона благодаря четко определенным интерфейсам компонентов и ограниченному объему компонентов.

Таблица 1 – Сравнение анализируемых архитектурных шаблонов

Шаблон	**Преимущества**	**Недостатки**
Layered pattern	Нижние компоненты могут использоваться более высокими. Внедрение компонентов упрощает стандартизацию, поскольку четко определяется уровень компонента. Изменения вносятся внутри компонента, не затрагивая другие	Не может быть универсальным решением
Pipe-filter pattern	Демонстрация параллельной обработки. Легко добавляемые фильтры. Возможность повторно использовать фильтры	Эффективность ограничивается самым медленным процессом фильтрации
MVC	Позволяет быстро создавать несколько представлений одной и той же модели. Отключение и подключение во время выполнения процессов	Может привести ко множеству ненужных обновлений для действий пользователя

Архитектурные шаблоны проектирования играют важную роль в разработке программного обеспечения, так как они предоставляют проверенные временем и обобщенные решения для ряда распространенных проблем, возникающих при проектировании архитектуры. Основываясь на опыте предыдущих проектов, архитектурные шаблоны помогают разработчикам создавать масштабируемые, гибкие и поддерживаемые системы.

Выводы, сделанные в результате исследования архитектурных шаблонов проектирования:

1. Обобщенные решения: Архитектурные шаблоны представляют собой обобщенные решения для типовых проблем, возникающих при проектировании архитектуры программного обеспечения.

2. Структура и организация: Шаблоны помогают структурировать и организовать код, что в свою очередь облегчает разработку, тестирование и поддержку системы.

3. Модульность и разделение обязанностей: Шаблоны обеспечивают разделение обязанностей между различными компонентами системы, что улучшает модульность и упрощает внесение изменений.

4. Повторное использование и стандартизация: Архитектурные шаблоны способствуют повторному использованию кода и стандартизации подходов к разработке, что может сократить время и усилия, затрачиваемые на проект.

5. Улучшение качества и снижение рисков: Применение проверенных архитектурных шаблонов может улучшить качество программного обеспечения и снизить риски, связанные с архитектурными решениями.

Однако важно помнить, что архитектурные шаблоны не являются универсальными решениями для всех ситуаций. При выборе и применении шаблонов необходимо учитывать контекст и требования конкретного проекта, а также возможные ограничения и компромиссы, связанные с использованием того или иного шаблона. Команда разработчиков должна убедиться, что, проведя анализ требований к разрабатываемому продукту полностью вписываются в выбранную архитектуру.

Список литературы

1. Байдыбеков А.А., Гильванов Р.Г., Молодкин И.А. Современные фреймворки для разработки WEB-приложений // Интеллектуальные технологии на транспорте. 2020. URL: https://cyberleninka.ru/article/n/sovremennye-freymvorki-dlya-razrabotki-web-prilozheniy (дата обращения: 28.03.2023).
2. Ихтиар В.Ф. Сравнение кросс-платформенных фреймворков // Вестник магистратуры. 2018. URL: https://cyberleninka.ru/article/n/sravnenie-kross-platformennyh-freymvorkov (дата обращения: 30.03.2023).
3. Бастрикина В.В. Сравнительный анализ адаптивных css фреймворков // Актуальные проблемы авиации и космонавтики. 2016. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-adaptivnyh-css-freymvorkov (дата обращения: 31.03.2023).

References

1. Baidybekov A.A., Gilvanov R.G., Molodkin I.A. Modern frameworks for WEB-applications development // Intelligent Technologies in Transport. 2020. URL: https://cyberleninka.ru/article/n/sovremennye-freymvorki-dlya-razrabotki-web-prilozheniy (accessed 28.03.2023).
2. Ikhtiar V.F. Comparison of cross-platform frameworks // Bulletin of Magistracy. 2018. URL: https://cyberleninka.ru/article/n/sravnenie-kross-platformennyh-freymvorkov (accessed: 30.03.2023).
3. Bastrykina V.V. Comparative analysis of adaptive css frameworks // Actual problems of aviation and cosmonautics. 2016. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-adaptivnyh-css-freymvorkov (accessed: 03/31/2023).

Хмелёв И.С. Анализ современных программных продуктов для тепловых и гидравлических расчётов тепловых сетей // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 55–58

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 62

АНАЛИЗ СОВРЕМЕННЫХ ПРОГРАММНЫХ ПРОДУКТОВ ДЛЯ ТЕПЛОВЫХ И ГИДРАВЛИЧЕСКИХ РАСЧЁТОВ ТЕПЛОВЫХ СЕТЕЙ

Хмелёв И.С.
ФГБОУ ВО "Самарский Государственный Технический Университет", Самара, Россия (443100, г. Самара, Молодогвардейская ул., д.244), e-mail: igori111@mail.ru

Рассмотрены ведущие программные продукты в сфере моделирования и расчёта тепловых сетей: ZuluThermo, CityCom, ИВК «АНГАРА-ТС». Приведена краткая характеристика данных программ, а также ключевые достоинства и недостатки, связанные с проведением тепловых и гидравлических расчётов.

Ключевые слова: Тепловая сеть, ZuluThermo, CityCom, ИВК «АНГАРА-ТС», гидравлический расчёт.

ANALYSIS OF MODERN SOFTWARE PRODUCTS FOR THERMAL AND HYDRAULIC CALCULATIONS OF THERMAL NETWORKS

Khmelev I.S.
Samara State Technical University, Samara, Russia (443100, Samara, Molodogvardeyskaya St., 244), e-mail: igori111@mail.ru

The leading software products in the field of modeling and calculation of thermal networks are considered: ZuluThermo, CityCom, IVK "ANGARA-TS". A brief description of these programs is given, as well as the key advantages and disadvantages associated with thermal and hydraulic calculations.

Keywords: thermal network, ZuluThermo, CityCom, IVK "ANGARA-TS", hydraulic calculation.

В настоящее время наблюдается активный рост цифровизации во всех сферах деятельности. В данном вопросе теплоснабжение тоже не стоит в стороне, разрабатываются программные комплексы для проектирования и моделирования систем теплоснабжения и процессов с ними связанных.

Рассмотрим, что из себя представляют некоторые из таких программных комплексов, основанных на геоинформационных системах (ГИС) и используемых для осуществления тепловых и гидравлических расчетов тепловых сетей. А также сформулируем их основные достоинства и недостатки.

Для рассмотрения были выбраны следующие ведущие в данной области программные продукты:

- ZuluThermo;
- CityCom;

- ИВК «АНГАРА-ТС».

ZuluThermo – это набор инструментов и программ российской разработки. Разработчиком и поставщиком данного программного комплекса является компания ООО «Политерм». Программное обеспечение ZuluThermo предназначено для выполнения гидравлических и тепловых расчётов тепловых сетей. Основой для работы является геоинформационная система ZuluGIS, назначение которой состоит в создании карт населенных пунктов, городов или отдельных районов. Также разработчиками была предусмотрена возможность загрузки существующих карт из некоторых популярных сервисов: 2ГИС, OpenStreetMap, Космоснимки СКАНЭКС [1].

Достоинства:

- Автоматическое построение пьезометрического графика по результатам проведенных расчетов;
- Позволяет рассчитывать тепловые сети любой сложности (действительно только в полной версии программы, в бесплатной версии количество рассчитываемых участков ограничено);
- Определение оптимальных гидравлических режимов;
- Массовое изменение параметров участков тепловой сети.

Недостатки:

- Ограничивается предустановленными схемами присоединения потребителей и центральных тепловых пунктов;
- Ограничивается стандартным набором элементов тепловых сетей;
- Для расчета доступны только стационарные режимы работы.

CityCom – это ещё один программный продукт российской разработки, развитием и распространением которого занимается компания ООО ИВЦ «Поток». Сейчас под общим брендом CityCom выпускается и регулярно усовершенствуется ряд отраслевых подсистем, одной из таких является CityCom-ТеплоГраф. Подсистема CityCom-ТеплоГраф представляет собой специализированную геоинформационную систему для создания электронных моделей тепловых сетей и решения производственных задач теплоснабжающих предприятий [2].

Достоинства:

- Детальная настройка топологической структуры связности сети, включая описание внутренних схем узлов тепловой сети [4];
- Расчет тепловых сетей большого объема и различной сложности;
- Возможность добавления новых элементов тепловой сети и схем присоединения потребителей и ЦТП сверх предустановленных.

Недостатки:

- Необходимость детальной настройки топологической структуры связности тепловой сети;
- Для осуществления тонкой настройки модели требуется привлечение сил технической поддержки разработчика программного обеспечения, без этого не удастся добиться максимальной точности теплогидравлического расчета;

- Отсутствует возможность массового редактирования параметров элементов тепловой сети (осуществляется по запросу в техподдержку, в рамках действующего договора технической поддержки ПО).

Можно заметь, что один и тот же пункт отнесен и к достоинствам, и недостаткам, это не ошибка. Дело в том, что запуск расчета будет невозможен до тех пор, пока не будут описаны внутренние схемы всех узлов, в особенности сложных узлов с большим количеством запорной арматуры и сложной схемой коммутации трубопроводов [4]. Но настолько детальная проработка модели требуется далеко не всегда, что предполагает лишние трудозатраты при решении определённых задач.

ИВК «АНГАРА-ТС» - это информационно-вычислительный комплекс, разработанный в лаборатории трубопроводных и гидравлических систем Института Систем Энергетики им. Л.А. Мелентьева [5] и предназначенный для моделирования трубопроводных инженерных систем различного назначения и тепловых сетей, в частности.

Достоинства:

- Автоматическое определение кратчайшей трассы между выбранными узлами сети;
- Определение отклонений параметров теплоносителя от допустимых значений;
- Расчет гидравлического режима осуществляется с изменяющимися расходами теплоносителя у потребителей;

Недостатки:

- Ограниченный пакет элементов тепловой сети;

Из описанных выше достоинств и недостатков стоит отметить главный положительный эффект от применения этих и аналогичных программных комплексов – это уменьшение временных затрат на проведение тепловых и гидравлических расчетов.

На основе изученных материалов о данных программных продуктах можно сделать вывод, что все они предлагают примерно одинаковый набор возможностей, но с некоторыми уникальными особенностями.

Список литературы

1. ZuluThermo – гидравлические расчеты тепловых сетей [Электронный ресурс] – Электрон. Текстовые дан. – Санкт-Петербург – Режим доступа: https://www.politerm.com/products/thermo/zuluthermo/
2. ИГС CityCom-ТеплоГраф – решение задач теплоснабжения [Электронный ресурс] – Электрон. Текстовые дан. – Москва – Режим доступа: https://www.citycom.ru/citycom/heatgraph/
3. В.С. Пузаков, В.В. Сущенко, К.В. Вялых, Н.Г. Петров, Е.Н. Антонов. Сравнение программных продуктов для создания электронных моделей систем теплоснабжения на примере поселений. Новости теплоснабжения №2 (210) 2018 г.
4. А.Р. Ексаев. Послесловие: Комментарии разработчика. Новости теплоснабжения №2 (210) 2018 г.
5. Ангара комплекс [Электронный ресурс] – Электрон. Текстовые дан. – Иркутск – Режим доступа: http://51.isem.irk.ru/angara/products.php
6. Новицкий Н.Н., Алексеев А.В., Токарев В.В. Комплексное развитие и применение информационных технологий для автоматизации процессов анализа и разработки

эксплуатационных режимов инженерных систем тепло- и водоснабжения. Известия вузов. Инвестиции. Строительство. Недвижимость. 2018;8(4):139–161. DOI: 10.21285/2227-2917-2018-4-139-161

7. *Для цитирования*: Новицкий Н.Н., Токарев В.В., Шалагинова З.И., Алексеев А.В., Гребнева О.А., Баринова С.Ю. Информационно-вычислительный комплекс «АНГАРА-ТС» для автоматизации расчета и анализа эксплуатационных режимов при управлении крупными многоконтурными системами теплоснабжения. Вестник Иркутского государственного технического университета. 2018;22(11):126–144. DOI: 10.21285/1814-3520-2018-11-126-144.

References

1. ZuluThermo – hydraulic calculations of thermal networks [Electronic resource] – Electron. Text data. – Saint Petersburg – Access mode: https://www.politerm.com/products/thermo/zuluthermo/
2. IGS CityCom-Teplograph – solution of heat supply problems [Electronic resource] – Electron. Text data. – Moscow – Access mode: https://www.citycom.ru/citycom/heatgraph/
3. V.S. Puzakov, V.V. Sushchenko, K.V. Vyalykh, N.G. Petrov, E.N. Antonov. Comparison of software products for creating electronic models of heat supply systems on the example of settlements. Heat Supply News No.2 (210) 2018
4. A.R. Exaev. Afterword: Developer's comments. Heat supply News No.2 (210) 2018
5. Angara complex [Electronic resource] – Electron. Text data. – Irkutsk – Access mode: http://51.isem.irk.ru/angara/products.php
6. Novitsky N.N., Alekseev A.V., Tokarev V.V. Complex development and application of information technologies for automation of processes of analysis and development of operational modes of engineering systems of heat and water supply. News of universities. Investment. Construction. Realty. 2018;8(4):139–161. DOI: 10.21285/2227-2917-2018-4-139-161
7. For citation: Novitsky N.N., Tokarev V.V., Shalaginova Z.I., Alekseev A.V., Grebneva O.A., Barinova S.Yu. Information and computing complex "ANGARA-TS" for automation of calculation and analysis of operational modes in the management of large Multi-circuit heating systems. Bulletin of Irkutsk State Technical University. 2018;22(11):126–144. DOI: 10.21285/1814-3520-2018-11-126-144.

Волохов Г.С. Работа с большими данными в медицинских организациях: проблемы и риски // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 59–63

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

РАБОТА С БОЛЬШИМИ ДАННЫМИ В МЕДИЦИНСКИХ ОРГАНИЗАЦИЯХ: ПРОБЛЕМЫ И РИСКИ

Волохов Г.С.
Общество с ограниченной ответственностью «САЛЮС», Архангельск, Россия (163071, г Архангельск, ул. Тимме Я., д. 25), e-mail: jbignef@gmail.com

С развитием информационных технологий и появлением большого объема данных в медицинской отрасли, возникают новые вызовы для медицинских организаций. Большие данные в медицине могут быть полезны для многих целей, таких как улучшение качества здравоохранения, повышение эффективности лечения и разработка новых методов диагностики. Однако, работа с большими данными также сопряжена с рисками и проблемами, которые медицинские организации должны учитывать.

Ключевые слова: Медицинские организации.

WORKING WITH BIG DATA IN MEDICAL ORGANIZATIONS: PROBLEMS AND RISKS

Volokhov G.S.
SALUS Limited Liability Company, Arkhangelsk, Russia (163071, Arkhangelsk, Timme Y. street, 25), e-mail: jbignef@gmail.com

With the development of information technologies and the emergence of a large amount of data in the medical industry, new challenges arise for medical organizations. Big data in medicine can be useful for many purposes, such as improving the quality of healthcare, improving the effectiveness of treatment and developing new diagnostic methods. However, working with big data also involves risks and challenges that medical organizations must take into account.

Keywords: Medical organizations.

1. Проблемы работы с большими данными в медицинских организациях.

1.1. Необходимость управления большими объемами данных.

Одной из основных проблем, связанных с работой с большими данными в медицинских организациях, является необходимость управления этими большими объемами данных. Каждый день больницы и другие медицинские учреждения генерируют огромное количество данных, включая медицинские записи, результаты тестов, сканирования и т.д. Управление этими данными может стать сложной задачей, особенно если учесть, что медицинские организации должны соблюдать строгие требования по конфиденциальности и защите персональных данных.

1.2. Недостаток квалифицированных специалистов по обработке данных.

Другой важной проблемой при работе с большими данными в медицинских организациях является недостаток квалифицированных специалистов по обработке данных. Для управления большими объемами данных необходимы специалисты, обладающие знаниями и навыками в области баз данных, анализа данных, статистики и машинного обучения. Однако, несмотря на растущий спрос на таких специалистов, рынок труда пока еще не насыщен.

1.3. Проблемы совместимости данных.

Еще одной проблемой, связанной с работой с большими данными в медицинских организациях, являются проблемы совместимости данных. Данные в медицинской индустрии часто хранятся в различных форматах, их необходимо объединять и интегрировать для обеспечения полного и точного анализа. Однако, это может быть сложной задачей, так как системы управления данными в различных медицинских учреждениях могут отличаться.

1.4. Проблемы конфиденциальности и безопасности данных.

Еще одной серьезной проблемой при работе с большими данными в медицинских организациях являются проблемы конфиденциальности и безопасности данных. Медицинские данные содержат конфиденциальную информацию, которая может быть использована в нежелательных целях. Поэтому необходимо принимать меры по обеспечению безопасности данных, чтобы предотвратить утечки информации или несанкционированный доступ к ней.

2. Риски работы с большими данными в медицинских организациях:

- Нарушение конфиденциальности: Работа с большими данными в медицинских организациях может привести к нарушению конфиденциальности пациентов, если данные не будут защищены должным образом.
- Риск ошибок в принятии решений: Работа с большими данными может привести к принятию неправильных решений, если данные не будут интерпретированы правильно.
- Недостаточная защита от кибератак: Большие данные в медицине могут быть объектом кибератак, которые могут привести к утечке конфиденциальной информации, внедрению вредоносных программ и нарушению работы медицинских систем [1].

3. Меры по управлению рисками при работе с большими данными в медицинских организациях

- Обучение персонала: Медицинские организации должны обучать свой персонал правилам обработки больших данных и мерам безопасности, чтобы предотвратить ошибки и утечки данных.
- Защита данных: Медицинские организации должны использовать соответствующие технологии и методы для защиты конфиденциальной информации пациентов.
- Проверка качества данных: Медицинские организации должны использовать проверенные методы для обеспечения качества данных, включая проверку на ошибки и неточности.
- Создание системы контроля и управления рисками: Медицинские организации должны создавать систему контроля и управления рисками для работы с большими данными, включая мониторинг защиты данных и предотвращение нарушений [2].

4. Примеры решений для работы с большими данными в медицинских организациях

4.1. Использование систем управления данными.

Использование систем управления данными (СУД) является распространенной практикой в медицинских организациях для обработки больших объемов информации и обеспечения безопасности

данных. Эти системы позволяют эффективно управлять, хранить, обрабатывать и анализировать медицинские данные, такие как результаты тестов, история болезней, рецепты и другие [3].

Преимущества использования СУД в медицинских организациях включают:

- Улучшенная безопасность данных: СУД обеспечивают защиту медицинских данных от несанкционированного доступа, взломов и других угроз безопасности.
- Улучшенный доступ к информации: СУД позволяют медицинским работникам быстро получать доступ к необходимой информации о пациентах, что повышает качество медицинского обслуживания.
- Улучшенная эффективность: СУД позволяют медицинским работникам эффективнее управлять и обрабатывать медицинские данные, что позволяет сократить время, затрачиваемое на рутинные задачи.
- Улучшенный анализ данных: СУД позволяют медицинским работникам анализировать большие объемы медицинских данных для выявления тенденций и паттернов, что помогает улучшить процессы лечения и предотвращать заболевания.

4.2. **Использование аналитических инструментов.**

Использование аналитических инструментов является важной практикой в медицинских организациях для анализа больших объемов данных и выявления тенденций в здравоохранении. Эти инструменты позволяют медицинским организациям использовать данные, которые они уже имеют, для выявления тенденций и обнаружения новых путей для улучшения качества медицинского обслуживания.

Преимущества использования аналитических инструментов в медицинских организациях включают:

- Выявление тенденций и паттернов: Аналитические инструменты позволяют медицинским организациям анализировать большие объемы данных для выявления тенденций и паттернов, что помогает улучшить процессы лечения и предотвращать заболевания.
- Оптимизация использования ресурсов: Аналитические инструменты помогают медицинским организациям оптимизировать использование своих ресурсов, таких как оборудование и персонал, что позволяет повысить эффективность и снизить затраты.
- Улучшение качества медицинского обслуживания: Аналитические инструменты позволяют медицинским организациям определять, какие методы лечения наиболее эффективны, что помогает улучшить качество медицинского обслуживания.
- Предотвращение ошибок: Аналитические инструменты помогают медицинским организациям выявлять ошибки в медицинских данных и процессах, что помогает предотвратить потенциальные проблемы и повысить качество медицинского обслуживания.

4.3. Использование искусственного интеллекта.

Использование искусственного интеллекта (ИИ) в медицинских организациях становится все более распространенным для анализа больших объемов данных и принятия решений в здравоохранении. ИИ может использоваться для различных задач, от обработки и анализа медицинских данных до управления медицинскими устройствами и разработки новых лекарств.

Преимущества использования ИИ в медицинских организациях включают:

- Улучшение точности диагностики: ИИ может помочь врачам улучшить точность диагностики, используя анализ больших объемов данных и различные алгоритмы машинного обучения для выявления скрытых паттернов и зависимостей.

- Улучшение планирования лечения: ИИ может помочь медицинским организациям оптимизировать планирование лечения, учитывая данные о состоянии пациента, его медицинской истории и других факторах.
- Разработка новых лекарств: ИИ может использоваться в процессе разработки новых лекарств для ускорения и улучшения процесса [4-6].

Заключение.

Работа с большими данными в медицинских организациях может привести к многим проблемам и рискам, но при правильном подходе может также привести к улучшению качества здравоохранения и повышению эффективности лечения. Медицинские организации должны принимать меры по управлению рисками и использовать проверенные методы для обеспечения безопасности больших данных, таких как шифрование, аутентификация и авторизация пользователей, резервное копирование данных и мониторинг доступа к данным. Они также должны соблюдать соответствующие законодательные и регуляторные требования по обработке персональных данных.

В целом, работа с большими данными в медицинских организациях может быть сложной и вызывать много вопросов, но она является важным шагом в улучшении качества здравоохранения и обеспечении лучшего доступа к медицинской информации. Правильное управление рисками и использование соответствующих методов обеспечения безопасности данных могут помочь медицинским организациям получить максимальную выгоду от использования больших данных и добиться наилучших результатов в лечении и уходе за пациентами.

Список литературы

1. "Большие данные в медицине: проблемы и перспективы использования" / Под ред. О.В. Лазаревой, И.И. Брюханова. - М.: ГЭОТАР-Медиа, 2018. - 264 с.
2. "Анализ больших данных в медицине: современные технологии и перспективы" / Под ред. А.В. Крыловой. - М.: Издательство "Лань", 2016. - 224 с.
3. "Большие данные в медицинских исследованиях" / Под ред. Ю.В. Николаева, А.С. Медведева, А.Н. Колесникова. - М.: Издательство "Медицина", 2019. - 272 с.
4. "Big Data in Healthcare: From Diagnosis to Personalized Medicine" / Edited by A. Holzinger. - Cham: Springer, 2015. - p.320
5. "Data-Driven Healthcare: How Analytics and BI are Transforming the Industry" / Edited by L. Dunlop, R. Hayes. - Hoboken: Wiley, 2014. - p.288
6. "Big Data Analytics in Healthcare" / Edited by K. Elmagarmid, S. Fedorowicz, A. Saad. - Boca Raton: CRC Press, 2014. - p. 440

References

1. "Big data in medicine: problems and prospects for use" / Ed. O.V. Lazareva, I.I. Bryukhanov. - M.: GEOTAR-Media, 2018. - p.264
2. "Big data analysis in medicine: modern technologies and perspectives" / Ed. A.V. Krylova. - M.: Publishing house "Lan", 2016. - p.224
3. "Big data in medical research" / Ed. Yu.V. Nikolaeva, A.S. Medvedev, A.N. Kolesnikov. - M.: Publishing house "Medicine", 2019. - p.272
4. "Big Data in Healthcare: From Diagnosis to Personalized Medicine" / Edited by A. Holzinger. - Cham: Springer, 2015. - p.320
5. "Data-Driven Healthcare: How Analytics and BI are Transforming the Industry" / Edited by L. Dunlop, R. Hayes. - Hoboken: Wiley, 2014. - p.288

6. "Big Data Analytics in Healthcare" / Edited by K. Elmagarmid, S. Fedorowicz, A. Saad. - Boca Raton: CRC Press, 2014. - p.440

Минитаева А.М., Соколов А.В. Способы и виды инфицирования компьютера загрузочными вирусами // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 64–69

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.49

СПОСОБЫ И ВИДЫ ИНФИЦИРОВАНИЯ КОМПЬЮТЕРА ЗАГРУЗОЧНЫМИ ВИРУСАМИ

[1]Минитаева А.М., [2]Соколов А.В.
ФГБОУ ВО "Московский Государственный Технический Университет имени Н.Э. Баумана (Национальный Исследовательский Университет), Москва, Россия (105005, Москва, 2-Я Бауманская ул, д. 5 стр. 1), e-mail: [1]minitaeva@bmstu.ru, [2]andrey.sokolov515@gmail.com

Компьютерные вирусы могут вызывать программные и аппаратные сбои в работе ПК, уничтожать или похищать хранимую на них информацию. Также они могут блокировать работу пользователей, разрушать структуру размещения данных. Они потребляют ресурсы системы и захватывают место на накопителях информации, ухудшают функционирование ПК. В статье рассматриваются виды и способы заражения загрузочными компьютерными вирусами, которые направлены на различные системные области. Представлено описание и характер их воздействия на систему. Результаты анализа и приведенные виды инфицирования являются необходимыми для последующего предотвращения заражения.

Ключевые слова: Загрузочный вирус, главная загрузочная запись, система, инфицирование, сектор.

WAYS AND TYPES OF INFECTING A COMPUTER WITH BOOT VIRUSES

[1]Minitaeva A.M., [2]Sokolov A. V.
Bauman Moscow State Technical University (National Research University), Moscow, *Russia (*105005, *Moscow, 2nd Baumanskaya street, 5 bldg.* 1*), e-mail: [1]minitaeva@bmstu. ru, [2]andrey. sokolov515@gmail. com*

Computer viruses can cause software and hardware malfunctions on PCs and destroy or steal information stored on them. They can also block the user's work and disrupt the data layout. They consume system resources and take up storage space and impair the functioning of a PC. The article discusses the types and methods of infection by bootable computer viruses, which target different system areas. A description and the nature of their impact on the system is presented. The results of the analysis and the types of infection given are essential for the subsequent prevention of infection.

Keywords: Boot virus, master boot record, system, infection, sector.

Введение

Первыми известными успешными компьютерными вирусами были вирусы загрузочного сектора. В 1986 году два пакистанских брата на IBM PC создали первый такой вирус под названием Brain.

В настоящее время методика заражения при загрузке используется редко. Тем не менее, следует ознакомиться с загрузочными вирусами, поскольку они могут заразить компьютер независимо от установленной на нем фактической операционной системы.

1. Вирусы загрузочного типа

Загрузочные вирусы – это наиболее опасный вид вредоносных программ. В отличие от файловых вирусов они записывают свой код не в файлы, а в загрузочный сектор накопителя информации, изменяя программу начальной загрузки, которая должна была загрузить саму операционную систему и передать ей управление.

Вирусы загрузочного сектора используют процесс загрузки персональных компьютеров (ПК). Поскольку большинство компьютеров не содержат операционной системы (ОС) в своей постоянной памяти (ПЗУ), им необходимо загружать систему откуда-то еще, например, с диска или из сети (через сетевой адаптер) [1].

Типичный диск IBM PC состоит из четырех разделов, которым в нескольких операционных системах, таких как MS-DOS и Windows NT, присвоены логические буквы, обычно C:, D: и так далее. Большинство компьютеров используют только два из этих разделов, к которым можно легко получить доступ.

Некоторые поставщики компьютеров, такие как COMPAQ и IBM, часто используют скрытые разделы для хранения на диске дополнительных средств настройки BIOS. Скрытые разделы не имеют назначенных им логических имен, что затрудняет доступ к ним.

Обычно ПК загружают ОС с жесткого диска. Однако в ранних системах порядок загрузки нельзя было определить, и поэтому машина загружалась с дискеты, что давало большие возможности для загрузки компьютерных вирусов до загрузки ОС. ROM-BIOS считывает первый сектор указанного загрузочного диска в соответствии с настройками порядка загрузки в настройках BIOS, в случае успеха сохраняет его в памяти по адресу 0:0x7C00 и запускает загруженный код.

В более новых системах каждый раздел делится на дополнительные разделы. Диск всегда делится на головки, дорожки и сектора. Основная загрузочная запись (MBR) расположена в головке 0, дорожке 0, секторе 1, который является первым сектором на жестком диске. MBR содержит общий, специфичный для процессора код для поиска активного загрузочного раздела из записей таблицы разделов (TP). TP хранится в области данных MBR. В начале MBR находится небольшой код, который часто называют загрузчиком начальной загрузки.

Каждая запись PT содержит следующее:

- адреса первого и последнего секторов раздела
- флаг - всякий раз, когда раздел является загрузочным
- байт типа
- смещение первого сектора раздела от начала диска в секторах
- размер раздела в секторах.

Загрузчик находит активный раздел и загружает его первый логический сектор в качестве загрузочного. Загрузочный сектор содержит код, специфичный для ОС. MBR — это код общего назначения, не связанный с какой-либо ОС. Таким образом, IBM PC могут легко

поддерживать более одного раздела с различными типами файловых систем и операционных систем. Это также делает работу компьютерных вирусов очень простой.

Код MBR может легко заменяться кодом вируса, который загружает исходную MBR после себя и остается в памяти, в зависимости от установленной операционной системы. В случае с MS-DOS загрузочные вирусы могут легко оставаться в памяти и на лету заражать другие вставленные носители. Некоторые загрузочные вирусы, такие как Exebug, всегда заставляют компьютер сначала загружать их в систему, а затем самостоятельно завершать процесс загрузки. Exebug изменяет настройки CMOS в BIOS, чтобы обмануть ПК, заставив его думать, что у него нет дисковода для гибких дисков. Таким образом, ПК сначала загрузится с зараженной MBR. При запуске вирус (с жесткого диска) проверяет, есть ли дискета в дисководе A:, и если есть, загружает загрузочный сектор дискеты и передает ему управление. Таким образом, когда происходит загрузка с дискеты, вирус может заставить поверить, что загрузка действительно произошла с дискеты, но на самом деле это не так.

В случае гибких дисков загрузочным сектором является первый сектор дискеты. Загрузочная запись содержит имена файлов для загрузки, характерные для ОС, например IBMBIO.COM и IBMDOS.COM [2]. Желательно настроить процесс загрузки таким образом, чтобы сначала загружаться с жесткого диска. В IBM PC первого поколения процесс загрузки не был разработан таким образом, поэтому всякий раз, когда дискета оставалась в дисководе A:, ПК пытался загрузиться с нее. Загрузочные вирусы воспользовались этой ошибкой проектирования.

2. Методы заражения основной загрузочной записи

Заражение MBR — относительно тривиальная задача для вирусов. Размер MBR составляет 512 байт. Туда влезает только короткий код, но для небольшого вируса его более чем достаточно. Обычно MBR заражается сразу после загрузки с зараженной дискеты в дисководе A.

2.1. Заражение MBR путем замены кода начальной загрузки

Классический тип MBR-вирусов использует дисковую процедуру INT 13h BIOS для доступа к дискам для чтения и записи. Большинство вирусов MBR заменяют загрузочный код в начале MBR своей собственной копией и не изменяют TP. Это важно, поскольку доступ к жесткому диску возможен только при загрузке с дискеты, когда ПТ находится на месте. В противном случае DOS не сможет найти данные на диске.

Вирус Stoned является типичным примером этой техники. Вирус сохраняет исходную MBR в секторе 7, как показано на Рисунке 1. После того, как вирус получает управление через замененную MBR, он считывает сохраненную MBR, расположенную в 7-м секторе памяти, и передает ему управление. Пара пустых секторов обычно доступна после MBR, и Stoned этим пользуется. Однако это условие не может быть выполнено на 100%, и именно поэтому некоторые вирусы MBR делают систему не загружаемой после заражения.

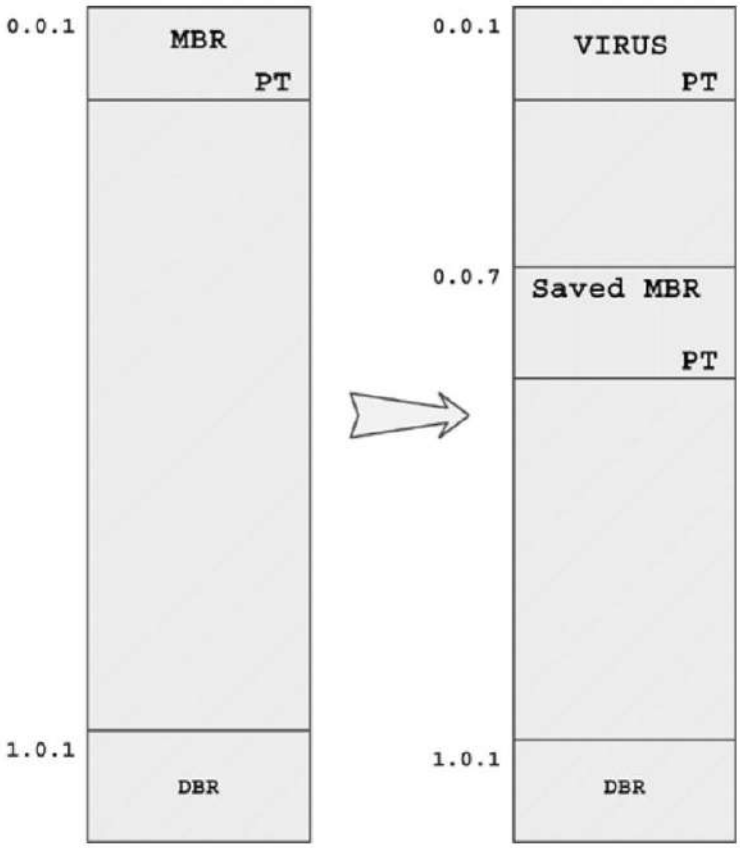


Рисунок 1 – Типичная схема диска до и после заражения Stoned

2.2. Замена кода главной загрузочной записи без его сохранения

Другой способ заражения MBR вирусами заключается в перезаписывании загрузочного кода, оставляя записи TP на месте, но нигде не сохраняя исходную MBR. Такие вирусы выполняют функцию исходного кода MBR. В частности, они ищут активный раздел, загружают его и передают ему управление после себя.

Одним из первых вирусов, использовавших этот метод, был Azusa, обнаруженный в январе 1991 года в Онтарио, Канада [3]. Такие вирусы нельзя вылечить штатными методами, потому что исходная копия MBR нигде не хранится. Антивирусные компании быстро отреагировали на эту угрозу, придумав единый код MBR. Для лечения этот универсальный код MBR был использован для перезаписи кода вируса.

2.3. Сохранение MBR в конец жесткого диска

Распространенный метод заражения MBR — полная замена MBR и сохранение оригинала в конце жесткого диска в надежде, что его там ничего не перезапишет. Некоторые из наиболее осторожных вирусов уменьшают размер раздела, чтобы гарантировать, что эта область диска не будет перезаписана снова. Многокомпонентный вирус Tequila использует эту технику.

3. Методы заражения DOS BOOT Record (DBR)

Вирусы загрузочного сектора заражают первый сектор, загрузочный сектор дискеты. При желании они также могут поражать загрузочные сектора жесткого диска. Существует большое количество известных методов заражения загрузочных секторов. Речь пойдет о самых основных.

3.1. Стандартный метод заражения при загрузке

Один из наиболее часто используемых методов заражения при загрузке был разработан для таких вирусов, как Stoned [4]. Stoned заражает загрузочный сектор дискеты, заменяя 512-байтный загрузочный сектор собственной копией и сохраняя оригинал в конец корневого каталога.

На практике этот метод в большинстве случаев безопасен, но может произойти случайное повреждение содержимого дискеты, если в каталоге дискеты хранится слишком много имен файлов. В таком случае содержимое исходного сектора может перезаписать содержимое каталога.

3.2. Загрузочные вирусы, форматирующие лишние сектора

Некоторые загрузочные вирусы просто слишком велики, чтобы поместиться в одном секторе. Большинство дискет можно отформатировать для хранения большего количества данных, чем их фактический форматированный размер. Не все дисководы гибких дисков поддерживают форматирование дополнительных секторов, но многие имеют это свойство.

Программное обеспечение для защиты от копирования часто использует специально отформатированные «лишние» сектора дискеты, расположенные за пределами обычных диапазонов. В результате обычные инструменты копирования дискет, такие как DISKCOPY, не могут создать идентичную копию таких дискет [5].

Некоторые вирусы специально форматируют набор дополнительных секторов дискеты, чтобы антивирусной программе было труднее получить доступ к исходной копии во время восстановления. Однако обычно дополнительные сектора используются для того, чтобы освободить больше места для более крупного тела вируса.

Заключение

Загрузочные вирусы действуют глубоко внутри компьютера на уровне Master Boot Record (MBR). При запуске электронное устройство действует согласно прописанному в БИОС протоколу. Там ему указывается, какую информацию показать первой, и обычно в приоритетах операционная система. Вирус меняет этот параметр. В итоге вирус загружается первым и может даже уничтожить файлы на жестком диске. Таким образом данный тип вредоносных носителей является одним из самых опасных для информационных систем.

Список литературы

1. Петер С. Искусство нахождения и защиты от компьютерных вирусов. 2005. С. 108-111.
2. Константин К. Компьютерные вирусы и антивирусы: взгляд программиста. 2018. С. 49-60.
3. Усманов А. А. Простые эффективные способы максимальной защиты компьютера от вирусов. 2019. С. 3-7.

4. Блазуцкая Е.Ю., Шарафутдинов А.Г. Вирусы нового поколения и антивирусы. 2015. Т. 1. № 35. С. 92-94.
5. Жуков Д.О. Модели различных стратегий распространения вирусов в компьютерных сетях. 2013. С. 113.

References

1. Peter Szor The art of computer virus research and defense. 2005. pp. 108-111.
2. Konstantin K. Computer viruses and antiviruses: a programmer's view. 2018. pp. 49-60.
3. Usmanov A. A. Simple tests of computer virus protection. 2019. pp. 3-7.
4. Blazutskaya E.Y., Sharafutdinov A.G. New Generation Viruses and Antiviruses. 2015. T. 1. No. 35. pp. 92-94.
5. Zhukov D.O. Models of different strategies of virus spreading in computer networks. 2013. pp. 113.

Кулаков К.А., Торосян Л.Е. Обзор перспективы внедрения беспилотных грузовых автомобилей в массовую эксплуатацию // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 70–77

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 623.746.4-519

ОБЗОР ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ БЕСПИЛОТНЫХ ГРУЗОВЫХ АВТОМОБИЛЕЙ В МАССОВУЮ ЭКСПЛУАТАЦИЮ

[1]Кулаков К.А., [2]Торосян Л.Е.
ФГБОУ ВО "Санкт-Петербургский Государственный Архитектурно-Строительный Университет", Санкт-Петербург, Россия (190005, г. Санкт-Петербург, 2-я Красноармейская ул., д.4), e-mail: [1]kulakovkirill@list.ru, [2]levantor@mail.ru

В данной научной статье рассматриваются перспективные внедрения беспилотных грузовых автомобилей. Описывается классификация процессов автоматизации автомобилей. Также приведена конструкция беспилотных автомобилей и алгоритм работы системы автоматизации.

Ключевые слова: Автомобилестроение, электроавтомобили, беспилотные грузовые автомобили, искусственный интеллект.

OVERVIEW OF PROMISING IMPLEMENTATIONS OF UNMANNED TRUCKS IN MASS OPERATION

[1]Kulakov K.A., [2]Torosyan L.E.
FSBEI of HE "St. Petersburg State University of Architecture and Civil Engineering", St. Petersburg, Russia (190005, St. *Petersburg, 2nd Krasnoarmeyskaya St., 4), e-mail: [1]kulakovkirill@list. ru, [2]levantor@mail. ru*

This scientific article discusses the promising introduction of unmanned trucks. The classification of car automation processes is described. The design of unmanned vehicles and the algorithm of the automation system are also given.

Keywords: Automotive industry, electric vehicles, unmanned trucks, artificial intelligence.

В ноябре 2018 года Премьер-министр РФ подписал постановление об использовании на дорогах беспилотных автомобилей. Опыт начался с 1 декабря в Москве и Татарстане. Участники опыта по тестированию беспилотных автомобилей (БПА) должны были получить одобрение Государственного научного центра ФГУП «НАМИ» (ГНЦ РФ ФГУП «НАМИ») [11]. Одно из главных условий к участникам опыта было страхование ответственности.

Актуальность и перспектива эксплуатации БПА вызывает интерес у транспортно-логистических компаний, так как предполагает возможное увеличение производительности труда и оптимизацию расходов, а также повышение технологического уровня и качества перевозочного процесса.

Разработкой БПА занимаются как IT-компании, так и крупные автомобильные заводы-производители. Но насколько разными получаются их результаты? Рассмотрим, действительно ли концепции различных производителей отличаются друг от друга.

Для начала надо рассмотреть, что собой представляет беспилотный автомобиль. Беспилотный автомобиль представляет собой транспортное средство, которое оборудовано системой автоматического управления, с возможностью передвигаться без участия человека.

Для данного беспилотного автомобиля программное обеспечение включает машинное зрение нейросети.

Машинное зрение – по-другому называется лидарами. Лидары расшифровывается как «Light Detectionand Ranging» (другими слова – это обнаружение и определение дальности светового источника). Они основаны на сенсорной технологии. Также машинное зрение создает карту окружающей среды вокруг устройства (Рисунок 1).

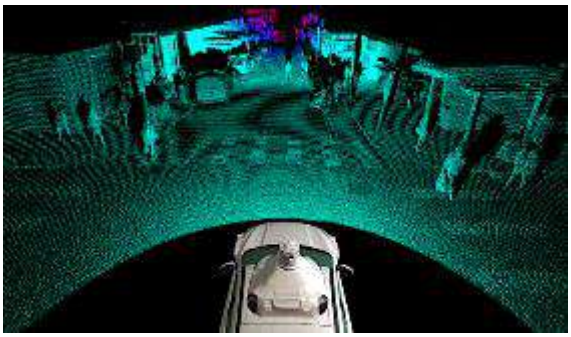


Рисунок 1 – Устройство лидара

Лидарные датчики излучают не только инфракрасный свет, но и измеряют время. Это нужно для того, чтобы свет отразился от объекта и вернулся обратно к датчику, тем самым создавая трёхмерную карту.

Существуют различные типа лидаров.

Первый тип – это лидар времени полёта (ToF); второй - лидар непрерывной волны с частотной модуляцией (FMCW).

Оба типа выполняют одну и ту же функцию, но каждый тип лидара имеет свои преимущества и недостатки.

Первый тип является наиболее распространённой формой лидара на транспортных средствах. Тип ToF отображает своё окружение путём измерения импульсов или фотонов света, которые он посылает и принимает обратно отражёнными от объекта. Данный тип имеет диапазон 360 градусов, что позволяет одному устройству выполнять эту работу. Второй тип лидара (FMCW) вместо импульсов посылает непрерывный поток света. Такой тип лидара, в отличие от первого типа, имеет недостаток, а именно - ограниченное поле зрения, поэтому на автомобиле их нужно несколько.

Карта, которая создана датчиком лидара, очень важна для самоуправляемого транспортного средства, потому что она помогает автомобилю «видеть» окружающий мир. В отличие от других решений (таких как радары и камеры) указанная технология обеспечивает большую глубину и детализацию.

Нейросети – это различные варианты сенсоров, т.е. камеры, лидары, радары и ультразвуковые датчики. Нейронные сети обрабатывают и подают данные с этих датчиков, чтобы сформировать основу событий, встречающихся на дороге.

Нейронные сети отвечают за распознавание важных объектов инфраструктуры и ситуаций, таких как светофоры, разметка, знаки и внезапно, появляющиеся на дороге люди.

Нейросети выделяют значимые объекты из дорожной среды и направляют автомобиль на реагирование, например, замедляя движение на пешеходных переходах (Рисунок 2).

Рисунок 2 – Принцип работы нейросетей

Нейросети начинаются с датасетов. Датасеты — это наборы данных информации, которые используются для обучения нейросетей. Данные с камер (лидаров), которые могут принимать форму фотографий или облаков точек лидара.

Некоторые системы полагаются на инфраструктурные системы (например, встроенные в дорогу или около неё). Современные и развитые технологии могут имитировать присутствие человека на уровне принятия решений об изменении положения руля и скорости, с помощью набора камер, сенсоров, радаров, лидаров и спутниковых навигационных систем.

Общие принципы работы у всех БПА примерно одинаковы. Рассмотрим классический проект беспилотного автомобиля. Сенсоры (perception) собирают информацию об окружающем мире, затем передают её в компонент системы управления (motion planning). На основе этой информации указанный компонент планирует действия, а также данных карт и локализации. После motion planning передаёт принятые решения компоненту «управление автомобилем» (vehicle control), который направляет его по заданной траектории.

Благодаря специальному программному обеспечению (ПО) и сенсорам БПА способны передвигаться самостоятельно. ПО управляет работой всех систем автомобиля, таких как рулевое управление, переключение передач, системы газа и тормозом. Датчики собирают информацию об окружающей обстановке, на основе которой строится работа автомобиля.

Современные беспилотные транспортные средства используют алгоритмы на основе метода Байеса для одновременного определения местоположения и составления карты. Принцип алгоритма заключается в объединении данных от датчиков автомобиля с данными карты (автономный режим).

Классификация процессов автоматизации автомобилей разработана «Сообществом автомобильных инженеров (SAE)» и содержит шесть уровней [7]. Перечислим их:

- Уровень 0. Данный уровень не имеет никакой автоматизации, и всю работу выполняет водитель.
- Уровень 1 называется «Hands on», «Помощь водителю». В данном уровне водитель и система управляют автомобилем вместе. Например: водитель управляет автомобилем, а система регулирует мощность двигателя для поддержания заданной

скорости и, при необходимости, снижает скорость для сохранения дистанции (адаптивный круиз-контроль). В других случаях, например, при автоматической парковке, водитель сам определяет скорость и автоматически управляет автомобилем.

- Следующий уровень 2 называется «Hands off», «Частичная автоматизация». Система полностью контролирует и управляет автомобилем, выполняет ускорение, торможение и рулевое управление. Функция водителя - следить за ездой и быть готовым вмешаться в любой момент, если система не сможет правильно отреагировать. Однако, несмотря на название «Hands off», такие системы часто требуют, чтобы водитель держал руки на руле в качестве доказательства своего намерения вмешаться.
- Уровень 3. «Eyes off», «Условная автоматизация». Это когда от водителя не требуется немедленной реакции. Он может, например, писать сообщения или смотреть фильм. Система сама реагирует на ситуации, требующие немедленной реакции, например, экстренное торможение. От водителя требуется готовность вмешаться в течение какого-то ограниченного времени, установленного производителем.
- Четвертый уровень «Mind off», «Широкая автоматизация», в отличие от третьего уровня, не требует постоянного внимания водителя. Например, водитель может лечь спать или покинуть свое водительское место. Полностью автоматизированное вождение происходит только в определенных пространственных зонах (геозонах) или в определенных ситуациях, например, в пробках. За пределами таких зон или ситуаций система может прекратить движение и припарковать автомобиль, если водитель не контролирует ситуацию.
- Уровень 5. «Steering wheel optional», «Полная автоматизация». На данном уровне не требуется никакого человеческого вмешательства.

Тестирование беспилотных автомобилей происходит в различных режимах. Традиционно режимы делятся на три основные категории:

- Тестирование алгоритмов в виртуальном симуляторе;
- Тестирование на закрытых треках и полигонах;
- Тестирование на дорогах общего пользования.

Первым шагом для проверки обновлений системы беспилотного управления является *виртуальное моделирование.* Данный вид тестирования обходится компаниям дешевле, чем другие виды тестирования с использованием настоящих автомобилей и водителей. Некоторые компании, например, Aurora, проводят большую часть своих испытаний в виртуальной среде. С другой стороны, многие утверждают, что имитационное тестирование не следует переоценивать. Причина в том, что дорожные и погодные условия, с которыми беспилотный автомобиль может столкнуться на дороге, невозможно идеально воспроизвести в лабораторных условиях. Это может быть не так важно при создании базовых сценариев на ранних стадиях разработки, но становится необходимым на последних стадиях. Моделирование также не позволяет проверить конструкторские и технологические решения, поведение датчиков и взаимодействие системы автопилота с блоками управления автомобиля.

Следующая рассматриваемая группа – это *испытания в закрытых помещениях.* Беспилотные транспортные средства испытываются до того, как они выйдут на открытую дорогу. Испытательные полигоны позволяют проверить то, что невозможно проверить на симуляторе (например, работу сенсоров (датчиков), качество сборки автомобиля), а также отработать основные дорожные сценарии. Будущие водители беспилотных автомобилей также могут пройти подготовку на испытательных полигонах.

Последняя группа, и самый важный этап для развития технологии – это *тестирование на дорогах общего пользования.* Беспилотные транспортные средства будут сталкиваться с самыми разными дорожными условиями, которые трудно воспроизвести в симуляторах или на испытательных треках. Основное внимание уделяется взаимодействию с пешеходами, велосипедистами и другими водителями на дорогах, которые не всегда соблюдают правила дорожного движения.

Конструкция беспилотных автомобилей включают в себя [1]:

- Датчики температуры, нагрузки на ось, давления, температуры в шинах, уровня топлива и открытия дверей;
- GPS/GSM антенна;
- Трекер, дисплей, модуль управления, видеорегистратор, TPMS, камера заднего вида.

Алгоритм работы системы и конструкции беспилотного автомобиля (Рисунок 3).

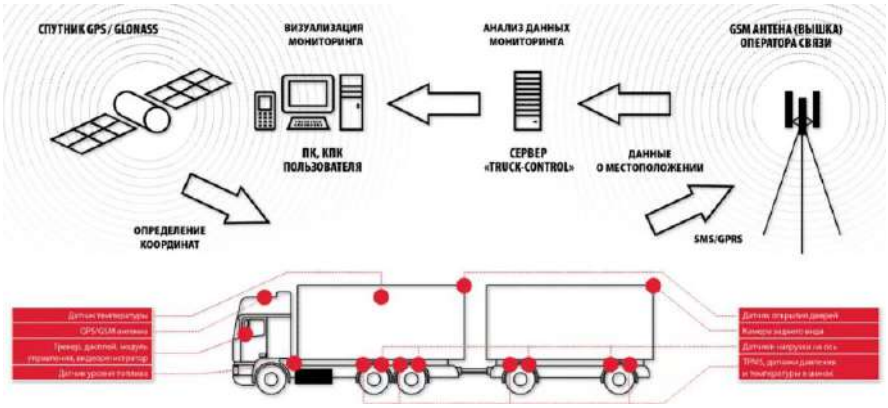


Рисунок 3 – Алгоритм работы системы автоматизации и конструкции беспилотного грузового автомобиля

На данный момент доступные сервисы – это беспилотные грузовые автомобили (или по-другому называется «высокоавтоматизированные транспортные средства») есть у следующих компаний:

Беспилотный тягач T-pod. (Рисунок 4).

Рисунок 4 – Беспилотный тягач T-pod.

Беспилотный тягач T-pod создала молодая шведская компания Einride, основанная в 2012 году. Особенностью этой опытной модели является полный отказ от элементов кабины и механических систем, которые занимают пространство под капотом, что позволяет уменьшить длину автомобиля при увеличении объема грузового отсека. Грузоподъемность беспилотного транспортного средства составляет 20 тонн. Электрическая силовая установка питается от электрической батареи общей емкостью 200 кВТ/ч. Тягач T-pod может проехать 200 км без подзарядки.

Беспилотный грузовой автомобиль Tesla (Рисунок 5).

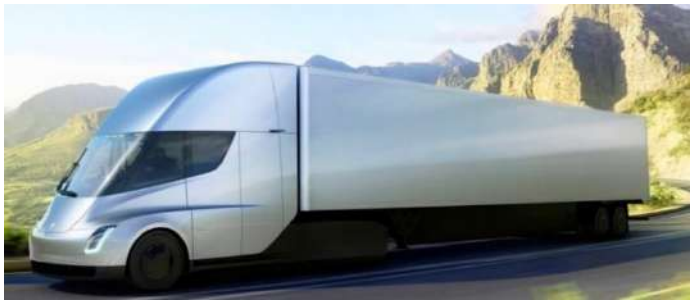


Рисунок 5 – Беспилотный грузовой автомобиль Tesla

Одним из первых производителей электромобилей является американская компания Tesla, основанная в июле 2003 года. Первоначально модельный ряд продукции Tesla включала три серии автомобилей, которые были оснащены электродвигателем мощностью 268 л.с. и 362 л.с. Разработка автономных автомобилей находится в стадии завершения, о технических характеристиках новых автомобилей пока ничего не известно. Предполагается, что дальность хода тягача на одном заряде аккумулятора составит около 400 километров.

Беспилотный грузовой автомобиль КАМАЗ (Рисунок 6).

Рисунок 6 – Беспилотный грузовой автомобиль КАМАЗ

Автомобиль оснащен системой помощи водителю с компонентом искусственного интеллекта - ADAS (Advanced Driver Assistance System). В отличие от аналогичных зарубежных продуктов, важнейшим преимуществом отечественного проекта является возможность реальной эксплуатации в российских условиях.

В настоящее время на разных стадиях разработки и производства беспилотных грузовых автомобилей находятся компании: Daimler, Uber, Paccar, Nvidia, Google, BAIC, Komatsu, Hyundai, Volvo, Mercedes, Starline.

Обзор перспективы внедрения беспилотных грузовых автомобилей в массовую эксплуатацию показывает:

- автоматизация автотранспортных средств может позволить снизить расход энергии по сравнению с обычными современными транспортными средствами;
- ожидаемый экономический эффект включает сокращение расхода топлива и снижения аварийности на дорогах;
- в структуре машиностроительной отрасли появляется более инновационная сфера разработок беспилотных грузовых автомобилей.

Список литературы

1. Умутбаев Р.Р., Р.И. Салимов. Алгоритм работы интеллектуальной системы дистанционного запуска с функцией автозапуска ДВС беспилотного грузового автомобиля, Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, г. Казань).
2. Халяфиев А.А., Халяфиев Р.А. «Беспилотные грузовые автомобили». [Электронный ресурс]: URL.: https://cyberleninka.ru/article/n/bespilotnye-gruzovye-avtomobili, (дата обращения: 22.02.23).
3. Айвазян А.В.Беспилотные технологии в сфере грузового коммерческого транспорта, ФГБОУ ВО «РГЭУ (РИНХ)».
4. А.А. Лотышева, к.т.н.д. А.А. Конорева. «Будущее беспилотных грузовиков в России», ФГБОУ ВО «СиБАДИ», «Сборник материалов V Международной научно-практической конференции».
5. А.А. Тюгашев, А.П. Долгинцев. «Использование логических подходов к интеллектуальному контролю и управлению транспортными средствами»

6. «Молодой ученый. Беспилотный транспорт будущего». [Электронный ресурс]: Официальный сайт. – URL.:https://moluch.ru/archive/246/56678/, (дата обращения: 22.02.23).
7. Кузнецова М.В., Веремеенко Е.Г. «Перспективы внедрения беспилотного управления автомобильными перевозками, Донской Государственный технический университет».
8. Т.Е. Мельникова, З.М. Адуллина, И.С. Степанова. «Перспективы развития автономных грузовых автотранспортных средств в России с учетом зарубежного опыта»
9. Халяфиев А.А., Халяфиев Р.А. «Программное обеспечение для беспилотных автомобилей»
10. А.В. Калинин, А.Н. Малая. «Разработка концепции алгоритма управления беспилотного колёсного тягача, движущегося в колонне за направляющим»
11. Зайцева Е.П., д.т.н., с.н.с. Сайкин А.М., Туктакиев Г.С., к.т.н. Журавлев А.В. «Развитие наземных беспилотных транспортных средств, систем помощи водителю и компонентов по данным патентных публикаций» – 10 с.

References

1. Umutbaev R.R., R.I. Salimov. The algorithm of the intelligent remote start system with the function of autorun of the internal combustion engine of an unmanned truck, Kazan National Research Technical University named after A.N. Tupolev-KAI, Kazan).
2. Khalafiev A.A., Khalafiev R.A. "Unmanned trucks". [Electronic resource]: URL.: https://cyberleninka.ru/article/n/bespilotnye-gruzovye-avtomobili , (date of application: 02/22.23).
3. Ayvazyan A.V.Unmanned technologies in the field of commercial cargo transport, FSUE VO "RSEU (RINH)".
4. A.A. Lotysheva, Candidate of Technical Sciences, D.A.A. Konoreva. "The future of unmanned trucks in Russia", SibADI, "Collection of materials of the V International Scientific and Practical Conference".
5. A.A. Tyugashev, A.P. Dolgintsev. "Using logical approaches to intelligent control and management of vehicles"
6. "Young scientist. Unmanned transport of the future". [Electronic resource]: Official website. – URL.:https://moluch.ru/archive/246/56678 /, (accessed: 22.02.23).
7. Kuznetsova M.V., Veremeenko E.G. "Prospects for the introduction of unmanned control of road transport, Don State Technical University".
8. T.E. Melnikova, Z.M. Adullina, I.S. Stepanova. "Prospects for the development of autonomous cargo vehicles in Russia taking into account foreign experience"
9. Khalafiev A.A., Khalafiev R.A. "Software for unmanned vehicles"
10. A.V. Kalinin, A.N. Malaya. "Development of the concept of an algorithm for controlling an unmanned wheeled tractor moving in a column behind a guide"
11. Zaitseva E.P., Doctor of Technical Sciences, S.N.S. Saikin A.M., Tuktakiev G.S., Candidate of Technical Sciences Zhuravlev A.V. "Development of ground–based unmanned vehicles, driver assistance systems and components according to patent publications" - p.10

Чуйко Д.О., Кретова А.А. Выбор технологии для разработки автоматизированной системы самообслуживания и инвентаризации в библиотеке // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 4(30) с. 78–83

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

ВЫБОР ТЕХНОЛОГИИ ДЛЯ РАЗРАБОТКИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ САМООБСЛУЖИВАНИЯ И ИНВЕНТАРИЗАЦИИ В БИБЛИОТЕКЕ

Чуйко Д.О., Кретова А.А.
ФГБОУ ВО "Национальный Исследовательский Университет "Высшая Школа Экономики", Москва, Россия (123592, Москва, Таллинская ул., 34), e-mail: daniilmaibe@gmail.com

Данная научная работа посвящена выбору наиболее оптимальной технологии для разработки автоматизированной системы самообслуживания и инвентаризации в библиотеке. В работе рассмотрены четыре технологии: RFID, штриховые коды, NFC и QR-коды, а также их преимущества и недостатки. В результате анализа было выявлено, что наиболее подходящей технологией для реализации данной системы является RFID, благодаря ее высокой скорости и точности считывания, возможности удаленного считывания и защиты от кражи. Однако, необходимо учитывать стоимость внедрения системы, которая может быть высокой.

Ключевые слова: Автоматизация процессов, автоматизированная система самообслуживания, инвентаризация, библиотека, RFID-технология, QR-код, баркод, штриховый код, NFC технология.

THE CHOICE OF TECHNOLOGY FOR THE DEVELOPMENT OF AN AUTOMATED SELF-SERVICE SYSTEM AND INVENTORY IN THE LIBRARY

Chuiko D.O., Kretova A.A.
National Research University Higher School of Economics, Moscow, *Russia (123592, Moscow, Tallinnskaya St., 34), e-mail: daniilmaibe@gmail. com*

This scientific work consists in choosing the most optimal technology for the development of an automated self-service system and inventory in the library. The paper considers four technologies: RFID, barcodes, NFC and QR codes, as well as their advantages and disadvantages. As a result of the analysis, it was revealed that the most suitable technology for the implementation of this system is RFID, due to its high speed and accuracy of reading, the possibility of remote reading and protection against theft. However, it is necessary to take into account the cost of implementing the system, which can be high.

Keywords: Process automation, automated self-service system, inventory, library, RFID technology, QR code, barcode, NFC technology.

Введение

В настоящее время библиотеки являются ключевым источником информации, который предоставляет доступ к знаниям и культурным ценностям. Вместе с тем, в современном обществе быстро развиваются технологии, что заставляет библиотеки пересматривать свои традиционные подходы к обслуживанию читателей. Одним из решений может стать

внедрение автоматизированных систем самообслуживания и инвентаризации, которые могут повысить эффективность работы библиотек и обеспечить более высокое качество обслуживания.

Однако, выбор конкретной технологии для разработки автоматизированной системы является сложным и многогранным процессом, требующим учета множества факторов, таких как функциональные требования, стоимость, интеграция с существующими системами и другие.

Цель данной научной работы - исследовать различные технологии, доступные для разработки автоматизированных систем самообслуживания и инвентаризации в библиотеках, а также проанализировать их преимущества и недостатки. На основе этого анализа будет предложена наиболее оптимальная технология, учитывающая потребности библиотеки и ограничения ее бюджета. Результаты и выводы данного исследования могут быть полезны как для библиотек, планирующих внедрить автоматизированные системы, так и для разработчиков, предлагающих свои решения, представляющие собой готовые продукты.

1. Технологии для разработки автоматизированной системы самообслуживания и инвентаризации.

Существует несколько технологий, которые могут быть использованы для разработки автоматизированных систем самообслуживания и инвентаризации в библиотеках. Некоторые из них включают:

1. RFID (Radio-Frequency Identification) технология: это технология, которая позволяет идентифицировать и отслеживать объекты, используя радиочастотные сигналы. В библиотеках RFID технология может быть использована для автоматизации процесса выдачи книг, возврата книг и инвентаризации коллекции;
2. технология штриховых кодов (баркодов): Баркоды используются для маркировки книг и других материалов в библиотеке. Они могут быть прочитаны с помощью сканеров, которые могут использоваться для автоматической выдачи и возврата книг;
3. NFC (Near Field Communication) технология: это технология беспроводной связи, которая позволяет устройствам взаимодействовать друг с другом на небольшом расстоянии. В библиотеках NFC технология может использоваться для обмена данными между книгами и мобильными устройствами читателей;
4. QR-коды: являются двухмерными штрих-кодами, которые могут содержать большое количество информации. В библиотеках они могут использоваться для быстрого доступа к информации о книгах, такой как автор, название, издательство, а также для автоматической выдачи книг и возврата книг.

Конечный выбор технологии зависит от потребностей и требований библиотеки, а также от доступности ресурсов и бюджета. В ходе работы каждая из технологий будет рассмотрена более подробно.

1.1. RFID технология

Для реализации системы самообслуживания и инвентаризации в библиотеке с помощью RFID технологии, необходимо установить специальные RFID-считыватели на разных точках библиотеки, таких как стойки выдачи, зоны возврата, зоны инвентаризации и т.д. Также, на

каждый экземпляр книги нужно установить RFID метку, которая будет содержать уникальный идентификатор книги. Когда читатель возьмет книгу, считыватель прочитает RFID метку, и информация об этом будет передана в базу данных библиотеки. При возврате книги читатель просто кладет книгу на стол в зоне возврата, где считыватель определит наличие RFID метки и автоматически вернет книгу в базу данных библиотеки [1].

Преимущества использования RFID технологии для системы самообслуживания и инвентаризации в библиотеке включают:

- быстроту и эффективность: автоматизированная система на основе RFID технологии позволяет читателям быстро и эффективно брать книги на выдаче и возвращать их в зоне возврата;
- точность: RFID технология позволяет точно отслеживать местонахождение книг в библиотеке, что упрощает инвентаризацию и уменьшает количество утерянных книг;
- минимальное вмешательство человека: система самообслуживания на основе RFID технологии может работать без участия библиотечных работников, что позволяет увеличить производительность и снизить затраты на персонал [2].

Недостатки использования RFID технологии для системы самообслуживания и инвентаризации в библиотеке включают:

- сложности в обновлении: если библиотека решает добавить новые функции или изменить конфигурацию системы, может потребоваться обновление оборудования и переустановка меток;
- возможные проблемы с защитой конфиденциальности: RFID метки могут содержать конфиденциальную информацию, которая без должного уровня шифрования может быть прочитана злоумышленниками;
- ограниченный диапазон считывания: RFID технология имеет ограниченный диапазон считывания, что может создавать проблемы при работе в больших помещениях или на открытых территориях [3].

Несмотря на некоторые недостатки, RFID технология является одним из наиболее эффективных и популярных способов автоматизации системы самообслуживания и инвентаризации в библиотеке [4]. Ее преимущества включают быстроту, точность и минимальное вмешательство человека, что позволяет библиотекам повысить эффективность работы и улучшить качество обслуживания читателей.

1.2. Штриховые коды

Система самообслуживания и инвентаризации в библиотеке может быть реализована с помощью штриховых кодов (баркодов). Для этого необходимо нанести его на каждый экземпляр книги и использовать специальный сканер для считывания информации [5].

Преимущества использования баркодов включают:

- низкая стоимость: в отличие от RFID меток, штриховые коды наносятся на книги с помощью простой печати, что значительно снижает стоимость внедрения системы;

- простота в использовании: система на основе баркодов легко интегрируется в существующую библиотечную инфраструктуру и не требует специальных знаний для работы с ней;
- доступность оборудования: сканеры широко распространены и доступны для приобретения.

Однако, подобная система имеет и некоторые *недостатки*:

- низкая скорость считывания: в отличие от RFID технологии, сканеру требуется физический контакт с баркодом для считывания информации, что может занимать дополнительное время при проведении инвентаризации или самообслуживания;
- риск повреждения: штриховые коды могут повреждаться или стираться со временем, что может создавать проблемы при считывании информации;
- ограниченный объем информации: баркоды позволяют хранить ограниченный объем информации, что может быть недостаточно для сложных систем инвентаризации и самообслуживания.

В целом, система на основе штриховых кодов может быть эффективным и доступным способом автоматизации системы самообслуживания и инвентаризации в библиотеке. Однако, перед выбором технологии необходимо учитывать конкретные потребности и особенности работы библиотеки.

1.3. NFC технология

Система самообслуживания и инвентаризации в библиотеке может быть реализована с помощью технологии бесконтактной связи NFC (Near Field Communication). Для этого на каждый экземпляр книги устанавливаются NFC-метки, которые могут быть считаны с помощью NFC-смартфона или специального считывающего устройства.

Преимущества использования NFC технологий включают:

- высокая скорость считывания: NFC-считывающие устройства могут считывать информацию с меток практически мгновенно, что позволяет быстро проводить инвентаризацию или самообслуживание;
- высокий объем информации: NFC-метки могут хранить больший объем информации, чем баркоды, что позволяет использовать их для более сложных систем инвентаризации и самообслуживания;
- безопасность: NFC-метки могут быть защищены паролем, что обеспечивает более высокий уровень безопасности при работе с системой.

Недостатки использования NFC технологий включают:

- высокая стоимость: NFC-метки и считывающие устройства могут быть более дорогими, чем баркоды и оборудование для их чтения;
- требования к смартфону: для использования NFC-меток при самообслуживании пользователи должны иметь смартфон с поддержкой NFC;
- ограниченное расстояние действия: NFC-метки имеют ограниченное расстояние действия, что может приводить к необходимости установки большого количества считывающих устройств в библиотеке.

Резюмируя вышесказанное, система на основе NFC технологий может быть эффективным и безопасным способом автоматизации системы самообслуживания и инвентаризации в библиотеке. Однако, необходимо учитывать особенности работы библиотеки и оценить экономическую целесообразность внедрения данной технологии.

1.4. QR-коды

Система самообслуживания и инвентаризации в библиотеке может быть реализована с помощью технологии QR-кодов [6]. Для этого на каждый экземпляр книги наносятся коды, которые могут быть считаны с помощью смартфона или специального считывающего устройства.

Преимущества использования QR-кодов включают:

- большой объем информации: возможно хранение большого объема информации, что позволяет использовать их для более сложных систем инвентаризации и самообслуживания;
- широкое распространение технологии: QR-коды являются широко распространенной технологией, которую могут использовать практически все пользователи мобильных устройств;
- быстрое сканирование: подобные коды могут быть быстро и легко отсканированы с помощью смартфона или специального считывающего устройства.

Недостатки использования QR-кодов включают:

- низкий уровень безопасности: подобные метки могут быть легко подделаны или скомпрометированы, что делает систему уязвимой для мошенничества;
- ограниченный радиус действия: необходима непосредственная близость к считывающему устройству, что ограничивает радиус действия системы самообслуживания или инвентаризации;
- низкая стойкость к износу: QR-коды, наложенные на бумажные наклейки или этикетки, могут быть повреждены или стерты при использовании.

Выводы

Исходя из анализа рассмотренных технологий для реализации системы самообслуживания и инвентаризации в библиотеке, можно сделать вывод, что наиболее подходящей является технология RFID.

RFID-технология имеет ряд преимуществ перед другими рассмотренными технологиями, такими как возможность удаленного считывания и увеличение скорости процесса инвентаризации, повышение точности и автоматизация процессов, а также возможность использования для защиты от кражи.

Хотя стоимость оборудования и внедрения RFID-системы может быть высокой, на долгосрочной перспективе это может окупиться за счет увеличения эффективности и экономии времени и ресурсов.

Таким образом, применение RFID-технологии может быть наиболее оптимальным решением для библиотек, которые стремятся автоматизировать свои процессы и повысить качество обслуживания своих пользователей.

Список литературы

1. Baashirah R., Elleithy K. Automation of the Baggage Check-in Process Using RFID System in Airports // 2019 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2019. Institute of Electrical and Electronics Engineers Inc., 2019.
2. Liu Y., Deng G. Automating inventorying of blood stations: A system based on ultrahigh-frequency radio-frequency identification (UHF RFID) technology // Transfusion Clinique et Biologique. Elsevier Masson, 2022. Vol. 29, № 2. pp. 134–137.
3. Морозова Т.В., Аржаков А.В. Анализ уязвимости RFID-транспондеров [Electronic resource]. 2017. URL: https://www.elibrary.ru/item.asp?id=29157697 (accessed: 11.03.2023).
4. Morev V.A., Timoschuk M.O. Use of radio frequency identification systems (RFID) in library services (based on experience of the Scientific Library of the National Research Tomsk State University) // Research result. Business and Service Technologies. Belgorod National Research University, 2020. Vol. 6, № 3.
5. Sriram T. et al. Applications of barcode technology in automated storage & retrieval systems // IECON Proceedings (Industrial Electronics Conference). IEEE, 1996. Vol. 1. pp. 641–646.
6. Сандульский А.А. QR Inventory: Учет имущества и инвентаризация по QR-коду [Electronic resource]. 2022. URL: https://www.elibrary.ru/item.asp?id=48492848 (accessed: 11.03.2023).

References

1. Baashirah R., Elleithy K. Automation of the Baggage Check-in Process Using RFID System in Airports // 2019 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2019. Institute of Electrical and Electronics Engineers Inc., 2019.
2. Liu Y., Deng G. Automating inventorying of blood stations: A system based on ultrahigh-frequency radio-frequency identification (UHF RFID) technology // Transfusion Clinique et Biologique. Elsevier Masson, 2022. Vol. 29, № 2. pp. 134–137.
3. Morozova T.V., Arzhakov A.V. Vulnerability analysis of RFID transponders [Electronic resource]. 2017. URL: https://www.elibrary.ru/item.asp?id=29157697 (accessed: 11.03.2023).
4. Morev V.A., Timoschuk M.O. Use of radio frequency identification systems (RFID) in library services (based on experience of the Scientific Library of the National Research Tomsk State University) // Research result. Business and Service Technologies. Belgorod National Research University, 2020. Vol. 6, № 3.
5. Sriram T. et al. Applications of barcode technology in automated storage & retrieval systems // IECON Proceedings (Industrial Electronics Conference). IEEE, 1996. Vol. 1. pp. 641-646.
6. SANDULSKY A.A. QR Inventory: Property accounting and inventory by QR code [Electronic resource]. 2022. URL: https://www.elibrary.ru/item.asp?id=48492848 (accessed: 11.03.2023).

Обливальный Н.Д. Определение оптимального способа взаимодействия с клиентом для увеличения доходности маркетинговых кампаний и снижения издержек на них // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 4(30) с. 84–91

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.891.2

ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОГО СПОСОБА ВЗАИМОДЕЙСТВИЯ С КЛИЕНТОМ ДЛЯ УВЕЛИЧЕНИЯ ДОХОДНОСТИ МАРКЕТИНГОВЫХ КАМПАНИЙ И СНИЖЕНИЯ ИЗДЕРЖЕК НА НИХ

Обливальный Н.Д.
ФГБОУ ВО "Челябинский Государственный Университет", Челябинск, Россия (454001, г. Челябинск, ул. Братьев Кашириных, д.129), e-mail: rfrepe@gmail.com

В данной работе рассматривается поиск и определение оптимального способа взаимодействия с клиентом для увеличения доходности маркетинговых кампаний и снижения издержек на них. В работе были проделаны следующие задачи: определение универсального подхода к Uplift моделированию для выбора типа коммуникации; формирование требований к структуре данных для достижения максимальной точности; реализация сервиса по работе с данными и получения расчетов для принятия решения о способе коммуникации. Решения данных задач рассматривалось в рамках прикладной области телеком провайдера. Практическим итогом данной работы является сервис, с помощью которого будет определена необходимости и способ коммуникации с абонентами телеком провайдера, имеющими задолженность.

Ключевые слова: Uplift моделирование, машинное обучение, большие данные, коммуникация с клиентами, доходность маркетинговых кампаний, телеком провайдер.

DETERMINING THE OPTIMAL WAY TO INTERACT WITH THE CLIENT TO INCREASE THE PROFITABILITY OF MARKETING CAMPAIGNS AND REDUCE THEIR COSTS

Oblivalny N.D.
FSBEI of HE "Chelyabinsk State University", Chelyabinsk, *Russia (454001, Chelyabinsk, Bratya Kashirin str., 129), e-mail: rfrepe@gmail.com*

In this paper, we consider the search and determination of the optimal way to interact with the client to increase the profitability of marketing campaigns and reduce their costs. The following tasks were performed in the work: defining a universal approach to Uplift modeling for choosing the type of communication; forming requirements for the data structure to achieve maximum accuracy; implementing a service for working with data and obtaining calculations to make a decision on the method of communication. Solutions to these problems were considered within the scope of the telecom provider's application area. The practical result of this work is a service with which the necessity and method of communication with subscribers of the telecom provider who have debts will be determined.

Keywords: Uplift modeling, machine learning, big data, communication with customers, profitability of marketing campaigns, telecom provider.

Введение

Целью данной работы является определение оптимального способа взаимодействия с клиентом для увеличения доходности маркетинговых кампаний и снижения издержек на них.

Задачами магистерской работы являются: определение универсального подхода к Uplift моделированию для выбора типа коммуникации, формирование требований к структуре данных для достижения максимальной точности, реализация сервиса по работе с данными и получения расчетов для принятия решения о способе коммуникации. Решения данных задач будут рассмотрены на прикладной области телеком провайдера. Практическим итогом данной работы будет являться сервис, с помощью которого будет определена необходимости и способ коммуникации с абонентами телеком провайдера, имеющими задолженность.

Большинство современного бизнеса не может существовать без использования цифровых технологий, особенно в сегменте B2C. Цифровые решения затронули все сферы бизнеса. Начиная от автоматизации внутренних бизнес-процессов, заканчивая различными видами коммуникации с клиентами.

Для любого бизнеса одной из основных целей всегда является увеличение прибыли. И первое, с чего начинается путь привлечения финансов в компанию, это взаимодействие с клиентом. Правильно взаимодействуя с клиентами, бизнес способен мотивировать их на действия. Например, на оформление подписки, покупки товара, рекомендации продукта своим друзьям или на повторную покупку.

При сегодняшнем многообразии каналов коммуникации: смс-сообщение, звонок, пуш-уведомление, электронное письмо, баннер, контекстная реклама и т.д. - выбор способа взаимодействия стал актуальной проблемой. При планировании бюджета нужно грамотно распределять его между всеми способами взаимодействия, при этом необходимо достичь максимального увеличения доходности.

Практика показала, что у клиентов есть собственные привычки взаимодействия с бизнесом. Кто-то отслеживает смс-сообщения, но при этом никогда не читает электронную почту. И сегодня большинство компаний стараются не экономить на коммуникации с клиентом и пользуются всеми доступными средствами. Из-за чего делают только хуже. Информационный шум, который они создают, понижает эффективность каналов коммуникации из-за снижения внимания у клиентов.

Так, например, по результатам исследования компании «Мета» (запрещённой в Российской Федерации) можно сделать вывод о том, что пользователи, получающие меньшее количество уведомлений в приложении, больше используют приложение (Рисунок 1).

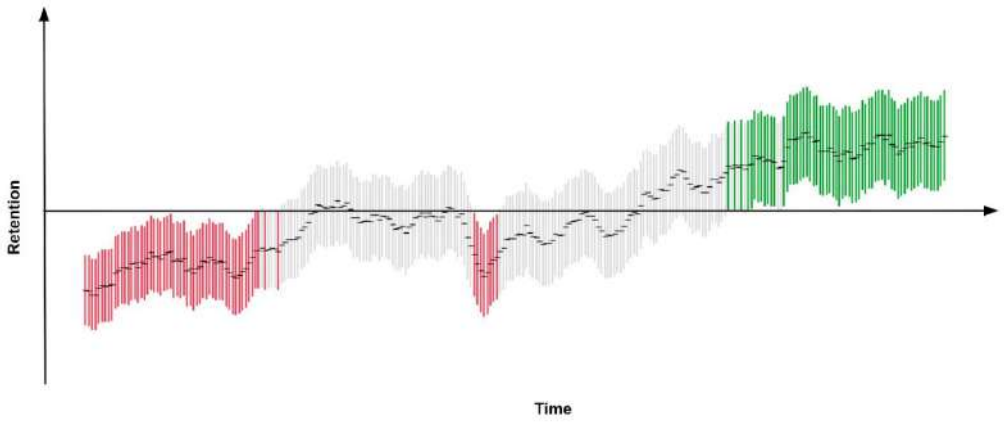


Рисунок 1 – График возвращения пользователей, получивших меньшее количество уведомлений.

Источник: исследование компании «Мета» (запрещённой в Российской Федерации)

На графике показан уровень вовлеченности пользователя в приложение. По данным исследованиям уменьшение числа уведомлений в начале привело к кратковременному снижению активности пользователя, но в конечном итоге спустя время увеличило его вовлеченность в приложение.

Таким образом, все вышеперечисленное доказывает актуальность данной работы.

Методы

Для принятия решений о выборе взаимодействия с клиентом рассмотрим несколько подходов к Uplift моделированию [1].

Первый подход основан на использовании одной модели классификации. Модель обучалась на данных клиентов, с которыми взаимодействовали и не взаимодействовали. Для определения эффекта от взаимодействия тип взаимодействия выводят в отдельный признак. После обучения модели при получении прогноза необходимо сделать прогноз для каждого типа взаимодействия. После чего определить тип, при котором вероятность совершения целевого действия максимальная.

Второй подход заключается в использовании двух независимых моделей. Для каждого типа взаимодействия формируется отдельный датасет. Далее на сформированных датасетах обучаются модели классификации. В результате мы получаем набор моделей, которые оценивают вероятность совершения ключевого действия для каждого типа взаимодействия. Получив прогноз от каждой модели, мы можем определить наилучший тип взаимодействия.

У второго подхода есть различные вариации реализации зависимостей между полученными моделями. Например, с зависимым представлением данных. Идея состоит в том, что при наличии различных меток можно построить столько же различных классификаторов, каждый из которых решает задачу бинарной классификации. В процессе обучения каждый следующий классификатор использует предсказания предыдущих в качестве дополнительных признаков. Авторы данного метода предложили использовать ту же идею для решения проблемы uplift моделирования в два этапа. Вначале мы обучаем классификатор по контрольным данным. Затем выполним предсказания в качестве нового признака для обучения второго классификатора на тестовых данных, тем самым вводя зависимость между двумя наборами данных.

Еще один подход основан на построении перекрестно зависимых моделей [2]. Его рекомендуется применять тогда, когда целевая группа достаточно маленькая. В этом случае есть риск, что модель, построенная на целевой группе, будет обладать недостаточной обобщающей способностью. Поэтому создается перекрестная зависимость двух моделей, чтобы усилить одну модель данными другой. Сначала обучаем параллельно две модели: одну на контрольной группе, другую — на целевой. Затем преобразуем обе целевые переменные, используя предсказания контрольной модели на данных целевой группы и предсказания целевой модели на данных контрольной группы. Полученные величины называются вменяемым эффектом от воздействия. Обучим две новые модели на преобразованных таргетах. Взвешенная с некоторым коэффициентом сумма предсказаний этих моделей и будет uplift.

Данные подходы являются базовыми в Uplift моделировании. Также существуют методы, основанные на деревьях, трансформации классов и много классовых моделях.

Метод подготовки данных

Предобработка данных и подготовка датасета - один из важнейших этапов построения моделей машинного обучения. От них напрямую зависит качество прогнозов моделей. Поэтому данному этапу нужно всегда уделять большое внимание.

Для нашей задачи всегда нужно определиться с ключевой метрикой. Как правило, ей является совершение определённого действия, категориальный признак. Например, покупка или оформление заказа. В таком случае лучше всего использовать модели классификации.

Но в ряде случаев ключевой метрикой может стать количественный признак. Например, сумма заказа или средний чек. В таком случае лучше использовать регрессионные модели в качестве основы для uplift моделирования.

Не зависимо от выбора базовых моделей необходимо провести стандартную предобработку данных. Традиционные EDA анализ поможет нормализировать данные, избавиться от выбросов и ошибок в датасетах.

В качестве данных для Uplift моделей может использоваться различная информация о клиенте. От текущих статусов клиента до агрегированной исторической информации[3].

Основными требованиями к датасету будут являться:

- Сбалансированность выборок с различными типами взаимодействия. Для каждого типа взаимодействий должно быть достаточно примеров для получения достоверных прогнозов.
- Идентификация конкретного клиента. Все данные должны быть привязаны к конкретному клиенту, по которому будут армироваться данные и в итоге формироваться прогноз.

Главной задачей на данном этапе становится построение универсального способа подготовки данных для формирования датасета. Так как данные можно разделить на 2 типа. Описывающие объект (человека) и описывающие событие (взаимодействие), то необходимо собрать 2 датасета.

В первом будет находиться вся информация по клиенту. Те признаки, которые его описывают в конкретный момент времени.

Структура первого датасета:

- Дата события
- Идентификатор клиента
- Признак
- Значение

Второй содержит информацию о взаимодействиях или отсутствии взаимодействия с клиентом и информацию о результате взаимодействия.

Структура второго датасета:

- Дата взаимодействие
- Идентификатор клиента
- Тип взаимодействия
- Результат

Для того чтобы получить итоговую обучающую выборку, нам необходимо агрегировать всю информацию о клиенте на даты взаимодействия. Для этого нужно предобработать первый датасет.

Сперва необходимо определить типы данных у всех признаков. Затем для категориальных признаков найти значения: часто встречающиеся, медианное и среднее значение промежутков времени между событиями. Для количественных признаков: среднее значение, медианное значение, сумму, дисперсию и медианное и среднее значение промежутков времени между событиями. Все признаки считаются на момент взаимодействия для каждого клиента.

Затем нужно объединить агрегированные данные из первого датасета с данными из второго. Добавить в первый датасет признаки “Тип взаимодействия” и “Результат”.

Таким образом, мы поделили датасет с информацией о клиенте на конкретный момент времени с указанием взаимодействия и итогом его взаимодействия. Дальнейшая его предобработка будет зависеть от выбранного подхода к построению Uplift модели.

Данные телеком провайдера

Для постановки эксперимента была выбрана область телеком провайдера. Необходимо собрать датасет для абонентов компании, попавших в статус должников.

Для первого датесета была собрана информация о всех услугах и сервисах, которыми пользуется или пользовался должник. В признаки попала следующая информация: трафик, смена тарифов, установление автоплатежей, заявки на подключение, сессии в мобильном приложении, платежи, блокировки услуг, взаимодействие с домофоном, обращения в техническую поддержку, информация о жилом фонде клиента и еще около 100 признаков.

Для каждого признака были подсчитаны агрегированные значения на момент запланированного взаимодействия. Итоговая размерность датасета составила 861 признаков.

Оценка результатов

Для оценки результатов работы uplift модели существуют специальные метрики.

Например, uplift@k. С помощью обученной uplift модели мы хотим отобрать какое-то количество клиентов, с которыми будем коммуницировать. Пусть бюджет рассчитан на k% клиентов. Тогда нам интересно оценить качество прогноза не на всей тестовой выборке, а только на объектах с наибольшими предсказаниями при отсечении по порогу в k процентов [4].

Для расчета uplift@k нужно отсортировать выборку по величине предсказанного uplift и посмотреть разницу средних значений таргета Y (в англоязычных статьях использую термин response rate, мы его тоже будем использовать в дальнейшем) в целевой и контрольной группах. Целевая группа - группа, которая получила коммуникацию. Контрольная группа - которая не получила (1).

$$uplift@k = response\ rate@k_{(treatment)} - response\ rate@k_{(control)}$$
$$response\ rate@k = mean(Y@k) \quad (1)$$
$$Y@k - \text{таргет на } k\%$$

Есть еще одна метрика, называющиеся кривая qini. Физический смысл qini кривой в том, чтобы не давать модели поднимать наверх в ранжировании только целевую (treatment) группу,

штрафуя ее за это множителем NT/NC, который уменьшает итоговое значение, если NT сильно больше, чем NC (2).

$$qini\ curve(t) = Y_t^T - \frac{Y_t^C N_t^T}{N_t^C} \quad (2)$$

Y_t^T, Y_t^C – таргет в $treatment$ группе, таргет в $control$ группе

N_t^T, N_t^C – размер $treatment$ группы, размер $control$ группы

Для перехода от кривых к числам используется коэффициент AUQC.

Для оценки результатов экспериментов будут использоваться две представленные метрики. Также для оценки качества классификаторов будет использовать метрика f1-score.

Результаты экспериментов

В рамках эксперимента использовался тестовый набор данных.

Сперва было необходимо определиться с подходом в методе, использующим две модели. Для этого были обучены модели с использованием одинаковых классификаторов. Результаты качества получившихся моделей представлены в Таблице 1.

Таблица 1 – Сравнение подходов с использованием двух моделей.

Подходы	**f1** (целевой группы)	**uplift@20%**	**AUQC**
Две независимые модели	0.5007	0.1744	0.1495
Две зависимые модели (зависимое представление данных)	0.5303	0.0597	0.0903
Две зависимые модели (перекрестная зависимость)	0.0514	0.0368	0.0846

Источник: анализ автора

В итоге максимальную точность имеет подход с использованием двух независимых моделей.

Следующим этапом стало определение подходящего классификатора. Также было произведено сравнение самых популярных моделей классификации. Результаты сравнения классификаторов представлены в таблице 2 [5-7].

Таблица 2 – Оценка модели при применении подхода с не зависимыми моделями

Модели	**Контрольная f1-score**		**Целевая f1-score**	
	Не оплатил	**Оплатил**	**Не оплатил**	**Оплатил**
XGBoost	0.811	0.742	0.806	0.555
CatBoost	0.814	0.72	0.807	0.522
LogReg	0.79	0.7	0.801	0.48

Источник: анализ автора

Лучший результат показала модель XGBoost. При подборе гиперпараметров удалось достичь следующих показателей. Результаты представлены в Таблица 3.

Таблица 3 – Лучшая модель подхода с использованием двух независимых моделей.

Best model XGboost	**f1**(целевой группы)	**uplift@20%**	**AUQC**
Две независимые модели	0.553	0.6594	0.3574

Источник: анализ автора

Данную модель взяли для проведения A/B теста в реальных условиях. Для подтверждения качества модели на практике необходимо было получить статистическую значимость у двух групп: «Убеждаемые» и «Не беспокоить». Эти две группы имеют противоположный по своему характеру смысл. Хорошая модель должна уметь максимально разводить их и иметь статистическую значимость.

Эксперимент с использованием A/B теста был поставлен на должниках телеком провайдера. Его результаты представлены в Таблице 4.

Таблица 4 – Результаты A/B теста подхода с использованием двух независимых моделей.

Группы	**Конверсия в оплату**		**Доверительный интервал**		**Значимость**
	A (звонок)	B (без звонка)	1	2	
Убеждаемые	30,65%	17,81%	-21,97%	-3,72%	Значимое
Потерянные	14,02%	10,57%	-8,08%	1,18%	Незначимое
Лояльные	35,66%	36,82%	-1,31%	3,63%	Незначимое
Не беспокоить	20,45%	25,48%	0,4%	10,03%	Значимое

Источник: анализ автора

По итогам A/B теста можно сделать вывод о том, что получившаяся модель действительно имеет практический эффект. Она определит группу людей, с которыми коммуникация будет наиболее эффективна, и группу людей, с которыми нет практической ценности взаимодействовать.

Заключение

За счет использования uplift модели, основанной на подходе с двумя независимыми моделями, удалось добиться:

1. Сохранения текущей конверсии должников в оплату. По данным эксперимента, процент вырос на группе «Убеждаемых», но в контексте всех должников данный прирост не является значительным. Поэтому точнее утверждать, что процент конверсии не снизился.
2. Снизили издержки на исходящих звонках должникам. За счет прекращения звонков оставшимся группам удалось высвободить большое количество ресурсов операторов, которые

были перераспределены на другие задачи. В рамках процесса обзвона должников процент экономии ресурсов составил более 80%.

Данный подход является универсальным за счет унификации работы с данными и имеет практическую ценность.

Список литературы

1. Artem Betlei, Eustache Diemert, Massih-Reza Amini. Uplift Modeling with Generalization Guarantees, 2021.
2. Robin M. Gubela, Stefan Lessmann. Interpretable Multiple Treatment Revenue Uplift Modeling, 2021.
3. Henrik Karlsson, Linda Wanstrom. Uplift Modeling: Identifying Optimal Treatment Group Allocation and Whom to Contact to Maximize Return on Investment, 2019.
4. Ta-Wei Huang, Eva Ascarza. When Less is More: Using Short-term Signals to Overcome Systematic Bias in Long-run Targeting, 2022.
5. Xgboost documentation. - Режим доступа: https://xgboost.readthedocs.io/en/stable/, свободный.
6. Catboost documentation. - Режим доступа : https://catboost.ai/en/docs/, свободный.
7. LogisticRegression documentation. - Режим доступа:: https://scikit-learn.org/stable/index.html, свободный.

References

1. Artem Betlei, Eustache Diemert, Massih-Reza Amini. Uplift Modeling with Generalization Guarantees, 2021.
2. Robin M. Gubela, Stefan Lessmann. Interpretable Multiple Treatment Revenue Uplift Modeling, 2021.
3. Henrik Karlsson, Linda Wanstrom. Uplift Modeling: Identifying Optimal Treatment Group Allocation and Whom to Contact to Maximize Return on Investment, 2019.
4. Ta-Wei Huang, Eva Ascarza. When Less is More: Using Short-term Signals to Overcome Systematic Bias in Long-run Targeting, 2022.
5. Xgboost documentation. - Режим доступа: https://xgboost.readthedocs.io/en/stable/, свободный.
6. Catboost documentation. - Режим доступа : https://catboost.ai/en/docs/, свободный.
7. LogisticRegression documentation. - Режим доступа:: https://scikit-learn.org/stable/index.html, свободный.

Воробьев С. А., Разумов П. А., Трофимов Е. С. Исследование системы "Автомобиль-Электросеть" (V2G) // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 92–95

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 62

ИССЛЕДОВАНИЕ СИСТЕМЫ "АВТОМОБИЛЬ-ЭЛЕКТРОСЕТЬ" (V2G)

Воробьев С. А., Разумов П. А., Трофимов Е. С.
ФГБОУ ВО "Санкт-Петербургский Государственный Архитектурно-Строительный Университет", Санкт-Петербург, Россия (190005, г. Санкт-Петербург, 2-я Красноармейская ул., д.4), e-mail: wolftier@mail.ru

Система «автомобиль-электросеть» (V2G) относится к технологиям связи, посредством которых автомобиль взаимодействует с окружающей средой и объектами через сеть или напрямую. В статье рассмотрены результаты имитационного моделирования подхода V2G к экономии электроэнергии. Показано, что при повышении стоимости сетевого электричества проявляется ожидаемая положительная корреляция с использованием V2G в диапазоне 50% – 100%.

Ключевые слова: Электроэнергия, аккумуляторная батарея, имитационная модель, корреляция, переменные расходы.

RESEARCH OF THE "CAR-ELECTRIC GRID" SYSTEM (V2G)

Vorobyev S.A., Razumov P.A., Trofimov E.S.
FSBEI of HE "St. Petersburg State University of Architecture and Civil Engineering", St. Petersburg, Russia (190005, St. *Petersburg, 2nd Krasnoarmeyskaya St., 4), e-mail: wolftier@mail.ru*

The car-electric grid (V2G) system refers to communication technologies through which a car interacts with the environment and objects through a network or directly. The article discusses the results of simulation modeling of the V2G approach to energy saving. It is shown that with an increase in the cost of network electricity, the expected positive correlation with the use of V2G in the range of 50% – 100% is manifested.

Keywords: Electric power, battery, simulation model, correlation, variable costs.

Стремление к энергетической независимости и растущие экологические проблемы являются ключевыми факторами растущей популярности аккумуляторных автомобилей (АА) – электрических и подключаемых гибридных. Источником энергии для АА являются аккумуляторы, которые обеспечивают возможность ее хранения, которую можно эффективно пополнять, когда транспортное средство (ТС) подключено к электросети. Когда такая машина подключается к сети, она отправляет беспроводное сообщение серверу, и, когда местной электрической компании нужно больше электричества, она забирает ее из этого электромобиля. Концепция использования АА в качестве распределенного энергоресурса – нагрузки и ресурса – известна как технология «автомобиль-электросеть» (vehicle-to-grid или V2G) [1-3].

Подход V2G, а именно система "автомобиль-электросеть", позволяющая подключать машины в общую энергосеть для подзарядки автомобиля или возвращения лишней

электроэнергии обратно, более широко используется в Европе по сравнению с США, принимая во внимание, что сетевое электричество в Европе намного более дорогое. Наличие положительной корреляции между стоимостью сетевого электричества и использованием V2G ведет к увеличению количества электроэнергии, хранящейся с помощью V2G при повышающихся ценах на электричество. В России внедрение технологии подключенных автомобилей (connected car, CC), в которую входит и система V2G, регламентировано дорожной картой Национальной технологической инициативы "Автонет" [4].

В данной статье будет изучен подход V2G путем анализа количества электроэнергии, поставляемой бортовыми аккумуляторными батареями транспортных средств при изменении исходных параметров стоимости сетевого электричества и переменных расходов системы V2G. Исследование проводилось с помощью имитационной модели, разработанной авторами в системе VIKUS как одноузловый вариант имитационной модели URBS [5]. Первым параметром, включенным в данный анализ, является стоимость сетевого электричества, так как она определяет, является ли хранение энергии, генерируемой от непостоянных ВИЭ, экономически целесообразным, либо же менее затратно использование сетевого электричества [6]. Вторая переменная – это связанные с V2G расходы на киловатт-час аккумулируемой энергии. Эти переменные расходы служат для учета той вероятности, что дополнительные циклы зарядки при использовании V2G могут оказывать негативное влияние на срок службы аккумуляторных батарей [7, 8]. Как стоимость сетевого электричества, так и стоимость V2G испытывают существенное влияние неопределенности. По этой причине значения указанных показателей варьируют в широких пределах – от 50% (100% = базовое значение, следовательно, половина базового значения) до 200% (значение, в два раза большее, чем базовое). Расчетная доля потребностей в электроэнергии, обеспечиваемая V2G, показана на Рисунок 1 для 2025 и 2035 гг.

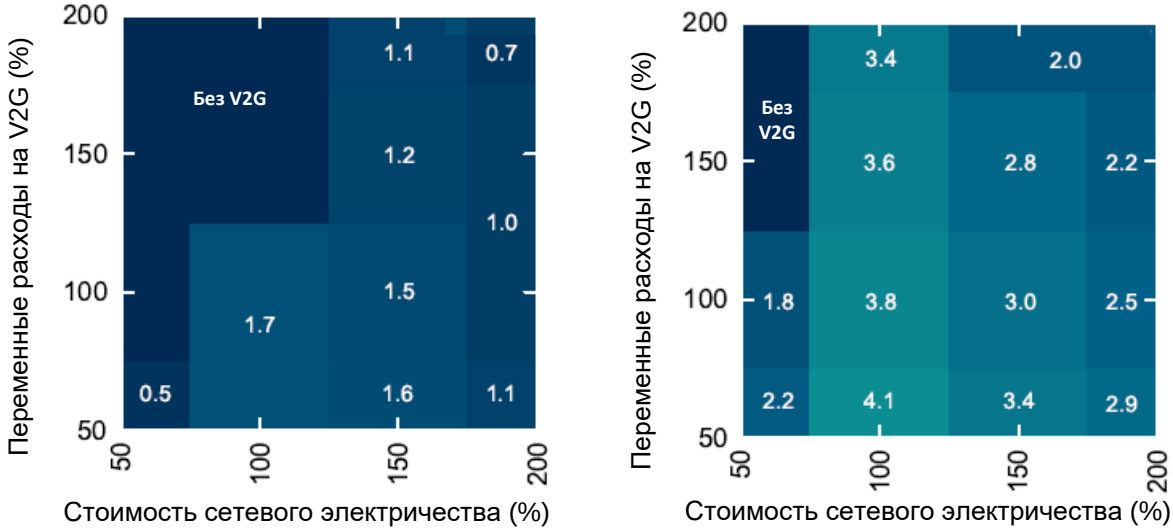


Рисунок 1 – Двусторонний анализ чувствительности (переменные расходы на V2G / стоимость сетевого электричества) доли потребления электроэнергии, покрываемой V2G: а) 2025 г.; б) 2035 г.

Цифрами показана доля потребности в электроэнергии, обеспечиваемая V2G (%).

Для рассмотренных случаев и временных рамок отмечается обратная корреляция между переменными расходами на V2G и масштабом использования V2G. Анализ чувствительности показал отрицательную корреляцию между масштабами использования V2G и переменными расходами, связанными с V2G. Чем более дорогостоящим становится подход V2G, тем меньше он применяется. Аналогично можно ожидать наличия положительной взаимосвязи между повышением стоимости сетевого электричества и использованием V2G.

Эти наблюдения являются результатом конкуренции между двумя технологиями хранения электроэнергии – V2G и стационарными аккумуляторными батареями.

На основании результатов, можно сделать заключение, что вложение средств в стационарные аккумуляторные батареи не является экономически оправданным, когда стоимость сетевого электричества имеет базовое значение. Соответственно, в этих условиях V2G предоставляет возможность хранения электроэнергии, вырабатываемой непостоянными возобновляемыми источниками энергии (ВИЭ), пока стоимость V2G (с поправкой на потери энергии) ниже стоимости сетевого электричества. В условиях повышающейся стоимости электроэнергии вложения в стационарные аккумуляторные батареи нивелируются экономией, достигаемой в случае аккумулирования большего объема электроэнергии от ВИЭ с целью снижения потребления сетевого электричества. Принимая во внимание тот факт, что основной целью стационарных аккумуляторных батарей является снижение доли электроэнергии, вырабатываемой от ВИЭ, весь износ, связанный с эксплуатацией этого актива в течение срока его службы, считается составляющей капиталовложений. С учетом этого после развертывания аккумуляторных батарей они используются до задействования V2G для предотвращения возникновения переменных затрат, связанных с V2G. Формируемый таким образом порядок ранжирования еще более важен, если учесть, что стационарные аккумуляторные батареи более эффективны, чем V2G.

Выводы: при повышении стоимости сетевого электричества проявляется ожидаемая положительная корреляция с использованием V2G в диапазоне 50% – 100%. Дальнейшее повышение стоимости сетевого электричества до 150% и 200% ведет к возникновению положительной корреляции с использованием стационарных аккумуляторных батарей, что ведет к уменьшению использования V2G. В большинстве сценариев V2G несет для явную выгоду. Это объясняется снижением переменных расходов и доступностью большего количества АА с аккумуляторными батареями большей емкости, а соответственно и ростом емкости V2G.

Список литературы

1. İnci M., Savrun M. M., Çelik Ö. Integrating electric vehicles as virtual power plants: A comprehensive review on vehicle-to-grid (V2G) concepts, interface topologies, marketing and future prospects // Journal of Energy Storage. – 2022. – Т. 55. – С. 105579.
2. Khan M. D. S. A. et al. Technical investigation on V2G, S2V, and V2I for next generation smart city planning // Journal of Electronic Science and Technology. – 2019. – Т. 17. – № 4. – С. 100010.
3. Калашников В. И., Чепига А. А. Анализ концепции vehicle-to-grid // Вестник Донецкого национального технического университета. – 2019. – № 2. – С. 89-94.

4. "План мероприятий ("дорожная карта") Национальной технологической инициативы "Автонет" (приложение N 2 к протоколу заседания президиума Совета при Президенте РФ по модернизации экономики и инновационному развитию России от 24.04.2018 N 1) // КонсультантПлюс URL: http://www.consultant.ru/document/Cons_doc_LAW_309650/06c0c45bdeebe4748100b5811a8c2c4f96801769/ (дата обращения: 05.04.2023).
5. Dorvner J., Hamacher T. URBS – a model of linear optimization of distributed energy systems. // Technical University of Munich – Institute of Renewable and Sustainable Energy Systems. URL: https://github.com/tum-ens/urbs (дата обращения: 25.03.2023)
6. Тачмухаммедов Г. М., Тачмухаммедова Б. Б. Экономическая эффективность рационального использования электроэнергии // Традиции и инновации в системе образования. – 2019. – С. 129-134.
7. Ерунов А. С. Срок службы аккумуляторной батареи автомобиля и ее неисправности // Инновации. Наука. Образование. – 2020. – № 23. – С. 663-665.
8. Hu X. et al. Battery lifetime prognostics // Joule. – 2020. – Т. 4. – № 2. – С. 310-346.

References

1. Inchi M., Savrun M. M., Chelik O. Integration of electric vehicles as virtual power plants: a comprehensive review of vehicle-to-grid (V2G) concepts, interface topology, marketing and prospects for the future // Journal of Energy Storage. – 2022. – Vol. 55. – pp. 105579.
2. Khan M. D. S. A. et al . Technical research of V2G, S2V and V2I for intelligent urban planning of the next generation // Journal of Electronic Science and Technology. – 2019. – Vol. 17. – No. 4. – pp. 100010.
3. In Kalashnikov. I., And Chepiga. A. Car-for-grid Concept analysis // Bulletin of Donetsk National Technical University. – 2019. – No. 2. – pp. 89-94.
4. "Action plan ("roadmap") The National Technological Initiative "Autonet" (Appendix number 2 to the minutes of the meeting of the Presidium of the Presidential Council for Economic Modernization and Innovative Development of Russia dated 04/24/2018 N in 1) // ConsultantPlus URL: http://www.consultant.ru/document/Cons_doc_LAW_309650/06c0c45bdeebe4748100b5811a8c2c4f96801769 / (accessed: 05.04.2023).
5. Dorvner J., Hamacher T. URBS – a model of linear optimization of distributed energy systems. // Technical University of Munich – Institute of Renewable and Sustainable Energy Systems. URL: https://github.com/tum-ens/urbs (accessed: 03/25/2023)
6. Tachmukhammedov G. M., Tachmukhammedova B. B. Economic efficiency of rational use of electricity // Traditions and innovations in the education system. – 2019. – pp. 129-134.
7. Yerunov A. S. The service life of the car battery and its malfunctions // Innovations. The science. Education. – 2020. – No. 23. – pp. 663-665.
8. Hu H. et al. Battery life prediction // Joule. – 2020. – Vol. 4. – No. 2. – pp. 310-346.

Воробьев С. А., Разумов П. А., Трофимов Е.С. Энергетический баланс систем теплоснабжения с учетом эффекта ранжирования// Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 4(30) с. 96–101

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 62

ЭНЕРГЕТИЧЕСКИЙ БАЛАНС СИСТЕМ ТЕПЛОСНАБЖЕНИЯ С УЧЕТОМ ЭФФЕКТА РАНЖИРОВАНИЯ

Воробьев С. А., Разумов П. А., Трофимов Е. С.
ФГБОУ ВО "Санкт-Петербургский Государственный Архитектурно-Строительный Университет", Санкт-Петербург, Россия (190005, г. Санкт-Петербург, 2-я Красноармейская ул., д.4), e-mail: wolftier@mail.ru

Для моделирования теплоснабжения применена имитационная система моделирования. Модели оптимизирована для городских энергетических систем. Особое внимание уделено эффекту ранжирования, возникающему при использовании разных технологий отопления с различными переменными затратами. Было обеспечено условие одинаковых долей потребления тепла в зимнее и летнее время.

Ключевые слова: Теплоснабжение, имитационная модель, процессы, системы отопления, потери тепла.

ENERGY BALANCE OF HEAT SUPPLY SYSTEMS TAKING INTO ACCOUNT THE RANKING EFFECT

Vorobyev S.A., Razumov P.A., Trofimov E.S.
FSBEI of HE "St. Petersburg State University of Architecture and Civil Engineering", St. Petersburg, Russia (190005, St. *Petersburg, 2nd Krasnoarmeyskaya St., 4), e-mail: wolftier@mail.ru*

A simulation modeling system is used to simulate heat supply. The model is optimized for urban energy systems. Particular attention is paid to the ranking effect that occurs when using different heating technologies with different variable costs. The condition of equal shares of heat consumption in winter and summer was provided.

Keywords: *Heat supply, simulation model, processes, heating systems, heat loss.*

Первоначально модель VICUS была разработана для моделирования процессов преобразования одного вида энергоресурсов на входе в другой вид энергоресурсов на выходе [1]. VICUS - это модель линейного программирования для многотоварных энергетических систем с акцентом на оптимальные размеры и использование накопителей. С помощью этой программы моделируется энергетическая система с минимальной стоимостью, удовлетворяющая заданному временному ряду спроса на несколько товаров (например, электроэнергию). По умолчанию работает с часовыми интервалами (настраивается). Благодаря Pandas (быстрый, мощный, гибкий и простой в использовании инструмент анализа и манипулирования данными с открытым исходным кодом на основе языка программирования Python) выполняется комплексный анализ данных [2]. Сама модель имеет малый объем (<40 Кб исходного кода) и включает в себя функции создания отчетов и построения графиков. VICUS представляет собой упрощённую версию программы URBS [3]. Это оптимизационная модель линейного программирования для планирования расширения мощностей и

определения удельных затрат в распределенных энергетических системах. Его название, полатыни означающее "город", связано с его происхождением как модели оптимизации городских энергетических систем. С тех пор он был адаптирован к различным масштабам - от районов до континентов [4-6].

Имитационная модель определяет наиболее оптимальную (с точки зрения затрат) конфигурацию энергетической системы, что приводит к «ранжированию» в случае, когда для обеспечения изменяющихся во времени потребностей используются разные технологии с различными переменными затратами. Дополнительные сведения об эффекте ранжирования изложены Зенсфуссом и др. на примере электроэнергетического сектора в [7]. В случае электроэнергии этот эффект ожидается всегда, когда все технологии (т.е. сеть энерогоснабжения, солнечные панели и ветряные электростанции) фактически способны удовлетворять потребности в электроэнергии посредством сети распределения энергии.

Однако в случае потребления тепла каждое жилое и коммерческое здание для удовлетворения своих потребностей в отоплении использует отдельную отопительную систему [8, 9]. Соответственно, система отопления дома А не может быть использована для удовлетворения потребности в отоплении дома В. Однако, так как для целей моделирования все отдельные потребности в отоплении необходимо свести в единый профиль потребления, то в первоначальной модели VICUS такая ситуация могла иметь место.

В примере, описанном далее, эти обстоятельства раскрываются более подробно. Для обеспечения потребностей в тепле устанавливают две различные системы отопления, каждая из которых включает процесс генерации тепла и хранилище горячей воды. 30% от их количества составляют системы резистивного отопления электричеством, 70% используют природный газ. Считается, что системы второго типа имеют меньшие переменные затраты.

В течение зимних месяцев обе системы работают на полную мощность, покрывая потребность в отоплении помещений и горячей воде. Доли потребления тепла, покрываемого системами, составляют $\kappa_{рез}$(зима) = 30% и $\kappa_{газ}$(зима) = 70%, соответственно. В течение летних месяцев помещения не нуждаются в отоплении, поэтому потребление тепла снижается до уровня потребления горячей воды, которое в это время может обеспечивать любая из систем отопления. В первоначальной версии системы VICUS выбор был сделан в пользу газовых котлов ($\kappa_{газ}$(лето) = 100%), так как их переменные расходы меньше по сравнению с отопительной системой с резистивным нагревом (рис. 1). Недостатком этого решения является то, что домашние хозяйства и офисные здания, оборудованные электрическими системами отопления, должны будут отказаться от использования горячей воды ($\kappa_{рез}$(лето) = 0%), а в зданиях с системами отопления, работающими на природном газе, вырабатывается слишком много тепла.

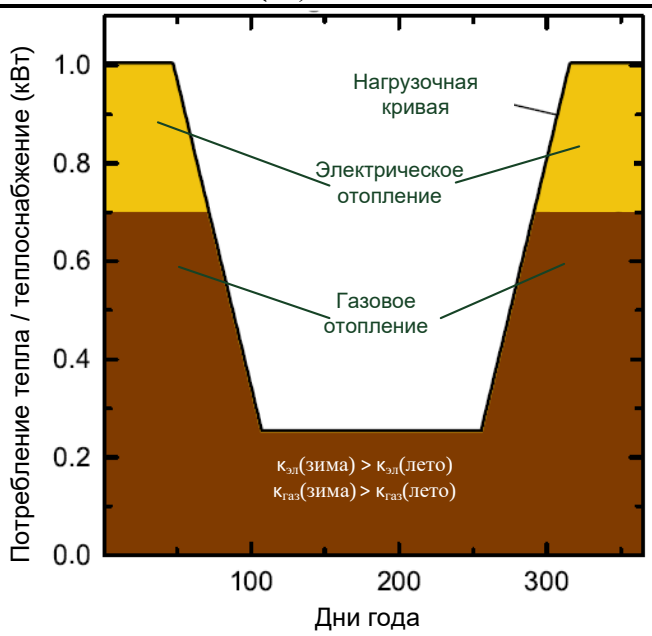


Рисунок 1 – Первоначальная версия модели VICUS

Для того, чтобы устранить этот эффект была введена дополнительная система уравнений и переменных. Это позволяет обеспечить, условие κ_p(зима) = κ_p(лето) = *const* для каждой системы отопления и покрывает фиксированную долю потребления тепла в течение всего года.

На первом этапе потребовалось сформировать четыре идентичные системы хранения горячей воды и присвоить каждую из них одному из четырех процессов отопления в имитационной модели: резистивное отопление электричеством; электрический тепловой насос, использующий теплоту воздуха; котлы, работающие на природном газе или топочном мазуте. На втором этапе для каждой системы была определена независимая от времени переменная κ_p, представляющая соответствующую долю потребления тепла, которая определяется как:

$$\kappa_p = \frac{E_p^{\text{out}}(t,c^{\text{in}},\text{heat}) + \overbrace{E_s^{\text{out}}(t,\text{heat}) - (E_s^{\text{in}}(t,\text{heat})}^{\Delta s} - \overbrace{E_{\text{w}}^{\text{in}}(t,\text{heat,потери})}^{\text{излишки генерации}}}{\underbrace{(D(t,\text{heat})\cdot\gamma(\text{heat})}_{\text{потребление тепла}}} \quad \forall\, t \in [1.8760]$$

где E_p^{out} – выходная энергия одного из четырех процессов,

t – время, E_s^{out} - выходная энергия хранилища, E_s^{in} - входная энергия хранилища,

E_{w}^{in} – энергия потерь,

Δ_s - количество энергии, отдаваемое или запасаемое соответствующим хранилищем горячей воды, c^{in} – исходный энергоресурс (солнечная энергия, энергия ветра, сетевое электричество, природный газ, мазут, теплоэнергия и др.),

heat – переменная модели, означающая «тепло»,

D(t,heat) – потребность в тепле, $\gamma(\text{heat})$ - пиковые нагрузки при потреблении тепла.

Например, для газового котла:

$$\kappa_{\text{кот\_газ}} = \frac{E^{\text{out}}_{\text{кот\_газ}}(t, \text{gas}, \text{heat}) + \overbrace{E^{\text{out}}_{\text{кот}}(t, \text{heat}) - (E^{\text{in}}_{\text{кот}}(t, \text{heat})}^{\Delta s} - \overbrace{E^{\text{in}}_{\text{w}}(t, \text{heat}, \text{потери})}^{\text{излишки генерации}}}{\underbrace{(D(t, \text{heat}) \cdot \gamma(\text{heat})}_{\text{потребление тепла}}}$$

Энергия потерь обеспечивает возможность выработки излишков тепла путем уничтожения избытков тепла. Это применимо только к случаям, в которых рассматриваются процессы комбинированного производства тепла и электроэнергии, так как в этом случае обеспечивается возможность генерации электроэнергии в периоды низкого потребления тепла или его отсутствия.

Последний этап заключается в введении ограничения, обеспечивающего покрытие потребностей в отоплении всеми процессами в совокупности, описывающееся уравнением вида:

$$\sum_{p} \kappa_p = \kappa_{\text{котел\_газ}} + \kappa_{\text{котел\_мазут}} + \kappa_{\text{рез}} + \kappa_{\text{насос}}$$

Значения переменной κ_p определяются во время работы имитационной модели. Результат этого подхода показан на Рисунке 2.

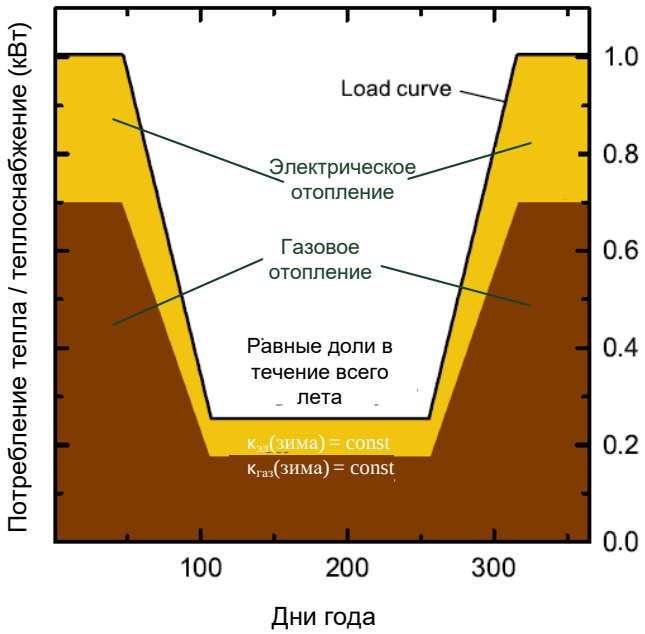


Рисунок 2 – Изменение модели VICUS с целью обеспечения реалистичного распределения тепла

Этот подход служит только для введения ограничения, обеспечивающего условие, что доля процесса снабжения тепла остается неизменной в течение года.

Выводы. Для уточнения имитационной модели теплоснабжения реализован подход ранжирования процессов отопления. Предложенный подход позволяет более рационально использовать энергию от различных видов источников и делает модель более точной. Соответственно, и результаты прогнозирования будут иметь большую точность и достоверность.

Список литературы

1. VICUS // Technical University of Munich – Institute of Renewable and Sustainable Energy Systems. URL: https://github.com/ojdo/vicus#readme (дата обращения: 25.03.2023)
2. Pandas URL: https://pandas.pydata.org/ (дата обращения: 25.03.2023)
3. Dorvner J., Hamacher T. URBS – a model of linear optimization of distributed energy systems // Technical University of Munich – Institute of Renewable and Sustainable Energy Systems. URL: https://github.com/tum-ens/urbs (дата обращения: 25.03.2023)
4. Hetterich B. et al. Optimal energy supply system and hourly operation plan for the TUM campus Garching using linear programming model URBS //Proceedings of ECOS 2016. – 2016. – С. 15.
5. Kriechbaum L., Scheiber G., Kienberger T. Grid-based multi-energy systems modelling, assessment, open source modelling frameworks and challenges // Energy, Sustainability and Society. – 2018. – Т. 8. – № 1. – С. 1-19.
6. Stüber M., Odersky L. Uncertainty modeling with the open source framework URBS // Energy Strategy Reviews. – 2020. – Т. 29. – С. 100486.
7. Sensfuß F., Ragwitz M., Genoese M. The merit-order effect: A detailed analysis of the price effect of renewable electricity generation on spot market prices in Germany // Energy policy. – 2008. – Т. 36. – № 8. – С. 3086-3094.
8. Гашо Е. Г., Козырь А. В. О комплексной оценке эффективности отопительных систем зданий в нерасчетных режимах // Известия высших учебных заведений. Проблемы энергетики. – 2003. – № 3-4. – С. 3-12.
9. Казачков В. С., Шалай В. В., Попов А. А. Расчет значения погрешности системы индивидуального учета и распределения потребления тепла в многоквартирных домах // Омский научный вестник. – 2009. – № 3 (83). – С. 141-144.

References

1. VICUS // Technical University of Munich – Institute of Renewable and Sustainable Energy Systems. URL: https://github.com/ojdo/vicus#readme (accessed: 03/25/2023)
2. Pandas URL: https://pandas.pydata.org / (accessed: 03/25/2023)
3. Dorvner J., Hamacher T. URBS – a model of linear optimization of distributed energy systems // Technical University of Munich – Institute of Renewable and Sustainable Energy Systems. URL: https://github.com/tum-ens/urbs (accessed: 03/25/2023)
4. Hetterich B. et al. Optimal energy supply system and hourly operation plan for the TUM campus Garching using linear programming model URBS //Proceedings of ECOS 2016. – 2016. – pp. 15.
5. Kriechbaum L., Scheiber G., Kienberger T. Grid-based multi-energy systems modeling, assessment, open source modeling frameworks and challenges // Energy, Sustainability and Society. – 2018. – Vol. 8. – No. 1. – pp. 1-19.
6. Stüber M., Odersky L. Uncertainty modeling with the open source framework URBS // Energy Strategy Reviews. – 2020. – Vol. 29. – pp. 100486.

7. Sensfuß F., Ragwitz M., Genoese M. The merit-order effect: A detailed analysis of the price effect of renewable electricity generation on spot market prices in Germany // Energy policy. - 2008. – Vol. 36. – No. 8. – pp. 3086-3094.
8. Gasho E. G., Kozyr A.V. On a comprehensive assessment of the efficiency of heating systems of buildings in non-accounting modes // Izvestiya higher educational institutions. Energy problems. - 2003. – No. 3-4. – pp. 3-12.
9. Kazachkov V. S., Shalai V. V., Popov A. A. Calculation of the error value of the system of individual accounting and distribution of heat consumption in apartment buildings // Omsk Scientific Bulletin. – 2009. – № 3 (83). – pp. 141-144.

Биткулов К.Р. и др. Анализ работы спроектированного комплекса РЗА при различных видах коротких замыканий // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 102–108

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 621

АНАЛИЗ РАБОТЫ СПРОЕКТИРОВАННОГО КОМПЛЕКСА РЗА ПРИ РАЗЛИЧНЫХ ВИДАХ КОРОТКИХ ЗАМЫКАНИЙ

Биткулов К.Р., Зализная Е.А., Зализный С.А., Умурзаков Д.Д.
ФГБОУ ВО "Национальный Исследовательский Университет"МЭИ", Москва, Россия (111250, Москва, Красноказарменная ул, д. 14, стр. 1), e-mail: madamliza2@yandex.ru

Разработан комплекс релейной защиты и автоматики для проектируемой ТЭЦ 3х32 МВт, выполненный на базе микропроцессорных терминалов фирм ООО НПП «ЭКРА» и ООО «НТЦ «Механотроника». В данной статье рассмотрено действие комплекса релейной защиты и автоматики при следующих повреждениях: КЗ на воздушной линии 110 кВ с успешным ТАПВ; КЗ на выводах НН трансформатора с отказом выключателя на его присоединении; КЗ в токоограничивающем реакторе кабельной линии, отходящей от генераторного РУ 10,5 кВ, с отказом срабатывания защиты шин.

Ключевые слова: Релейная защита, автоматика, дистанционная защита, воздушная линия, короткое замыкание.

ANALYSIS OF THE OPERATION OF THE DESIGNED RZA COMPLEX FOR VARIOUS TYPES OF SHORT CIRCUITS

Bitkulov K.R., Zaliznaya E.A., Zalizny S.A., Umurzakov D.D.
National Research University MPEI, Moscow, *Russia (111250, Moscow, Krasnokazarmennaya street, 14, bldg. 1), e-mail: madamliza2@yandex.ru*

A relay protection and automation complex has been developed for the projected 3x32 MW thermal power plant, made on the basis of microprocessor terminals of the companies NPP EKRA LLC and STC Mechanotronika LLC. This article discusses the operation of the relay protection and automation complex in the following damages: short circuit on the 110 kV overhead line with a successful TAPV; short circuit on the terminals of the transformer with a failure of the switch on its connection; short circuit in the current-limiting reactor of the cable line departing from the generator RC 10.5 kV, with a failure of the bus protection.

Keywords: Relay protection, automation, remote protection, overhead line, short circuit.

Для изображения временных диаграмм, поясняющих работу комплекса релейной защиты и автоматики (РЗА) при КЗ в различных точках схемы защищаемого объекта, необходимо принять несколько основных положений и допущений, касающихся схемы рассматриваемой сети и работы самого комплекса РЗА (Рисунок 1)[1]:

1. Для всех случаев отсчёт времени ведется от момента начала КЗ ($t = 0$ с).
2. Условно принимаем, что микропроцессорная защита реагирует на повреждение за время, равное 30 мс.

3. Предположим, что две рабочие системы шин работают в следующем режиме: шиносоединительный выключатель *QCE* разомкнут, первая система шин (*K1E*) является рабочей, к ней подключены все присоединения, а вторая (*K2E*) система шин является резервной. Секционные выключатели на РУ НН (*QC1G, QC2G)* нормально замкнуты, т.е. генераторы имеют поперечную связь.
4. Примем выдержку времени МТЗ фидеров 10,5 кВ равной $t_{\text{с.з.}} = 1{,}5$ с, как наиболее распространенный случай. Тогда время срабатывания МТЗ секционных выключателей $t_{\text{с.з. СВ}} = 1{,}5 + + 0{,}5 = 2{,}0$ с, а МТЗ НН трансформатора $t_{\text{с.з. МТЗ НН}} = 2{,}0 + 0{,}5 == 2{,}5$ с.

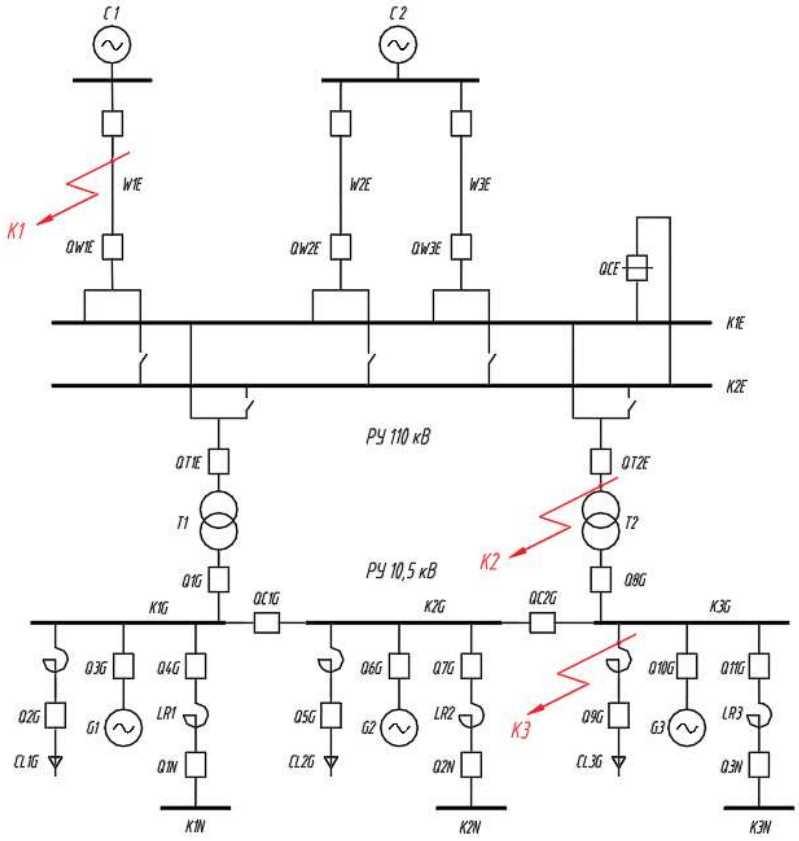


Рисунок 1 – Схема сети с наименованиями элементов и указанием точек КЗ

Рассмотрим следующее повреждение — трёхфазное короткое замыкание в конце линии *W1E.*

Для дифференциально-фазной защиты (ДФЗ) линии *W1E* данное КЗ внутреннее: с обоих концов срабатывают блокирующие пусковые органы и производят пуск высокочастотных (ВЧ) приемопередатчиков. Одновременно с блокирующими пусковыми органами срабатывают отключающие пусковые органы, и без выдержки времени (в принятой конфигурации терминала) разрешают работу органа сравнения фаз. Так как КЗ внутреннее, то уставка органа сравнения фаз однозначно превышена, и с минимальной выдержкой времени $T_{\text{ДФЗ}} = 0{,}01$ с происходит срабатывание ДФЗ. Срабатывание ДФЗ приводит к формированию сигнала "Запрет ВЧ", который действует:

- на срабатывание отключение выключателя своей стороны

- на останов ВЧ приемопередатчика, который вызывает срабатывание ДФЗ и отключение выключателя с другого конца линии

Отключение выключателя *QW1E* и выключателя на стороне системы *C1* происходит спустя время, равное сумме собственного времени отключения выключателей и времени гашения дуг, приблизительно за 60 мс.

Параллельно с ДФЗ пускались дистанционные защиты — все три ступени на линии *W1E* и третья ступень на смежных линиях, а также чувствительная ступень резервных защит стороны ВН трансформаторов *T1* и *T2*. Сработать данные защиты не успели, возврат защит произошел раньше, чем успели набраться выдержки времени защит.[2][1] Также при срабатывании ДФЗ был запущен алгоритм устройства резервирования отказа выключателя (УРОВ), при исчезновении тока произошел возврат схемы УРОВ.

После отключения повреждённой линии и возврата всех защит начинается набор выдержки времени автоматического повторного включения (АПВ), условно примем $t_{\text{АПВ}} = 1{,}0$ с. По истечению выдержки времени срабатывает АПВ, действует на включение выключателя *QW1E,* и затем, если КЗ было неустойчивое, АПВ на противоположном конце линии подаёт команду на включение своего выключателя.

Временные диаграммы представлены на Рисунке 2.

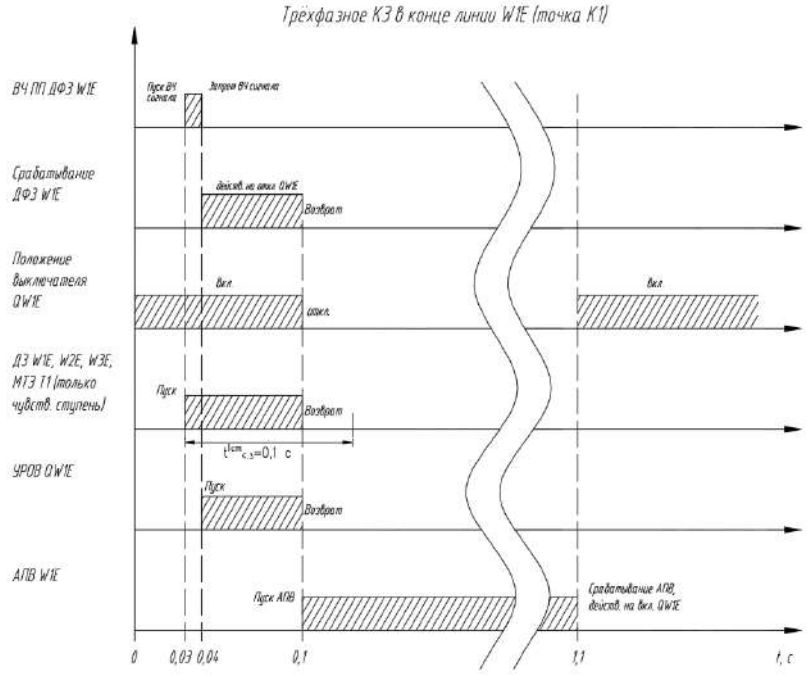


Рисунок 2 – Временные диаграммы при КЗ в точке К1

Рассмотрим междуфазное короткое замыкание на выводах ВН трансформатора *T2* с отказом выключателя *QT2E*.

$t = 0{,}03$ с: Пускаются защиты трансформатора Т2 (ДЗТ, МТЗ), ДЗТ без выдержки времени действует на отключение трансформаторных выключателей. От ДЗТ пускается алгоритм УРОВ и без выдержки времени дублирует команду на отключение выключателей. Начинается набор выдержки времени на отключение смежных элементов, $t_{\text{УРОВ}} = 0{,}3$ с.

[1] Для первой ступени ДЗ также была введена малая выдержка времени: $t^{\text{I}}_{\text{с.з.}} = 0{,}1$ с

$t = 0{,}09$ с: Выключатель на стороне НН (*Q8G*) отключается, выключатель на стороне ВН (*QT2E*) отказал и остаётся во включённом положении.

$t = 0{,}13$ с: Срабатывает первая ступень МТЗ ВН трансформатора, положение *QT2E* не изменятся.

$t = 0{,}33$ с: Выдержка времени УРОВ истекла, и алгоритм срабатывает, действуя через выходные цепи ДЗШ на отключение всех присоединений системы шин *K1E*.

$t = 0{,}36$ с: Через время, необходимое для срабатывания, отключаются выключатели линий 110 кВ и присоединения трансформатора *T1*. Происходит возврат всех защит.

По итогу, для локализации данного повреждения комплексу РЗА пришлось отключить полностью систему шин *K1E*, и, тем самым, изолировать станцию от энергосистем на время оперативных переключений, т.е. перевода названных выше присоединений на резервную систему шин *K2E*.

Временные диаграммы представлены на Рисунке 3.

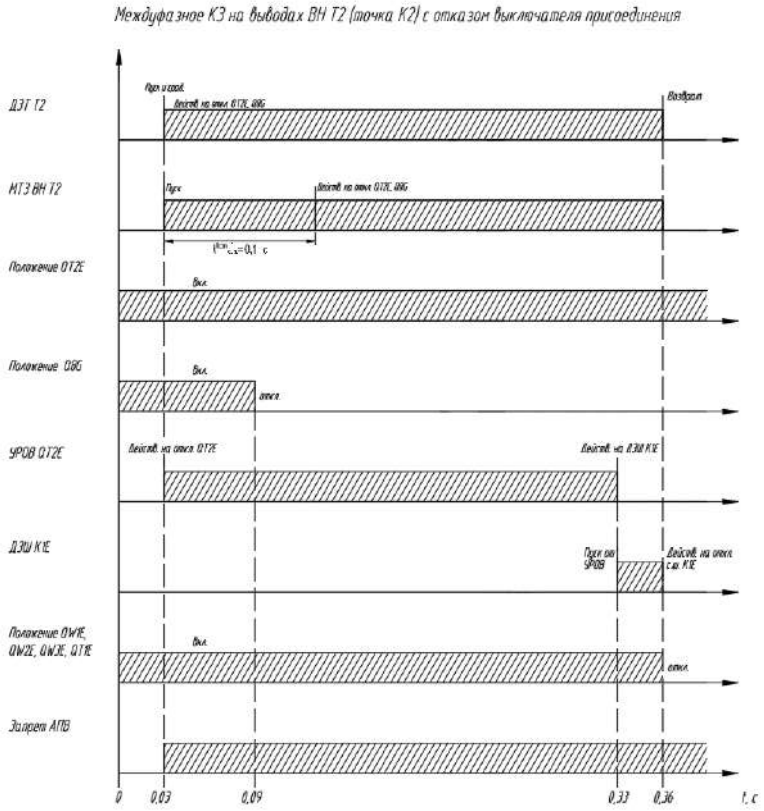


Рисунок 3 – Временные диаграммы при КЗ в точке К2

Повреждение: междуфазное КЗ в токоограничивающем реакторе, установленном на присоединении кабельной линии к ГРУ 10,5 кВ. Рассмотрим порядок действия защит, в случае несрабатывания основной защиты.

Данное повреждение находится в зоне действия двухступенчатой неполной дифференциальной защиты шин (НДЗШ). Первая ступень данной защиты должна подействовать без выдержки времени на отключение всех источников питания, за исключением генераторов, отключение которых осуществляется их токовыми защитами. Вторая ступень защиты, осуществляя ближнее резервирование, должна действовать с первой

выдержкой времени $t^{II}_{\text{с.з. НДЗШ, 1}} = 1{,}5 + 0{,}5 = 2{,}0$ с на отключение трансформатора *T2* и секционного выключателя (СВ) *QC2G*, и со второй выдержкой $t^{II}_{\text{с.з. НДЗШ, 2}} == 2{,}0 + 0{,}5 = 2{,}5$ с на отключение генератора, подключённых к повреждённой секции шин (*G3*).

Рассмотрим случай, когда первая ступень НДЗШ откажет в срабатывании, например, вследствие повреждения цепи отключения.

$t \approx 0$ с: Пускается основная защита, НДЗШ (обе ступени), и ряд смежных защит: МТЗ с комбинированным пуском по напряжению генератора *G3*, МТЗ секционного выключателя, МТЗ НН трансформатора *T2*, МТЗ реактированной линии питания собственных нужд (реактора *LR3*). Из-за отказа срабатывания первой ступени НДЗШ команд на отключение выключателей *QC2G*, *Q8G*, *Q11G* не подаётся. Начинают набираться выдержки времени резервных защит [3-4].

$t = 2{,}0$ с: Одновременно срабатывают II ступень НДЗШ, МТЗ с ПОН *G3* и МТЗ СВ. II ступень НДЗШ подаёт сигналы на отключение *QC2G*, *Q8G*, *Q11G*, предположим, что КЗ устойчивое, и сохраняется из-за подпитки от генератора. МТЗ с ПОН *G3* по истечению своей первой выдержки времени 2,0 секунды подействовала на деление шин — сформировала сигнал на отключение *QC2G*. МТЗ секционного выключателя *QC2G* так же сработала, и подала команду на деление шин.

$t = 2{,}5$ с: Защиты генератора и шин одновременно срабатывают на второй выдержке времени и подают команду на отключение генераторного выключателя *Q10G*, на автомат гашения поля (АГП) генератора *G3* и останов его турбины. Таким образом, генератор отключается, КЗ ликвидировано и происходит возврат защит.

Временные диаграммы представлены на Рисунке 4.

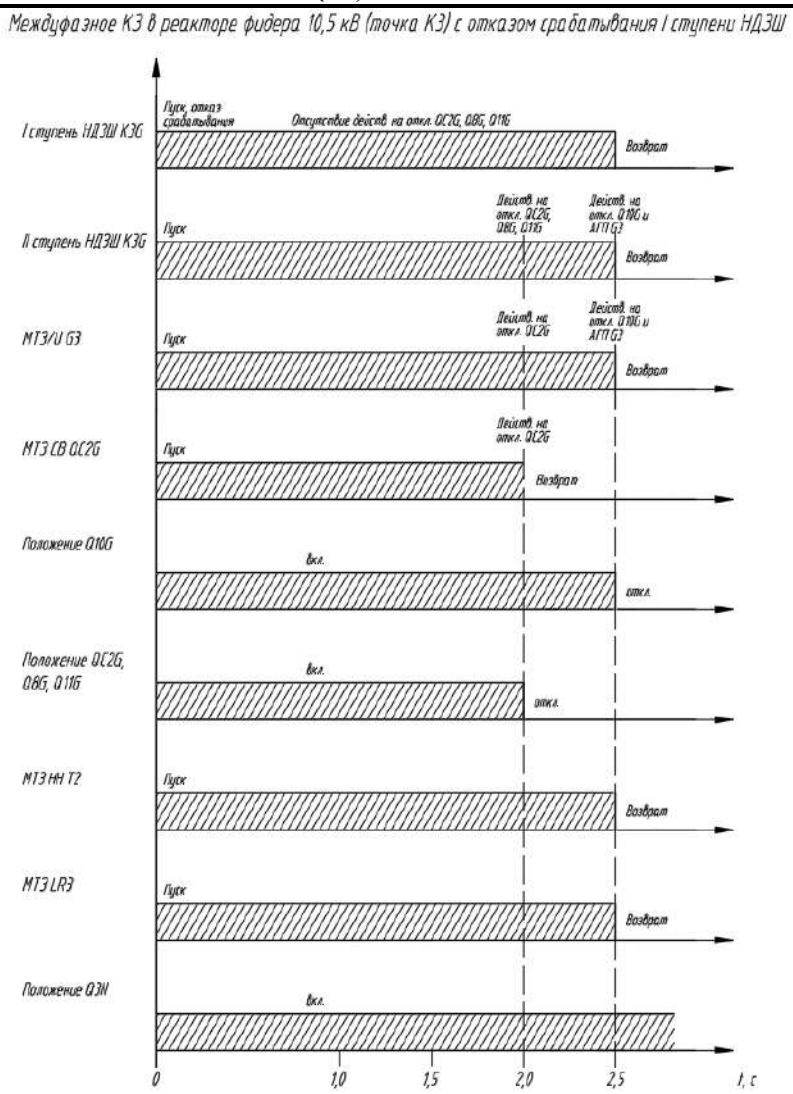


Рисунок 4 – Временные диаграммы при КЗ в точке К2

Так как релейная защита сети основана на принципе перекрытия защищаемых элементов зонами нескольких защит, то сеть оказалась успешно зарезервирована при отказах отдельных устройств РЗА. Тем не менее, последствия от отказа основных устройств РЗА обычно оказываются очень тяжёлыми для защищаемого оборудования либо для потребителей электроэнергии, поэтому при проектировании следует учитывать необходимость дублирования терминалов защит при соответственном обосновании.

Список литературы

1. Федосеев А.М. Релейная защита электрических систем. — М.: "Энергия", 1976.
2. Сборник лабораторных работ: Методическое пособие по курсу «Расчеты релейной защиты электроэнергетических систем» /Н.К. Давыдова, М.Н. Желнина, О.О. Николаева, Р.В. Темкина; под ред. Р.В. Темкиной. — М.: Издательство МЭИ, 2016. — 48 с.
3. СТО ДИВГ-048-2012. Линии электропередач 35–220 кВ. Дистанционная защита. Методика расчета уставок защит. СПб : НТЦ Механотроника, 2012.

4. СТО «Методические указания по выбору параметров срабатывания устройств РЗА подстанционного оборудования производства ООО НПП «ЭКРА» № 56947007-29.120.70.99-2011.

References

1. Fedoseev A.M. Relejnaya zashchita elektricheskih sistem. — M.: "Energiya", 1976.
2. Sbornik laboratornyh rabot: Metodicheskoe posobie po kursu «Raschety relejnoj zashchity elektroenergeticheskih sistem» /N.K. Davydova, M.N. ZHelnina, O.O. Nikolaeva, R.V. Temkina; pod red. R.V. Temkinoj. — M.: Izdatel'stvo MEI, 2016. — p. 48
3. STO DIVG-048-2012. Linii elektroperedach 35–220 kV. Distancionnaya zashchita. Metodika rascheta ustavok zashchit. SPb : NTC Mekhanotronika, 2012.
4. STO «Metodicheskie ukazaniya po vyboru parametrov srabatyvaniya ustrojstv RZA podstancionnogo oborudovaniya proizvodstva OOO NPP «EKRA» № 56947007-29.120.70.99-2011.

Биткулов К.Р. и др. Разработка и испытание алгоритма дистанционной защиты воздушной линии 110 кв в среде MATLAB // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 109–116

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 621

РАЗРАБОТКА И ИСПЫТАНИЕ АЛГОРИТМА ДИСТАНЦИОННОЙ ЗАЩИТЫ ВОЗДУШНОЙ ЛИНИИ 110 КВ В СРЕДЕ MATLAB

Биткулов К.Р., Зализная Е.А., Зализный С.А., Умурзаков Д.Д.
ФГБОУ ВО "Национальный Исследовательский Университет"МЭИ", Москва, Россия (111250, Москва, Красноказарменная ул, д. 14, стр. 1), e-mail: madamliza2@yandex.ru

В данной статье представлен результат разработки алгоритма дистанционной защиты воздушной линии электропередач, реализованный в графической среде моделирования и проектирования Simulink. Данная операционная среда входит в пакет прикладных программ Matlab, разработанный компанией MathWorks. Для моделирования электротехнических устройств и систем была применена встроенная в Simulink библиотека блоков SimPowerSystems.

Ключевые слова: MATLAB Simulink, алгоритм, воздушная линия, дистанционная защита, энергетика..

DEVELOPMENT AND TESTING OF AN ALGORITHM FOR REMOTE PROTECTION OF A 110 KV OVERHEAD LINE IN A MATLAB ENVIRONMENT

Bitkulov K.R., Zaliznaya E.A., Zalizny S.A., Umurzakov D.D.
National Research University MPEI, Moscow, *Russia (111250, Moscow, Krasnokazarmennaya street, 14, bldg. 1), e-mail: madamliza2@yandex.ru*

This article presents the result of the development of an algorithm for remote protection of an overhead power line implemented in the Simulink graphical modeling and design environment. This operating environment is included in the Matlab application software package developed by MathWorks. To simulate electrical devices and systems, a library of SimPowerSystems blocks built into Simulink was used.

Keywords: MATLAB Simulink, algorithm, overhead line, remote protection, power engineering.

Дистанционными называют направленные защиты с относительной селективностью, выполняемые с использованием реле минимального сопротивления.

Для реле сопротивления (РС) отношение напряжения на "зажимах" реле к току в реле пропорционально расстоянию (т.е. — дистанции) от места КЗ до места установки защиты, что определило название защиты.

Разработка и испытание алгоритма будет осуществлено на примере терминала БМРЗ-ЛТ-62 фирмы «Механотроника» [1], для которого были рассчитаны уставки. В рамках данной работы рассмотрен алгоритм дистанционной защиты только от междуфазных КЗ (ДЗМФ), без учёта составляющих нулевой последовательности. Моделирование и испытание

дистанционной защиты будет производиться непосредственно для схемы сети, представленной на Рисунке 1. Результат моделирования представлен на Рисунке 2.

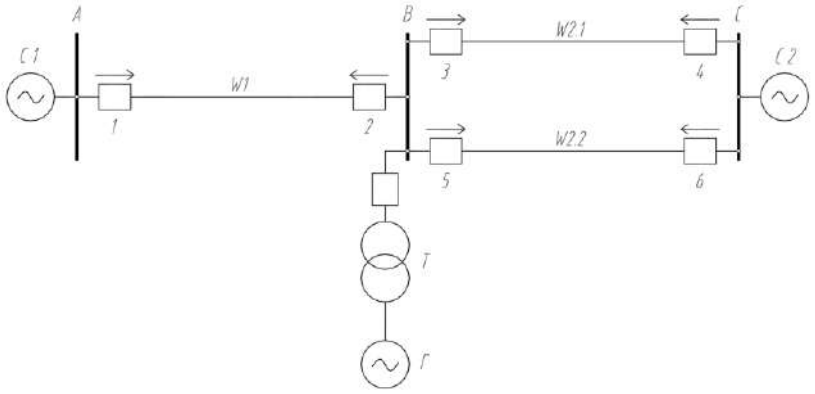


Рисунок 1 – Схема размещения полукомплектов ДФЗ на ВЛ 110 кВ

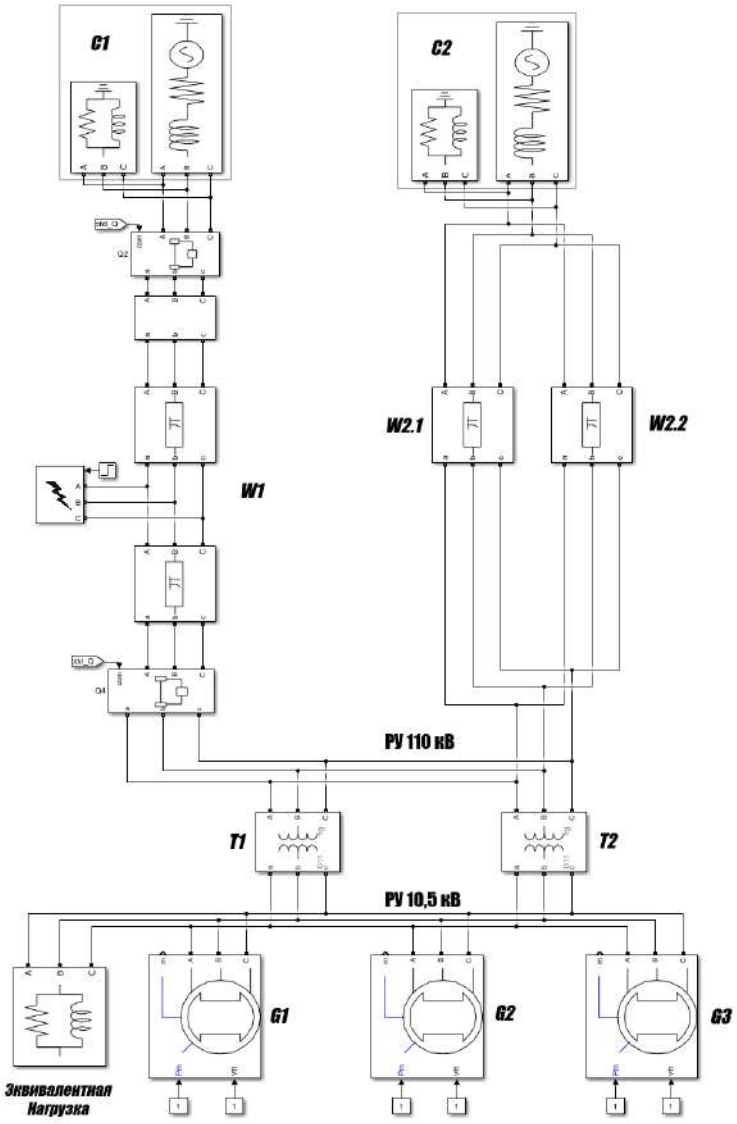


Рисунок 2 – Схема сети в Simulink

В общем виде алгоритм работает по следующему принципу: на вход модели ДЗ от блока измерений подаются трёхфазные сигналы токов и напряжений, преобразовываются в значения активных и индуктивных сопротивлений «на зажимах» цифровых РС; далее алгоритм по заданным значениям уставок определяет, попадает ли измеренное значение внутрь области срабатывания РС; логическая часть формирует сигнал "1", в случае срабатывания защиты и передаёт его, инвертируя, на выход модели, таким образом на блок выключателя поступит сигнал "0" и произойдет отключение.

На рис. 3 представлен общий интерфейс модели, а также названия сигналов, которые будут сняты при испытании алгоритма. Рабочая область в Simulink содержит блок powergui, который обеспечивает расчёт электрической схемы методами Matlab [2]. Был выбран метод дискретизации электрической системы с расчетом на фиксированных временных отрезках с шагом $5{,}5 \cdot 10^{-5}$ с.

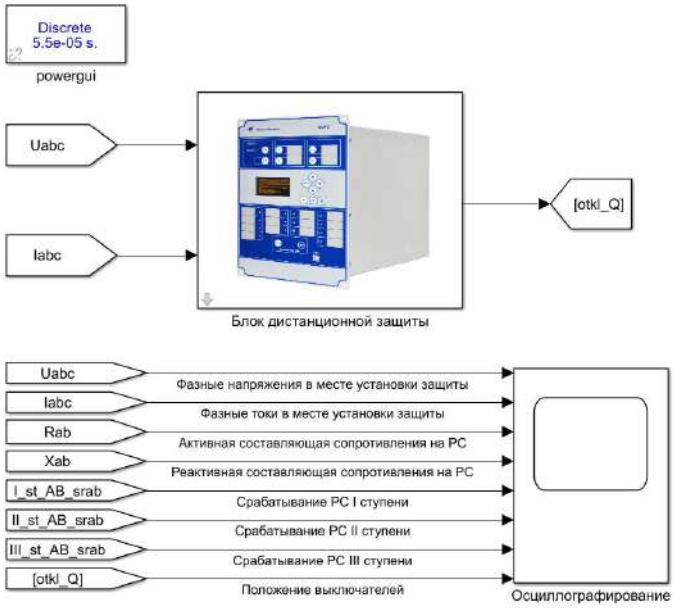


Рисунок 3 – Интерфейс модели ДЗ в Simulink

Для каждого случая были сняты осциллограммы токов и напряжений в месте установки защиты, показания ИОС, сигналы срабатывания трёх ступеней защиты, положение выключателя. Осциллограммы представлены на Рисунках 5, 6 и 7.

Входные сигналы U_{abc} и I_{abc} со входов модели преобразуются от первичных величин ко вторичным через коэффициенты трансформации измерительных ТТ и ТН, задаваемые в модель через интерфейс (рис. 4). Преобразованные сигналы проходят поступают на блоки фильтров Фурье, которые используются для выделения из измеренных мгновенных значений токов и напряжений ортогональных составляющих по прямоугольной системе координат, другими словами, мнимой и действительной частей.

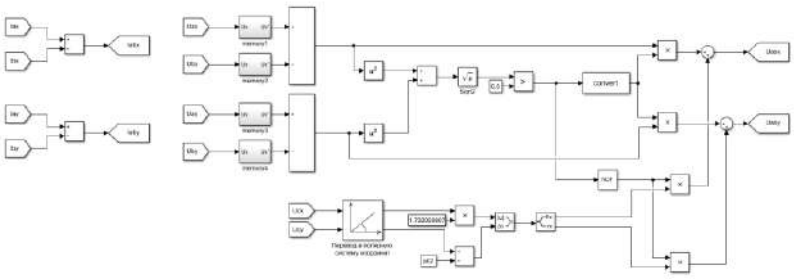


Рисунок 4 – Формирование междуфазных значений токов и напряжений

Далее необходимо для каждого измерительного РС рассчитать соответствующие ему сопротивление R и X [3]. Таким образом будут сформированы сигналы на РС, которые являются параметром, по которому определяется срабатывание защиты. Переход от токов и напряжений к сопротивлениям осуществляется по следующим формулам:

$$R = \frac{Re(U) \cdot Re(I) + Im(U) \cdot Im(I)}{Re(I)^2 + Im(I)^2}, \quad (1)$$

$$X = \frac{Im(U) \cdot Re(I) + Re(U) \cdot Im(I)}{Re(I)^2 + Im(I)^2} \quad (2)$$

Испытание алгоритма проведено для комплекта ДЗ №1, для которого были предварительно рассчитаны уставки и характеристики срабатывания трёх ступеней. Смоделированы три случая КЗ в рассматриваемой схеме сети (Рисунок 1):

1. Трёхфазное КЗ в середине линии W1 — точка К1.
2. Двухфазное КЗ в конце линии W1 — точка К2.
3. Двухфазное КЗ в конце линии W2 — точка К3.

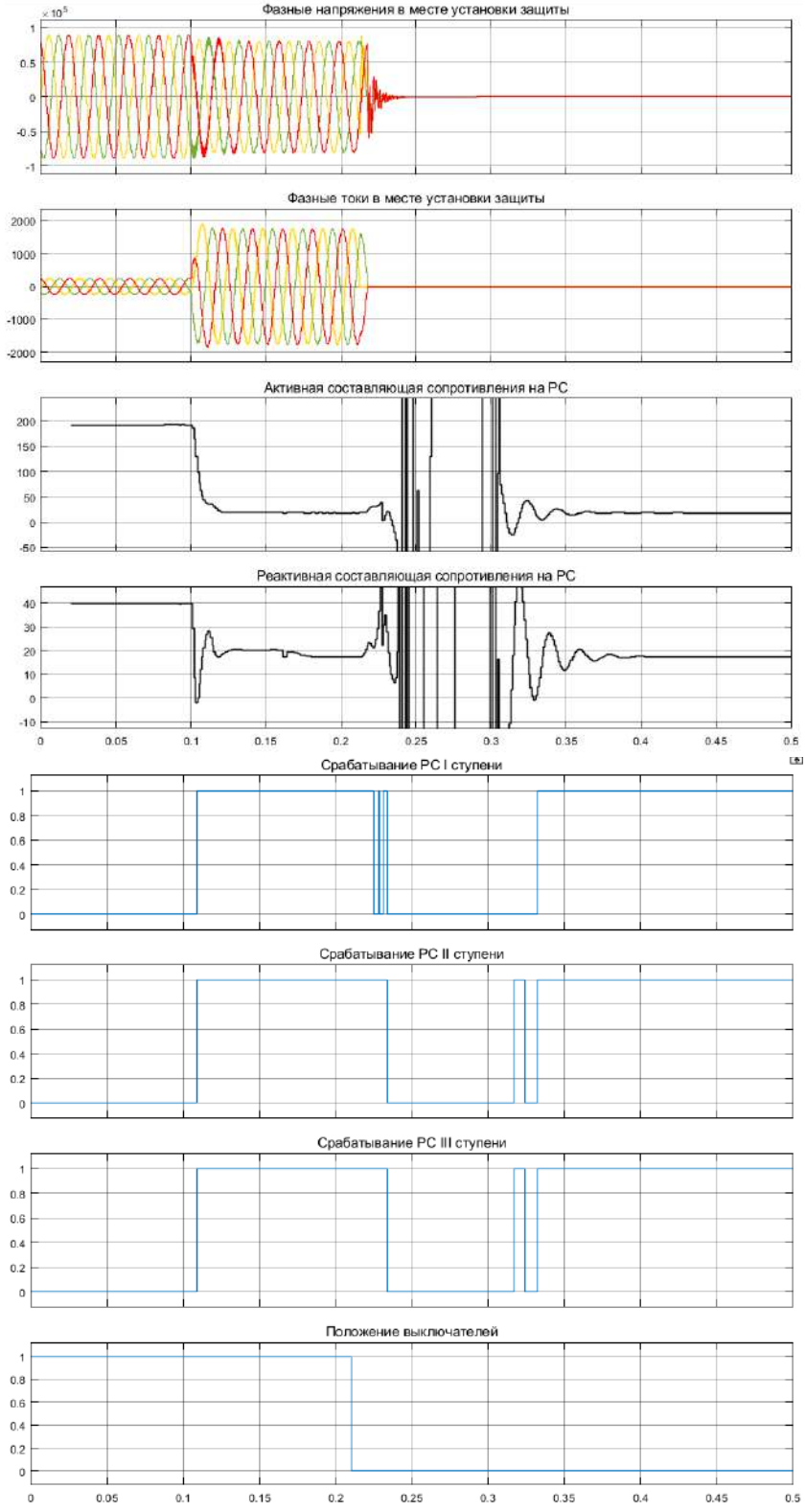


Рисунок 5 – Осциллограммы при КЗ в точке К1

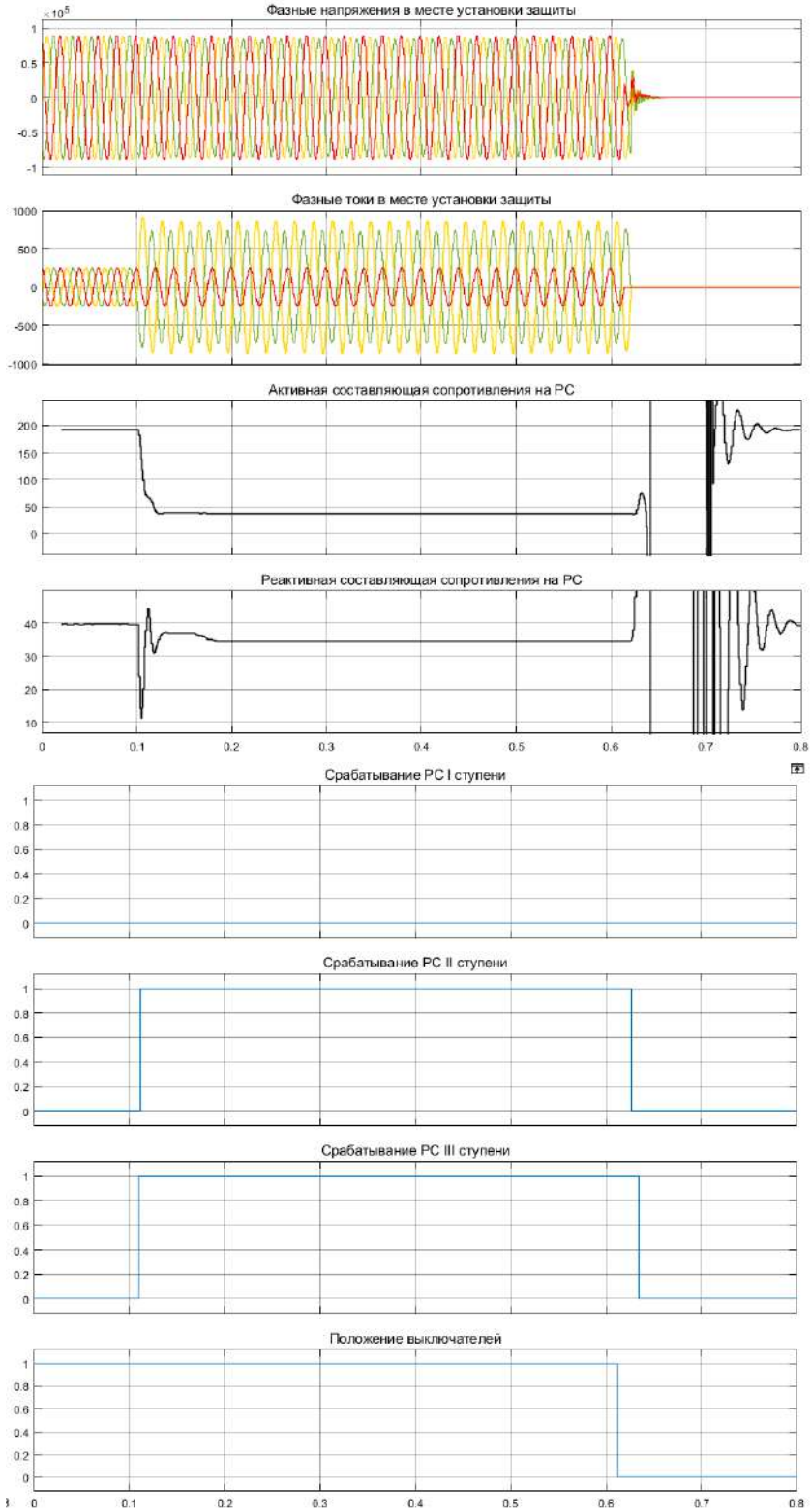


Рисунок 6 – Осциллограммы при КЗ в точке К2

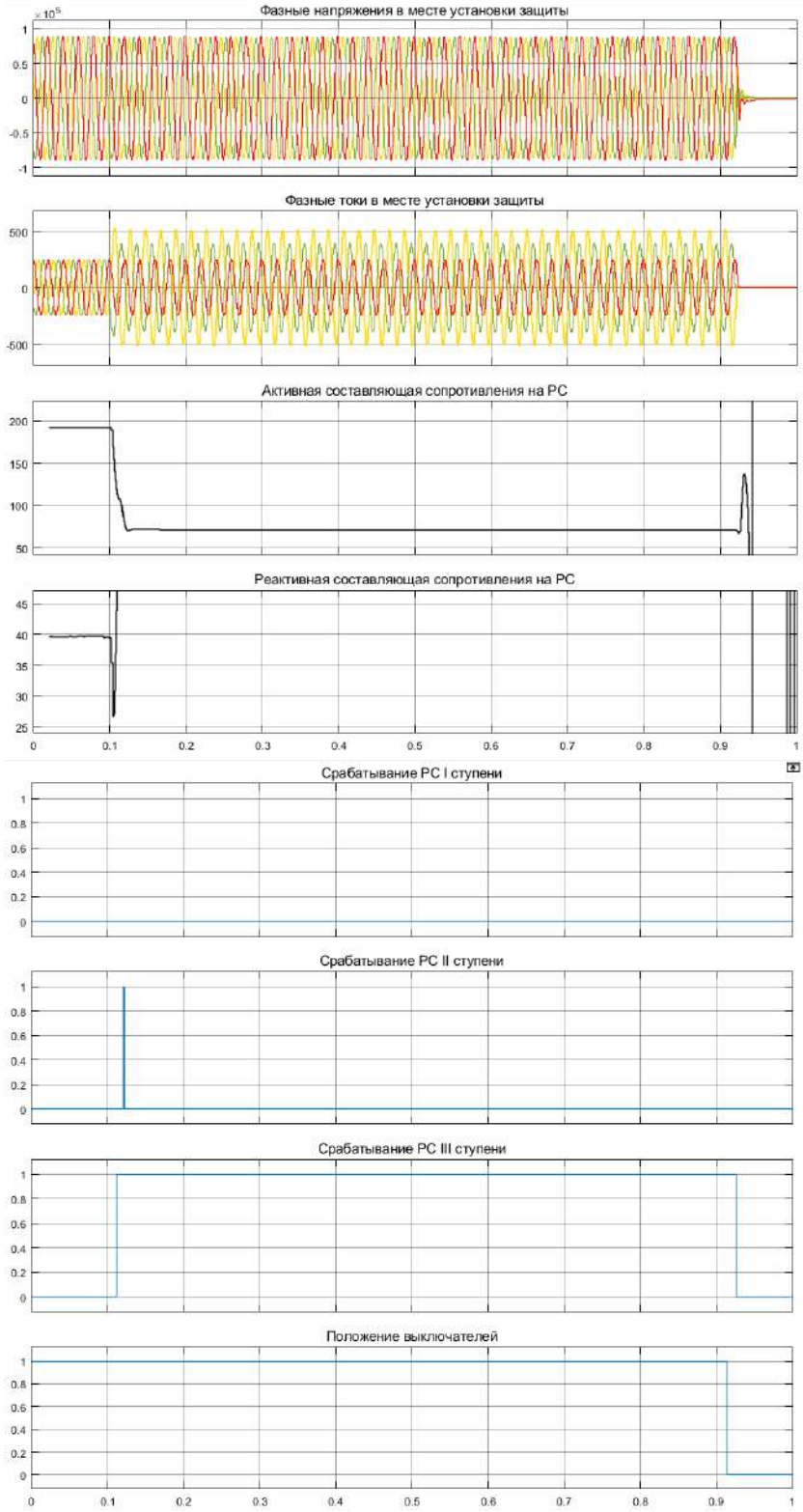


Рисунок 7 – Осциллограммы при КЗ в точке К3

Как видно из полученных осциллограмм, алгоритм работает успешно в каждом из испытаний. Повреждения отключаются селективно, все ступени защиты действуют чётко по своим зонам. Время отключения КЗ приблизительно соответствует выдержке времени защиты, отличаясь на величину задержки срабатывания выключателя и прочих задержек при

работе блоков схемы. Стоит отметить, что в результатах присутствуют погрешности, которые, в целом, не влияют на конечный результат — защита успешно отключает свой выключатель.

Список литературы

1. СТО «Нормы технологического проектирования подстанций переменного тока с высшим напряжением 35–750 кВ (НТП ПС)» № 56947007-29.240.10.248-2017.
2. Черных, И.В. Моделирование электротехнических устройств в MATLAB, SimPowerSystems и Simulink. — М.: ДМК Пресс; СПб.: Питер, 2008. — 288 с.: ил.
3. СТО ДИВГ-048-2012. Линии электропередач 35–220 кВ. Дистанционная защита. Методика расчета уставок защит. СПб : НТЦ Механотроника, 2012.

References

1. STO «Normy tekhnologicheskogo proektirovaniya podstancij peremennogo toka s vysshim napryazheniem 35–750 kV (NTP PS)» № 56947007-29.240.10.248-2017.
2. CHernyh, I.V. Modelirovanie elektrotekhnicheskih ustrojstv v MATLAB, SimPowerSystems i Simulink. — M.: DMK Press; SPb.: Piter, 2008. — 288 s.: il.
3. STO DIVG-048-2012. Linii elektroperedach 35–220 kV. Distancionnaya zashchita. Metodika rascheta ustavok zashchit. SPb : NTC Mekhanotronika, 2012.

Биткулов К.Р. и др. Разработка и испытание алгоритма дифференциально-фазной защиты линии в среде MATLAB // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 117–124

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 621

РАЗРАБОТКА И ИСПЫТАНИЕ АЛГОРИТМА ДИФФЕРЕНЦИАЛЬНО-ФАЗНОЙ ЗАЩИТЫ ЛИНИИ В СРЕДЕ MATLAB

Биткулов К.Р., Зализная Е.А., Зализный С.А., Умурзаков Д.Д.
ФГБОУ ВО "Национальный Исследовательский Университет"МЭИ", Москва, Россия (111250, Москва, Красноказарменная ул, д. 14, стр. 1), e-mail: madamliza2@yandex.ru

Цель данной статьи — разработка функционирующей модели, реализующей алгоритм дифференциально-фазной токовой защиты с высокочастотной блокировкой (далее — ДФЗ) при помощи среды моделирования MATLAB Simulink, а также проведение необходимых опытов, демонстрирующих корректность работы модели. Это позволит наглядно представить работу микропроцессорного терминала с функцией ДФЗ и понять его логику. Разработка проведена на основании руководства по эксплуатации терминала БМРЗ-ДФЗ-51.

Ключевые слова: MATLAB, алгоритм, воздушная линия, дифференциально-фазная защита, энергетика.

DEVELOPMENT AND TESTING OF THE DIFFERENTIAL-PHASE LINE PROTECTION ALGORITHM IN THE MATLAB ENVIRONMENT

Bitkulov K.R., Zaliznaya E.A., Zalizny S.A., Umurzakov D.D.
National Research University MPEI, Moscow, *Russia (111250, Moscow, Krasnokazarmennaya street, 14, bldg. 1), e-mail: madamliza2@yandex.ru*

The purpose of this article is to develop a functioning model that implements the algorithm of differential—phase current protection with high-frequency blocking (hereinafter referred to as DF) using the MATLAB Simulink modeling environment, as well as conducting the necessary experiments demonstrating the correctness of the model. This will allow you to visualize the operation of the microprocessor terminal with the DPZ function and understand its logic. The development was carried out on the basis of the operating manual of the terminal BMRZ-DFZ-51.

Keywords: MATLAB, algorithm, overhead line, differential-phase protection, power engineering.

ДФЗ является основной защитой воздушной линии с абсолютной селективностью. Принцип действия защиты основан на косвенном сравнении фаз токов с двух сторон линии. Для работы защиты требуются два полукомплекта БМРЗ-ДФЗ [1], установленных на противоположных концах защищаемой линии. Связь между полукомплектами может быть реализована как по высокочастотным (далее — ВЧ), так и по волоконно-оптическим каналам связи [2]. В статье рассмотрен первый вариант, как наиболее часто применяемый. Упрощенная

структурная схема ДФЗ изображена на Рисунке 1. На Рисунке 2 представлена упрощенная схема взаимодействия полукомплектов ДФЗ.

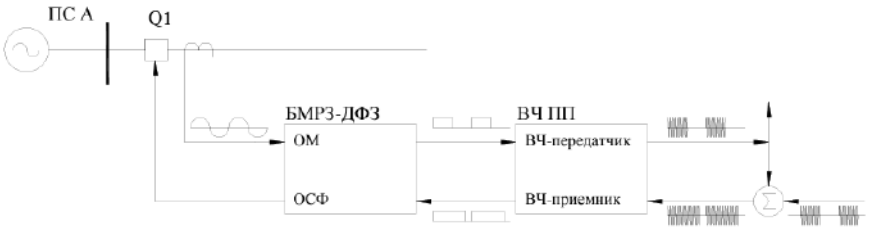


Рисунок 1 – Структурная схема ДФЗ

При внешних КЗ (точка К1) токи манипуляции на концах защищаемой линии электропередачи (ЛЭП) находятся в противофазе, пакеты ВЧ сигналов, посылаемые с разных концов ЛЭП, сдвинуты относительно друг друга на 180º, образуя тем самым сплошной сигнал в ВЧ канале [3]. Орган сравнения фаз не срабатывает.

При внутренних КЗ (точка К2) фазы токов манипуляции по концам защищаемой ЛЭП примерно равны. Огибающая ВЧ сигнала образует меандр, что приводит к срабатыванию органа сравнения фаз и отключению линии.

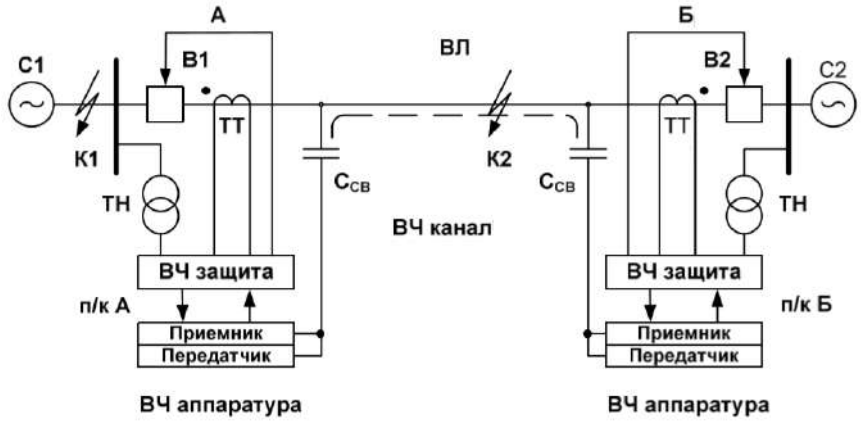


Рисунок 2 – Упрощенная схема взаимодействия полукомплектов ДФЗ

Исследование алгоритма произведено на примере опытной сети, представленной на Рисунке 3. Так как моделируемая защита имеет практически идеально абсолютную селективность, то нет необходимости моделировать всю схему сети. Достаточно рассмотреть одно из присоединений воздушных линий к шинам РУ 110 кВ опытной ТЭЦ — выберем для этого линию W1E, связывающую электростанцию с приёмной энергосистемой.

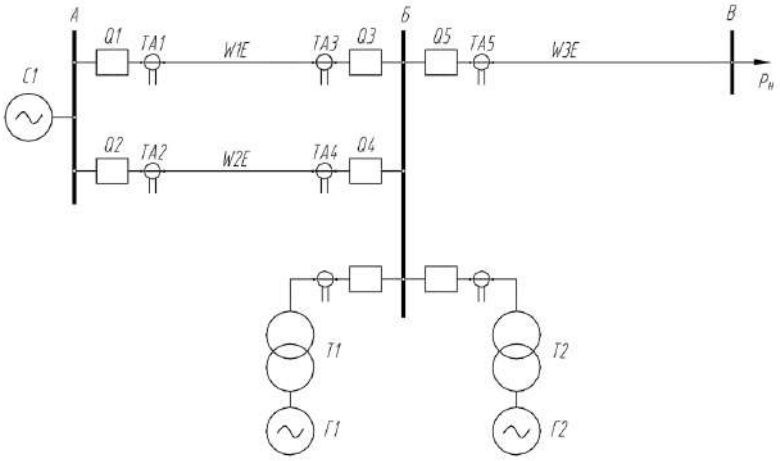


Рисунок 3 – Принципиальная схема опытной электростанции

Защита, установленная с каждой стороны защищаемой линии, включает в себя 2 полукомплекта, расположенных по обоим ее концам и состоящих из микропроцессорного терминала релейной части защиты и высокочастотного оборудования.

На Рисунке 4 представлена модель защищаемой линии и блок ДФЗ, свернутый в подсистему.

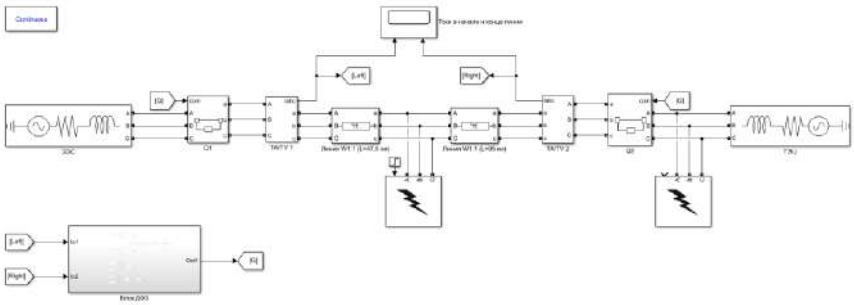


Рисунок 4 – Модель сети в MATLAB

Параметры, передаваемые в модель:

Номинальное напряжение сети: $U_{\text{с}} = 110$ кВ

Длина линии W1E: $l = 95$ км

Значения выбранных уставок:

- Уставка ОМ по коэффициенту K_{Φ} комбинированного фильтра токов:
$$K_{\Phi} = 3{,}0;$$
- Уставки ПО (отключающие) для обоих полукомплектов:
$$I_{\text{л от}} = 79{,}7 \text{ А};$$
- Уставка ОСФ по углу, при котором происходит блокирование действия защиты на отключение, регулируется в пределах от ±40° до ±65°. ОСФ срабатывает при одной паузе в ВЧ сигнале, равной или большей 90°;

- Уставка длительности скважности: Половина периода = 0,01 с = 180°. Срабатывание при наличии скважности длительностью более 20 % (примерно 40°) от половины периода (t = 0,008 с).

Для испытания алгоритма были смоделированы три разных вида короткого замыкания в разных точках моделируемой сети:

1. Точка К1 — внутреннее однофазное КЗ на землю в середине линии;
2. Точка К2 — внутреннее двухфазное КЗ в конце линии;
3. Точка К3 — внешнее трехфазное КЗ со стороны системы.

Для каждого случая были сняты осциллограммы, показывающие сигналы в разных точках алгоритма: первичные токи от ТА, ток манипуляции, ток на входе пускового органа (для примера показана составляющая прямой последовательности), срабатывание ПО, пакеты ВЧ импульсов на приемнике, сигнал на отключение. Сигналы снимались только для левого полукомплекта ввиду симметричности схемы.

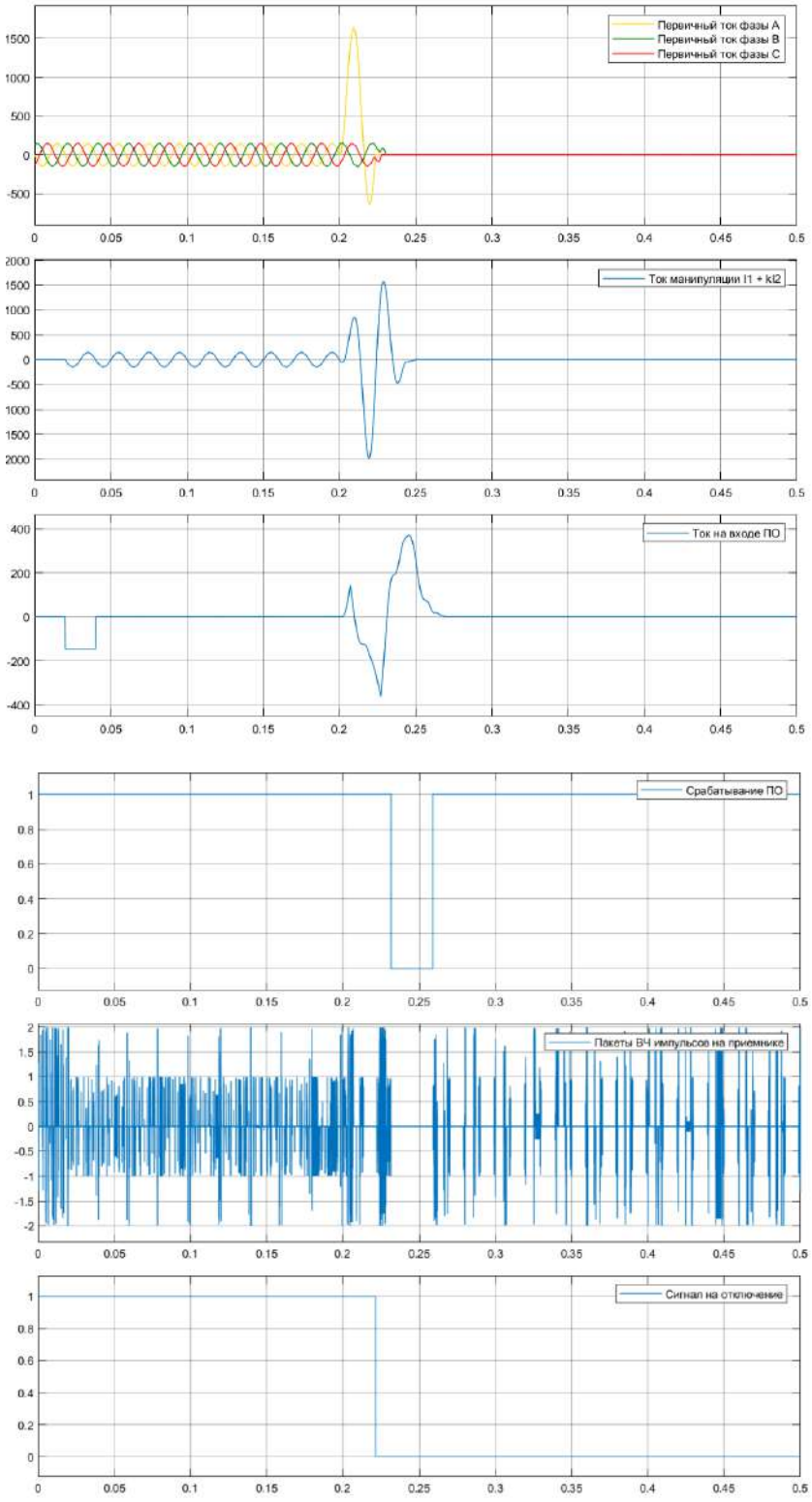


Рисунок 5 – Осциллограммы при КЗ в точке К1

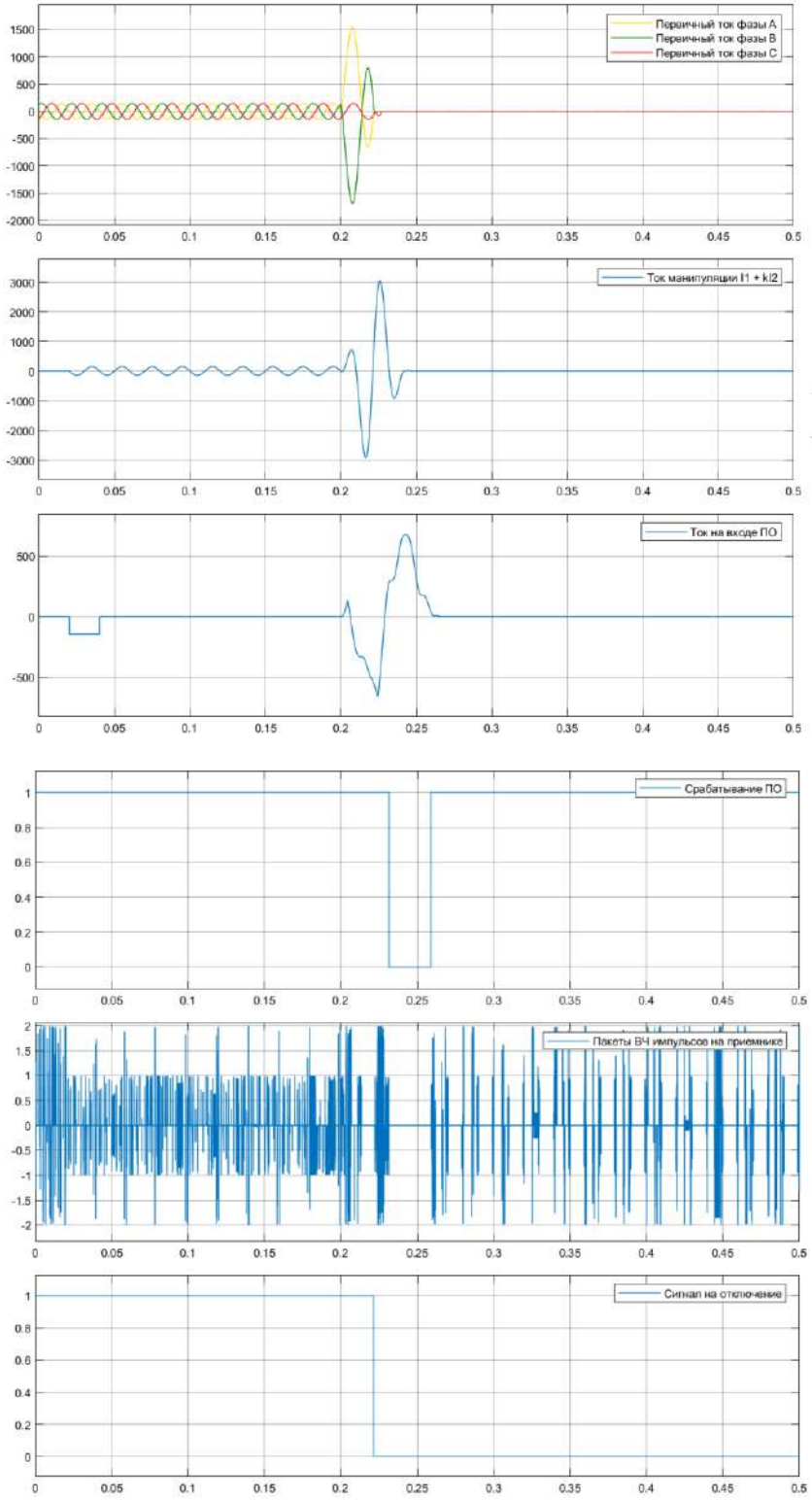


Рисунок 6 – Осциллограммы при КЗ в точке К2

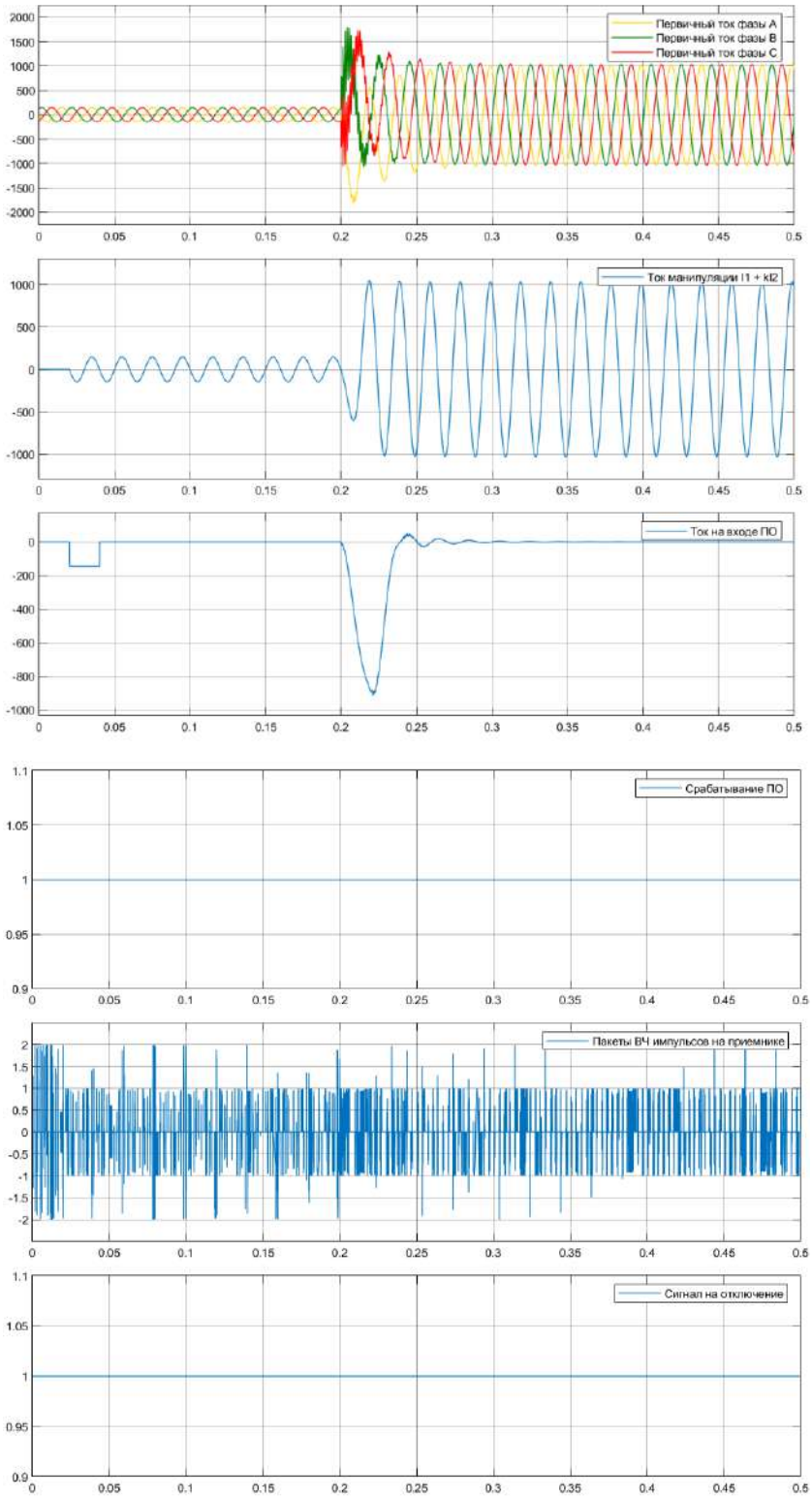


Рисунок 7 – Осциллограммы при КЗ в точке К3

Из полученных в результате испытаний осциллограмм видно, что разработанный алгоритм ДФЗ срабатывает и подает команду на отключение выключателя вне зависимости от места происхождения и вида КЗ в пределах защищаемой линии и не срабатывает при внешнем повреждении. Чувствительность и точность работы алгоритма подтверждается тем, что

защита реагирует и отключает КЗ с минимальным током повреждения — в середине линии, и не реагирует на внешнее КЗ с максимальным током — трёхфазное на шинах системы.

Список литературы

1. СТО ДИВГ.648228. .080-14.03 РЭ1. Блок микропроцессорный релейной защиты БМРЗ-ДФЗ-51. Руководство по эксплуатации. СПб.: НТЦ Механотроника, 2020.
2. Черных, И.В. Моделирование электротехнических устройств в MATLAB, SimPowerSystems и Simulink. — М.: ДМК Пресс; СПб.: Питер, 2008. — 288 с.: ил.
3. Правила устройства электроустановок (ПУЭ). — 7-е изд. Глава 3.2, раздел 3. — М. : Ростехнадзор, 2010. — 411 с.

References

1. STO DIVG.648228. .080-14.03 RE1. Blok mikroprocessornyj relejnoj zashchity BMRZ-DFZ-51. Rukovodstvo po ekspluatacii. SPb.: NTC Mekhanotronika, 2020.
2. CHernyh, I.V. Modelirovanie elektrotekhnicheskih ustrojstv v MATLAB, SimPowerSystems i Simulink. — M.: DMK Press; SPb.: Piter, 2008. — p.288: il.
3. Pravila ustrojstva elektroustanovok (PUE). — 7-e izd. Glava 3.2, razdel 3. — M. : Rostekhnadzor, 2010. — p.411.

Балтиков Д. Ф. и др. Электроснабжение базовой станции сотовой связи на базе фото-ветро-дизельных энергоустановок // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 125–129

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 621.311.6

ЭЛЕКТРОСНАБЖЕНИЕ БАЗОВОЙ СТАНЦИИ СОТОВОЙ СВЯЗИ НА БАЗЕ ФОТО-ВЕТРО-ДИЗЕЛЬНЫХ ЭНЕРГОУСТАНОВОК

Балтиков Д. Ф., Муратова Э. Ф., Ибрагимов Д. Р., Габдуллина И. И.
ФГБОУ ВО "Башкирский Государственный Аграрный Университет", Уфа, Россия (450001, Республика Башкортостан, г. Уфа, ул. 50-летия Октября, д. 34), e-mail: elviramuratova200@gmail.com

Условием нормального и бесперебойного функционирования базовой станции мобильной связи является качественное обеспечение электроснабжения. Поэтому при проектировании и строительстве особое внимание необходимо уделить электропитанию всех элементов сети мобильной связи, таких как базовые станции и оборудование управления базовыми станциями. В данной работе анализируется схема системы электроснабжения (СЭС) для базовой станции с генераторными установками, подключенной к промежуточным шинам постоянного тока (и при смешанном подключении), а также анализируются общие нормативные требования к базовым станциям сотовой связи для обеспечения надежности электроснабжения.

Ключевые слова: Децентрализованная базовая станция сотовой связи, фотоэлектрическая установка, шина постоянного тока, солнечная панель, ветрогенератор, система электроснабжения.

POWER SUPPLY TO BASE STATIONS OF CELLULAR COMMUNICATION ON THE BASIS OF PHOTO-WIND-DIESEL POWER PLANTS

Baltikov D. F., Muratova E. F., Ibragimov D. R., Gabdullina I. I.
FSBEI of HE "Bashkir State Agrarian University", Ufa, Russia (450001, Republic of Bashkortostan, Ufa, 50-letiya Oktyabrya street, 34), e-mail: elviramuratova200@gmail.com

The condition for the normal and uninterrupted functioning of a mobile communication base station is a high-quality power supply. Therefore, when designing and building, special attention must be paid to the power supply of all elements of the mobile communication network, such as base stations and base station control equipment. This paper analyzes the scheme of the power supply system (PSS) for a base station with generator sets connected to the intermediate DC bus (and mixed connection), and also analyzes the general regulatory requirements for cellular base stations to ensure the reliability of power supply.

Keywords: decentralized cellular base station, photovoltaic installation, DC bus, solar panel, wind generator, power supply system.

Наиболее известный вариант СЭС на базе шины постоянного тока показан на Рисунке 1.

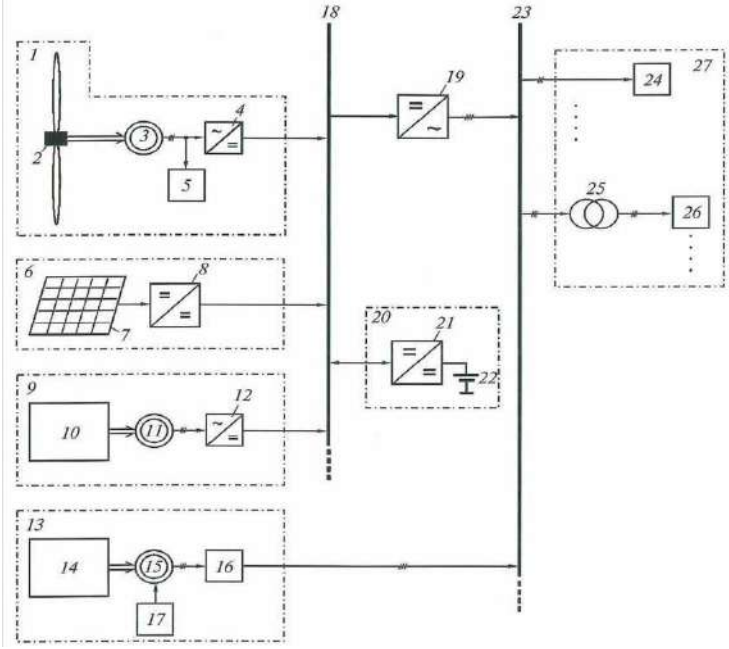


Рисунок 1 – Схема базовой станции СЭС с генераторными установками, подключенными к промежуточной шине постоянного тока (иногда со смешанным подключением):

1 – ветряная электростанция; 2 – ветровая турбина; 3, 11, 15 – синхронные электромашинные генераторы; 4, 12 – управляемые выпрямители; 5 – балластный блок нагрузок; 6 – фотоэлектрическая установка; 7– фотоэлектрическая панель; 8 – преобразователь напряжения; 9, 13 – дизель-генераторы; 16 – устройство плавного пуска; 17 – регулятор тока возбуждения; 18 – шина постоянного тока; 19 – инвертор напряжения; 20 – буферный накопитель энергии; 21 – двунаправленный импульсный преобразователь; 22 – блок АБ; 23 – шина переменного тока 220/380 В, 50 Гц; 24 – потребители 230/400 В; 25 – силовой повышающий трансформатор; 26 – потребители 6 или 10 кВ; 27 – объект децентрализованного электроснабжения.

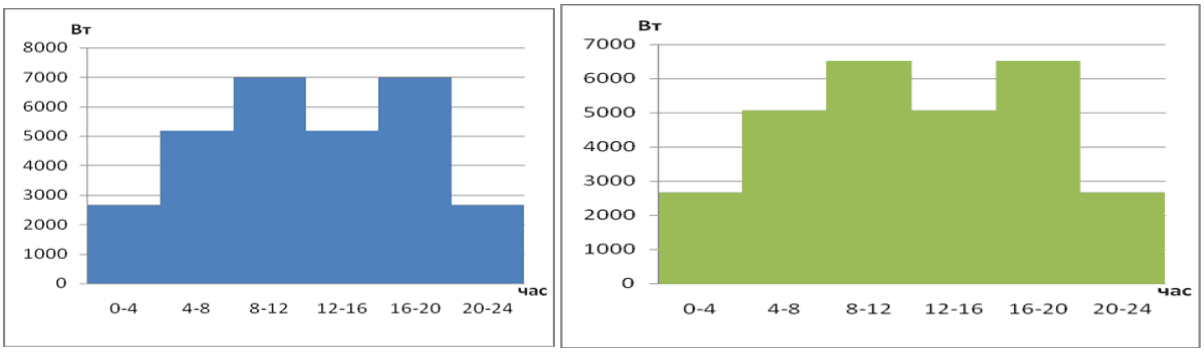
Преимуществами схемы СЭС заключаются в отсутствии проблем с синхронизацией напряжения частоты при переключении между ветряным и дизельным генераторами, а также в легком и простом масштабировании [1-3].

Состав нагрузки потребителей базовой станции приведен в Таблице 1.

Таблица 1 – Состав нагрузки

№	Наименование оборудования	Количество, шт.	Мощность, Вт	Суммарная мощность Вт	Время работы течение дня, ч	Суточное потребление электроэнергии, кВт·ч
1	Сигнализация	1	100	100	24	2,4
2	Кондиционер	1	2400	2400	16	38,4
3	Дренажный нагреватель	1	120	120	16	1,92
4	Бытовой потребитель	2	700	1400	8	11,2
5	Светильник	2	200	400	4	1,6
6	Радиотехническое оборудование	1	800	800	24	19,2
Общая установленная мощность 5,22 кВт					Общее ежедневное использование 74,72 кВт	

Суточные графики нагрузки базовой станции в зимний и летний периоды приведены в графическом виде на Рисунке 2.



а б

Рисунок 2 – Суточные графики нагрузки базовой станции:
а – зимний; б – летний.

Обобщенная структурная схема фотоэлектрической-ветровой-дизельной установки показана на Рисунке 3.

Основным источником энергии является фотоэлектрический модуль, который в течение дня заряжает аккумуляторную батарею (АБ) с помощью солнечного зарядного устройства (СЗУ). Второй источник электроэнергии - ветрогенератор, который преобразует энергию ветра в трехфазный переменный ток. Выпрямители с регулятором заряда заряжают батареи путем преобразования трехфазного тока в постоянный. Ограничитель сверхтока имеет защиту пакетного зарядного устройства от высоких токов. Инвертор подключается к аккумулятору и преобразует постоянное напряжение 48 В в стандартную синусоиду 220 В 50 Гц для подачи переменного тока на потребители базовой станции. Регуляторы заряда предотвращают перезарядку аккумулятора. Когда аккумулятор

заряжен, контроллер заряда переключает избыток электроэнергии на термоэлектрический нагреватель (ТЭН). Режим зарядки аккумуляторной батареи программно управляется контроллером инвертора. Когда АБ полностью заряжена, инвертор генерирует сигнал на отключение ДГ [4-8].

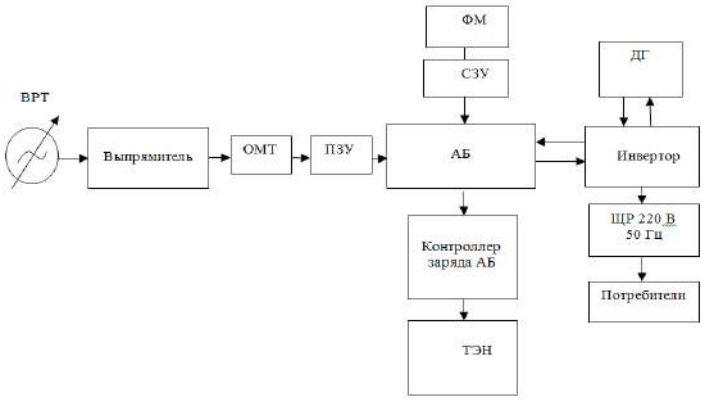


Рисунок 3 – Принципиальная схема фотоэлектрической - ветровой -дизельной установки:

ВРТ - ветровая роторная турбина; ДГ - дизельный генератор; ОМТ - ограничитель максимального тока; ЩР - щиток распределительный; ПЗУ - порционное зарядное устройство; АБ - аккумуляторные батареи; СЗУ - солнечное зарядное устройство; ТЭН - термоэлектрический нагреватель; ФМ – фотоэлектрический модуль.

Вывод.

Правила устройства электроустановок подтверждают, что базовые станции мобильной связи относятся к электропотребителям 1-й категории и что для обеспечения их работы в зонах децентрализованного энергоснабжения рекомендуется строить гибридные фото-ветро-дизельные установки. Общая мощность потребителей базовой станции составляет 5,22 кВт, а суточное потребление 74,72 кВт·ч. Самым мощным электроприемником является кондиционер мощностью 2400 кВт, а беспроводнок (телекоммуникационное) оборудование - 800 Вт [9-10].

Список литературы

1. Балтиков Д.Ф., Юсупов А.Н., Гиниатуллин И.И. Разработка автоматизаций системы учета электроэнергий для зерноочистительной машины // Вестник науки. 2022. Т. 5. № 5 (50). С. 283-287.
2. Балтиков Д.Ф., Ибатуллин К.А. разработка электротехнологической установки для производства биогумуса // Вестник науки. 2022. Т. 3. № 6 (51). С. 216-220.
3. Балтиков Д.Ф., Юсупов А.Н., Гиниатуллин И.И. Разработка автоматизаций системы учета электроэнергий для зерноочистительной машины // Вестник науки. 2022. Т. 5. № 5 (50). С. 283-287.
4. Балтиков, Д.Ф., Ибатуллина А.Ф., Балтиков И.И. Утилизация птичьего помёта в газогенераторной установке // Актуальные вопросы социально-экономических, технических и естественных наук: матер. национал. (Всерос.) науч. конф. Челябинск: Южно-Уральский государственный аграрный университет, 2021. С. 165 – 171.
5. Балтиков Д.Ф., Ибатуллина А.Ф., Ахметшин А.Т. Энергообеспечение птицеводческих хозяйств // Известия Оренбургского государственного аграрного университета. 2022. № 2 (94). С. 170 – 175.

6. Габитов И.И., Балтиков Д.Ф. Ибатуллина А.Ф. Энергообеспечение птицеводческих хозяйств с использованием газогенераторной установки // Технический сервис машин. 2022. № 1 (146). С. 87 – 94.
7. Валиев Р.Н., Балтиков Д.Ф. Технические характеристики системы теплопотребления // Инновации. Наука. Образование. 2022. № 55. С. 52-56.
8. Балтиков Д.Ф., Ахметшин А.Т., Ибатуллина А.Ф. Энергообеспечение птицеводческих хозяйств // Известия Оренбургского государственного аграрного университета. 2022. № 2 (94). С. 170-175.
9. Балтиков Д.Ф., Курбангалеев А.Р. Анализ микротурбинных установок для энергообеспечения предприятий. // Интернаука. 2022. № 12-3 (235). С. 52-54.
10. Ибатуллина А.Ф., Балтиков Д.Ф., Муратова Э.Ф. Разработка энергетического комплекса на базе газогенераторной установки для обеспечения птицеводческих хозяйств. // В сборнике: Современные тенденции агроинженерных наук и инновационные технологии в сельском хозяйстве. Материалы Международной научно-практической конференции Института агроинженерии. Челябинск, 2021. С. 202-212.

References

1. Baltikov D.F., Yusupov A.N., Giniatullin I.I. Development of automation systems for accounting for electricity for a grain cleaning machine. Vestnik nauki. 2022. V. 5. No. 5 (50). pp. 283-287.
2. Baltikov D.F., Ibatullin K.A. development of an electrotechnological installation for the production of biohumus // Vestnik nauki. 2022. Vol. 3. No. 6 (51). pp. 216-220.
3. Baltikov D.F., Yusupov A.N., Giniatullin I.I. Development of automation systems for accounting for electricity for a grain cleaning machine. Vestnik nauki. 2022. V. 5. No. 5 (50). pp. 283-287.
4. Baltikov D.F., Ibatullina A.F., Baltikov I.I. Utilization of bird droppings in a gas generating plant // Topical issues of socio-economic, technical and natural sciences: mater. national (All-Russian) scientific. conf. Chelyabinsk: South Ural State Agrarian University, 2021. pp. 165 – 171.
5. Baltikov D.F., Ibatullina A.F., Akhmetshin A.T. Energy supply for poultry farms // Proceedings of the Orenburg State Agrarian University. 2022. No. 2 (94). pp. 170 - 175.
6. Gabitov I.I., Baltikov D.F. Ibatullina A.F. Power supply of poultry farms using a gas generator unit // Technical service of machines. 2022. No. 1 (146). pp. 87 - 94.
7. Valiev R.N., Baltikov D.F. Technical characteristics of the heat consumption system // Innovations. The science. Education. 2022. No. 55. . pp. 52-56.
8. Baltikov D.F., Akhmetshin A.T., Ibatullina A.F. Energy supply for poultry farms // Proceedings of the Orenburg State Agrarian University. 2022. No. 2 (94). pp. 170-175.
9. Baltikov D.F., Kurbangaleev A.R. Analysis of microturbine installations for energy supply of enterprises. // Internauka. 2022. No. 12-3 (235). pp. 52-54.
10. Ibatullina A.F., Baltikov D.F., Muratova E.F. Development of an energy complex based on a gas-generating plant to provide poultry farms. // In the collection: Modern trends in agroengineering sciences and innovative technologies in agriculture. Materials of the International Scientific and Practical Conference of the Institute of Agroengineering. Chelyabinsk, 2021. pp. 202-212.

Дубовсков К.Ю., Шинкарев В.В., Полуэктов Е.К. Технологии накопления энергии// Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 4(30) с. 130–140

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 62

ТЕХНОЛОГИИ НАКОПЛЕНИЯ ЭНЕРГИИ

Дубовсков К.Ю., Шинкарев В.В., Полуэктов Е.К.
ФГБОУ ВО "Оренбургский Государственный Университет ", Оренбург, Россия (460018, г. Оренбург, проспект Победы, д.13, корп.3), e-mail: maildlyvsegoo56@mail.ru

Проблема с накоплением энергии и по сей день остаётся актуальной для современной энергетики. Как известно, электрическую энергию невозможно хранить в промышленных масштабах, поэтому актуальность проблемы заключается в тенденции инженеров-энергетиков усовершенствовать или разработать новые накопители энергии. В данной статье рассмотрены виды накопителей энергии, а также действующие технологии накопления энергии, которые применяются масштабно в энергетике на сегодняшний день.

Ключевые слова: Накопление энергии, аккумулирование, накопители энергии, супермаховики, термальные хранилища, аккумуляторные батареи, суперконденсаторы, проточные батареи.

ENERGY STORAGE TECHNOLOGIES

Dubovskov K.Yu., Shinkarev V.V., Poluektov E.K.
FSBEI of HE Orenburg State University, Orenburg, *Russia (460018, Orenburg, Pobedy Avenue, 13, building 3), e-mail: maildlyvsegoo56@mail.ru*

The problem with energy storage remains relevant for modern energy to this day. As you know, electric energy cannot be stored on an industrial scale, so the urgency of the problem lies in the tendency of power engineers to improve or develop new energy storage devices. This article discusses the types of energy storage devices, as well as current energy storage technologies that are used on a large scale in the energy sector today.

Keywords: Energy storage, storage, energy storage, supermachoviki, thermal storage, batteries, supercapacitors, flow batteries.

Традиционная структура энергосистем с самого начала их основания предопределялась одновременностью процессов генерации и потребления электроэнергии и необходимостью поддерживать в каждый момент времени баланс между произведённой и потребляемой мощностью в условиях нестабильного характера нагрузки. Главное отличие электроэнергетики от других отраслей промышленности заключается в том, что невозможно хранить произведённый ею товар в промышленных масштабах. В единицу времени в этой отрасли должно производиться ровно столько электроэнергии, сколько нужно заказчикам [4, с. 93-94].

В последние десятилетия в структуре энергосистем происходят значительные изменения в лучшую сторону. Во-первых, это связано со значительной и постоянно возрастающей долей производства электроэнергии с использованием возобновляемых источников энергии (ВИЭ) и развитием распределённой генерации. Если учитывать трудно

предсказуемый характер ВИЭ генерации, а также её зависимость от погодных условий, то для стопроцентного обеспечения баланса необходим объём резервной мощности, который пока реализуется в основном с помощью традиционной генерации. Данный способ поддержания баланса имеет свои ограничения, обусловленные техническими и экономическими факторами, и не может решить проблему интеграции ВИЭ в состав традиционной энергосистемы. Чтобы обеспечить компенсацию пиковых нагрузок, необходимы дорогие резервные генерирующие мощности, а также сложные географически распределенные энергосистемы [1, с. 10-11].

Классификация накопителей электроэнергии.

Накопитель энергии (НЭ) – это устройство, которое сохраняет и отдает энергию для использования, когда это необходимо. Накопители энергии различаются объемом запасаемой энергии, скоростью ее накопления и отдачи, удельной энергоемкостью, сроками ее хранения и другими параметрами, например, надежность и стоимость изготовления и обслуживания. НЭ все больше используются в электроэнергетических системах, транспорте, автономных энергетических установках и т. п. Все накопители можно разделить по виду энергии, с помощью которого происходит хранение (Рисунок 1).

Рисунок 1 – Классификация накопителей энергии по виду энергии

Системы хранения электроэнергии (ЭЭ) можно разделить на системы промышленного хранения энергии, которые характеризуются относительно большой емкостью, и на малые накопители, используемые для бытовых нужд потребителей. Наиболее применяемыми способами (99 % мировой мощности) промышленного хранения электрической энергии являются механические системы, а именно – гидроаккумулирующие. Однако в мире все более часто начинают применять «альтернативные» системы хранения энергии (например, доля последних в 2018 году составила 60 %). За последние несколько лет компании перешли от оценок возможности применения различных технологий хранения энергии к разработке оптимальных методов интеграции систем хранения в энергосистемы [5, с. 625-627].

Функции, возлагаемые на накопители энергии

Технологии накопления электроэнергии не смогли бы получить такого быстрого развития, если бы не имели серьёзного значения для всей энергетической системы. Основными функциями, возложенными на системы хранения, являются:

1. Быть основным источником энергии (а также аварийным источником энергии) и обеспечивать потребителей постоянным и бесперебойным питанием без подключения к электрическим сетям длительный период времени.
2. Регулировка параметров системы – снижать потери электроэнергии, выравнивать пиковые нагрузки в сети и повышать ее качество с помощью регулярного управления напряжением и частотой.
3. Оптимизация потребления (управляют графиком потребления за счет частичного обеспечения электроснабжения или аккумуляции электроэнергии). Использование НЭ позволит оптимизировать время нагрузки на наиболее дорогом генерирующем оборудовании.
4. Накопители необходимы для создания энергетического резерва без избыточной работы генерирующих мощностей. Они обеспечат спокойное прохождение ночного минимума и дневного пика нагрузок.
5. Исключение перебоев в питании – создается резерв на случай аварий, а также электроэнергия становится дешевле. [2, с. 77-78].

Основные технологии хранения энергии

На сегодняшний день многие технологии хранения энергии достигли своей коммерческой реализации или хотя бы рабочего прототипа. Среди таких технологий можно выделить насосное хранение, сжатый воздух, маховик, свинцово-кислотные батареи, литий-ионные батареи, натриевые серные батареи, проточные батареи, суперконденсаторы и сверхпроводящие магнитные накопители энергии и т. д. Кроме того, с активным развитием материаловедения проводятся исследования новых технологий хранения энергии, таких как технологии хранения энергии в электрохимических накопителях на основе графена. В действительности же сотни демонстрационных проектов по хранению энергии на уровне МВт были построены по всему миру в настоящее время.

Насосно-накопительные установки

Гидроаккумулирующие электростанции, они же насосно-накопительные установки, являются наиболее крупной формой накопления энергии в больших масштабах и в то же время, пожалуй, самой старой формой современного хранения энергии, привязанного к энергосети. Принцип работы прост: имеется два резервуара для воды, один выше другого. Когда потребность в электричестве низкая, энергию можно использовать для закачки воды наверх. В пиковые часы вода устремляется вниз, вращая гидрогенератор и вырабатывая электричество (Рисунок 2).

Реверсивные турбогенераторные узлы действуют как насос и турбина. Почти все подобные сооружения используют перепад высот между двумя водоемами. Подобные проекты разрабатывает, например, Германия в заброшенных угольных шахтах или сферических контейнерах на дне океана.

Рисунок 2 – Seneca Pumped Storage Generation Station, гидроэлектростанция в Пенсильвании в графстве Уоррен, использующая гидроаккумуляторы для выработки электроэнергии

Технология накопления энергии сжатого воздуха

Принцип работы пневматических аккумулирующих установок заключается в использовании избыточной энергии для сжатия воздуха для последующего производства электроэнергии. Сжатый воздух хранится в подземном резервуаре. В целом этот способ напоминает предыдущий, за исключением того, что вместо воды в резервуары нагнетается воздух. При необходимости воздух выпускается и вращает турбины. Эта технология существует в теории уже несколько десятков лет, но на практике, из-за ее высокой стоимости, есть всего лишь несколько рабочих систем и чуть больше — испытательных (Рисунок 3).

Рисунок 3 – Неадиабатическая установка сжатого воздуха мощностью 110 МВт в Макинтоше, Алабама

Пневматический аккумулятор может преодолеть разрыв между волатильностью производства и нагрузкой. Он удовлетворяет потребности потребителей в энергии, эффективно обеспечивая доступную энергию для покрытия спроса.

Сжатие воздуха создает тепло: при сжатии температура внутри накопительных резервуаров повышается. Расширение, со своей стороны требует тепловой энергии. Если не добавлять дополнительной энергии, воздух после расширения будет намного холоднее. Поэтому недостаток такого рода накопителей - низкий КПД из-за того, что часть энергии при сжатии газа переходит в тепловую форму. Эффективность не более 55%, для рационального использования накопитель требует много дешевой электроэнергии, поэтому на данный момент технология используется преимущественно в экспериментальных целях, общая установленная мощность в мире не превышает 400 МВт.

Технология накопления энергии маховиком

Супермаховик представляет собой технологию накопления кинетической энергии. Электричество запускает мотор, который запасает энергию вращения в барабане. Когда она нужна, маховик замедляется. Образец промышленного применения технологии супермаховика можно наблюдать на Рисунок 4.

Рисунок 4 – Энергонакопительная станция, основанная на технологии маховика

Накопитель энергии маховика работает за счет ускорения ротора (маховика) до очень высокой скорости, аккумулируя энергию вращения. Когда энергия извлекается, скорость вращения маховика уменьшается; добавление энергии соответственно приводит к увеличению скорости маховика.

Одно из преимуществ маховика – способность без ущерба самому себе отдавать огромную энергию за маленький промежуток времени. Получается, он и аккумулятор, и конденсатор в одном лице. Большинство подобных систем используют электричество для ускорения и замедления маховика, но рассматриваются и устройства, которые непосредственно используют механическую энергию.

Системы супермаховиков имеют относительно долгий срок службы (срок службы полного цикла, указанный для маховиков, варьируется от 10^5 до 10^7 циклов использования), высокая удельная энергия (100—130 Вт · ч/кг или 360—500 кДж/кг) и удельная мощность.

Но все достоинства (КПД до 90%, неограниченный цикл заряда-разряда и долговечность) не могут компенсировать его саморазряд. Изобретение не получило широкого распространения, хотя оно и может применяться для обеспечения бесперебойного питания.

Технологии накопления тепловой энергии. Термальные хранилища

Аккумулирование тепловой энергии заключается во временном хранении и отводе тепла или холода. Аккумулирование тепла использует преимущества нагрева материала для накопления энергии. Технологии сезонного накопления тепловой энергии позволяют использовать тепло или холод спустя месяцы после того, как оно было получено из природных источников или отходов. Так, например, ночью хранящуюся в цистернах воду замораживают, а днем лед тает и охлаждает соседние дома, позволяя экономить на кондиционерах (Рисунок 5). Лед производится только во время непиковой нагрузки на электросети, а затем, вместо расхода дополнительной электроэнергии, используется накопленный холод для

охлаждения помещений. Эта технология привлекательна для регионов с жарким климатом и прохладными ночами, например, для Австралии или Калифорнии.

Рисунок 5 – Накопитель холода Калифорнийской компании «Ice Energy»

Технологии накопления тепловой энергии часто имеют срок окупаемости в диапазоне от четырёх до шести лет. Например, в Браструпе (Дания) система коммунального солнечного теплоснабжения, также использует технологию накопления тепловой энергии при температуре хранения 65° С. Тепловой насос, который работает только при наличии избыточной энергии ветра в единой энергосети, используется для повышения температуры до 80° С для распределения. Когда избыточного электричества, генерируемого ветром, нет, используется газовый котел. 20 % процентов тепла Браструпа имеют солнечное происхождение

Расплавленная соль в качестве накопителя энергии

Солнечную энергию можно использоваться для нагревания соли до нужной температуры. Полученный пар либо немедленно перерабатывается генератором в электричество, либо хранится в течение нескольких часов в виде расплавленной соли, чтобы, например, нагревать дома вечером. На Рисунке 6 можно увидеть фотографию такой аккумулирующей станции.

Рисунок 6 – Башня с расплавленной солью и зеркала, направляющие солнечные лучи к вершине башни

Расплавленная соль удерживает тепло в течение длительного времени, поэтому ее размещают на солнечных тепловых установках, где сотни гелиостатов (1) (больших сконценирированных на солнце зеркал) собирают тепло солнечного света и нагревают жидкость внутри - в виде расплавленной соли. Затем она направляется в резервуар (2), далее посредством парогенератора (5) приводит во вращение турбину (6), так вырабатывается электроэнергия (Рисунок 7).

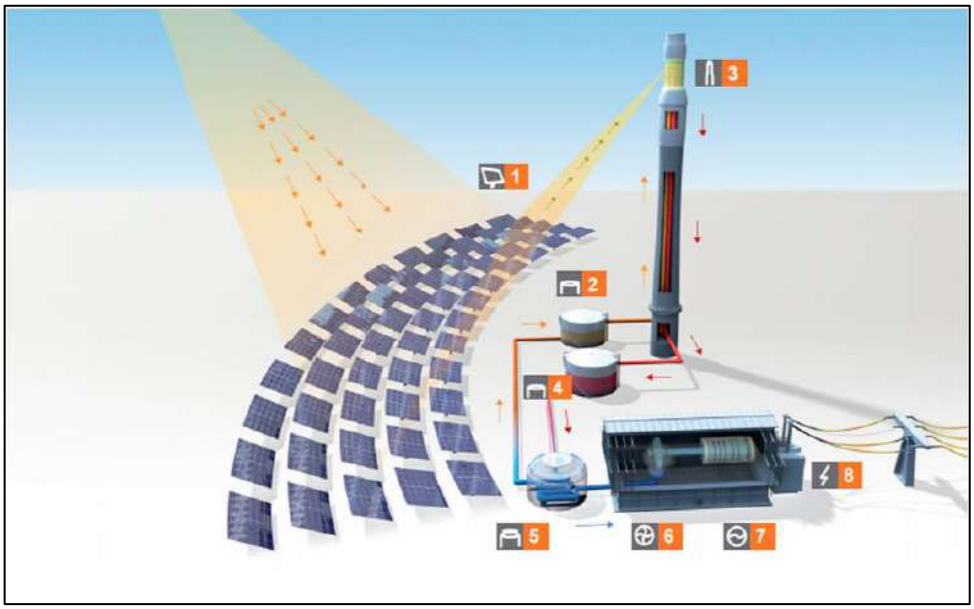


Рисунок 7 – Схема электростанции, работающей на расплавленной соли

Одним из плюсов является то, что расплавленная соль функционирует при высокой температуре - более 500 градусов по Цельсию и достигая 2000 градусов, что способствует эффективной работе паровой турбины.

Подобные технологии используются в солнечном парке имени Мохаммеда ибн Рашида Аль Мактума — самая крупной в мире сети солнечных электростанций, объединенных в едином пространстве в Дубаи [2, с. 77-78].

Проточные батареи

Одной из интересных технологий являются проточная батарея или проточная редокс-система (Рисунок 8).

Рисунок 8 – Комплект проточных батарей

Окислительно-восстановительные проточные батареи состоят из огромных цистерн с электролитом, которые пропускаются через мембраны, где происходит обмен ионов для зарядки (разрядки) элемента и создаётся электрический заряд. Обычно в качестве электролита используется ванадий, а также растворы цинка, хлора или соленая вода. Напряжение подобных установок обычно составляет от 1 до 2,2 В, а ёмкость накопителя зависит от объёма ёмкостей, в которых находится раствор.

Пока нет коммерческих проектов, которые стали бы использовать данную технологию. Общая установленная мощность — 320 МВт, в основном в рамках исследовательских проектов. Главный плюс — пока единственная технология на батареях с длительной выдачей энергии — более 4 часов. Также они надежны, просты в эксплуатации, у них долгий срок службы. Среди недостатков — громоздкость и отсутствие технологии утилизации, что является общей проблемой для всех батарей [7, с. 77-78].

Традиционная аккумуляторная батарея

Аккумуляторная батарея – это электрохимический источник энергии Он содержит один или несколько электрохимических элементов. Аккумуляторы бывают разных форм и размеров, от кнопок до мегаваттных энергосистем. Подобные энергоносители в наши дни окружают нас со всех сторон. Любое носимое устройство, смартфон, ноутбук, везде так или иначе будет компактный аккумулятор. На данный момент одним из самых распространенных типов аккумулятора является литий-ионный. Свое название эти элементы питания получили

из-за использования в качестве катодных материалов литиевых производных (литий-феррофосфатов, кобальтата лития, литий-марганцевой шпинели и т.д.), а в качестве переносчиков заряда - ионов лития.

Но помимо литий-ионных аккумуляторов существуют и другие аккумуляторные батареи различные по своему химическому составу:

1. Свинцово-кислотные аккумуляторы, занимающие самую большую долю рынка аккумуляторов. В заряженном состоянии отрицательный электрод из металлического свинца и положительный электрод из сульфата свинца погружают в электролит с разбавленной серной кислотой (H_2SO_4). В процессе разряда электроны выталкиваются из ячейки, так как на отрицательном электроде образуется сульфат свинца, а электролит восстанавливается до воды.
2. Никель-металлогидридная батарея (NiMH): первые коммерческие образцы появились в 1989 году. Сейчас это обычный потребительский и промышленный товар. Батарея имеет для отрицательного электрода вместо кадмия водородопоглощающий сплав.
3. Литий-ионный полимерный аккумулятор: эти аккумуляторы имеют малый вес и могут быть изготовлены в любой форме.
4. Графеновые аккумуляторы – это одна из новейших разработок. Графен является третьей формой углерода (первые две – это алмаз и графит). Данный материал экологически чист, что может решить проблему утилизации аккумуляторов. Принцип действия аккумулятора схож с литий-полимерным. Графеновые аккумуляторы превосходят все существующие электрохимические элементы как в энергоемкости, так и в массе.

Современные технологии позволили добиться высокой энергоемкости аккумуляторных элементов и повысить безопасность при их эксплуатации [3, с. 46-47].

Заключение

Мировой рынок систем накопления электроэнергии интенсивно развивается: совершенствуются технологии, накапливается опыт практического применения. Системы позволяют принципиально по-новому решать многие проблемы управления нормальными и аварийными режимами энергосистем. Наиболее интенсивно развиваются электрохимические накопители с литий-ионными аккумуляторными батареями, которые за последнее десятилетие подешевели вдвое, что заметно сказалось на их инвестиционной привлекательности.

Такая обширная область, как технологии накопления электроэнергии, только за последние 10 лет начала активно развиваться. Немаловажный фактор, который необходимо решить в будущем – это экологичность. С развитием альтернативных систем накопления энергии, таких как термальные хранилища, накопление сжатым воздухом или ГАЭС, а также модернизацией традиционных электрохимических источников энергии появится возможность снизить пагубное влияние систем накопления электроэнергии на экологию.

Список литературы

1. Васильков О. С. Повышение энергоэффективности электротехнических комплексов горнообогатительных предприятий с использованием систем накопления электроэнергии [Электронный ресурс]. // Диссертация. — 2021. — Режим доступа: https://spmi.ru/sites/default/files/zashita/vasilkov_dissertaciya.pdf (дата обращения 29.03.2023).

2. Зырянов В. М. Системы накопления энергии: Российский и зарубежный опыт [Электронный ресурс]. // Энергетическая политика. — 2020. — №6 (148). — Режим доступа: https://cyberleninka.ru/article/n/sistemy-nakopleniya-energii-rossiyskiy-i-zarubezhnyy-opyt (дата обращения 29.03.2023).
3. Коровин Н.В. Электрохимическая энергетика. – М.: Электроатомиздат, 1991, с. 46-47.
4. Кубарьков Ю. П. Проблемы и достижения технологии накопления энергии и ее применения в энергетических системах [Электронный ресурс]. // Инновационные процессы в науке и образовании. — 2019. — Том 1. — Режим доступа: https://www.elibrary.ru/item.asp?id=36692180 (дата обращения 29.03.2023).
5. Пермякова Д. К. Развитие технологий накопления и хранения энергии – основа для распространения ВИЭ [Электронный ресурс]. // Пермский национальный исследовательский политехнический университет. — 2019. — Режим доступа: https://elar.urfu.ru/bitstream/10995/88153/1/eir_2019_151.pdf (дата обращения 29.03.2023).
6. Физический энциклопедический словарь ред. Прохоров, А.М. Издательство: М.: Советская Энциклопедия. 1984 г.
7. Яковлева Э. В. Развитие технологий накопления электрической энергии [Электронный ресурс]. // Молодой ученый. — 2017. — №50 (184). — Режим доступа: https://moluch.ru/archive/184/47286/ (дата обращения 29.03.2023).

References

1. Vasilkov O. S. Improving the energy efficiency of electrical complexes of mining and processing enterprises using energy storage systems [Electronic resource]. // Dissertation. — 2021. — Access mode: https://spmi.ru/sites/default/files/zashita/vasilkov_dissertaciya.pdf (accessed 29.03.2023).
2. Zyryanov V. M. Energy storage systems: Russian and foreign experience [Electronic resource]. // Energy Policy. — 2020. — №6 (148). — Access mode: https://cyberleninka.ru/article/n/sistemy-nakopleniya-energii-rossiyskiy-i-zarubezhnyy-opyt (accessed 29.03.2023).
3. Korovin N.V. Electrochemical power engineering. – M.: Electroatomizdat, 1991, pp. 46-47.
4. Kubarkov Yu. P. Problems and achievements of energy storage technology and its application in energy systems [Electronic resource]. // Innovative processes in science and education. — 2019. — Volume 1. — Access mode: https://www.elibrary.ru/item.asp?id=36692180 (accessed 29.03.2023).
5. Permyakova D. K. The development of energy storage and storage technologies is the basis for the spread of RES [Electronic resource]. // Perm National Research Polytechnic University. — 2019. — Access mode: https://elar.urfu.ru/bitstream/10995/88153/1/eir_2019_151.pdf (accessed 29.03.2023).
6. Physical Encyclopedic Dictionary ed. Prokhorov, A.M. Publisher: Moscow: Soviet Encyclopedia. 1984
7. Yakovleva E. V. Development of electric energy storage technologies [Electronic resource]. // Young scientist. — 2017. — №50 (184). — Access mode: https://moluch.ru/archive/184/47286 / (accessed 29.03.2023).

Кошкин Ф.В. и др. Технологии беспроводной передачи энергии и их внедрение в повседневную жизнь человека // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 141–150

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 62

ТЕХНОЛОГИИ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ЭНЕРГИИ И ИХ ВНЕДРЕНИЕ В ПОВСЕДНЕВНУЮ ЖИЗНЬ ЧЕЛОВЕКА

Кошкин Ф.В., Дубовсков К.Ю., Шинкарев В.В., Полуэктов Е.К.
ФГБОУ ВО "Оренбургский Государственный Университет ", Оренбург, Россия (460018, г. Оренбург, проспект Победы, д.13, корп.3), e-mail: maildlyvsegoo56@mail.ru

В данной статье описаны технологии передачи электроэнергии за счёт явлений электромагнитной индукции и электростатической индукции, а также лазерным, ультразвуковым и микроволновым методами. Приведены исторические факты об открытии законов, связанных с беспроводной передачей электроэнергии, описаны методы беспроводной передачи, приведены примеры использования этих технологий в современной жизни людей.

Ключевые слова: Явление электромагнитной индукции, беспроводная передача электроэнергии, метод электростатической индукции, ультразвуковой метод, лазерный метод.

WIRELESS ENERGY TRANSMISSION TECHNOLOGIES AND THEIR IMPLEMENTATION IN THE DAILY LIFE OF A PERSON

Koshkin F.V., Dubovskov K.Yu., Shinkarev V.V., Poluektov E.K.
FSBEI of HE Orenburg State University, Orenburg, Russia (460018, Orenburg, Pobedy Avenue, 13, building 3), e-mail: maildlyvsegoo56@mail.ru

This article describes the technology of electric power transmission due to the phenomena of electromagnetic induction and electrostatic induction, as well as laser, ultrasonic and microwave methods. Historical facts about the discovery of laws related to wireless transmission of electricity are given, methods of wireless transmission are described, examples of the use of these technologies in modern people's lives are given.

Keywords: Electromagnetic induction phenomenon, wireless electric power transmission, electrostatic induction method, ultrasonic method, laser method.

Современный мир сложно представить без электрической энергии. Для людей использование приборов, которые питаются от электричества, является обычным делом в повседневной жизни. Электроэнергия стала основой прогресса. Её используют во всех сферах человеческой жизни, так как эту энергию можно преобразовывать в другие виды энергии простым образом, а её передача может происходить на большие расстояния. Наши дома оснащены разными проводами, устройствами. Чтобы включить какой-либо прибор, нам нужно всего лишь вставить вилку в розетку. Однако, человек всегда ищет способы облегчить себе жизнь. Попытки решить эту проблему привели ученых к разработкам в сфере беспроводной передачи электроэнергии.

Конечно, каждое решение порождает новые проблемы, но человек пытается решить и их. Но если в квартире не будет розеток, то не нужно будет заряжать телефон, использовать

чайник и вешать телевизор в определенном месте, а также можно будет избавиться от большого количества проводов, которые часто нам мешаются. [2, с. 58-60]

История беспроводной передачи электроэнергии

Первый, кто дошел до передачи электроэнергии без проводов был Никола Тесла. Он вложил большой вклад в создание устройств на переменном токе, многофазных систем, синхронного генератора и асинхронного двигателя. С 1889 года Никола Тесла исследовал токи высокой частоты и высоких напряжений. Эти исследования создали предпосылки для создания новой отрасли электротехники, где используется техника высокой частоты. Благодаря своим работам Никола Тесла смог впервые показать беспроводную передачу электроэнергии. Он смог заставить светиться газоразрядную лампу в своих руках, находясь в электрическом поле высокочастотной катушки (Рисунок 1).

Рисунок 1 – Тесла с горящей газоразрядной лампой

Никола Тесла продемонстрировал такое беспроводное освещение на всемирной выставке, проходившей в 1893 году в Чикаго. Также он зажег без проводов фосфорную лампу накаливания в 1894 году, которая была основана на резонансной частоте.

В его голове были идеи не только питания приборов без проводов, но и передача электроэнергии на расстояния. С помощью резонансных приемников он хотел создать всемирную беспроводную систему. Началом проекта была башня Ворденклиф, однако этот проект был закрыт, а сама башня была подвергнута демонтажу.

Таким образом, Никола Тесла был изобретателем, работы которого мы видим в повседневной жизни. Переход от постоянного тока к переменному и к беспроводной передаче электричества – это заслуги Никола Тесла, которые до сих пор имеют важное значение. [5, с. 1-3].

Методы беспроводной передачи электроэнергии

Есть несколько методов передачи электроэнергии:

- Метод электромагнитной индукции, в основе которого лежит использование катушек.
- Метод электростатической индукции. Основа – прохождение электроэнергии через диэлектрик.
- Лазерный метод – за счет использования лазера и фотоэлемента.
- Ультразвуковой метод, в основе лежит использование ультразвука и приемника.
- Микроволновый метод, в основе которого лежит передача микроволнового излучения от источника к приемнику. [4, с. 1-4].

Метод электромагнитной индукции

В основе этого метода лежит использование ближнего электромагнитного поля. Прибор состоит из двух катушек, одна из которых подключена к переменному источнику питания. Из-за протекания в катушке переменного тока создается переменное магнитное поле, которое действует на вторую обмотку, индуцируя в ней электрический ток (Рисунок 2).

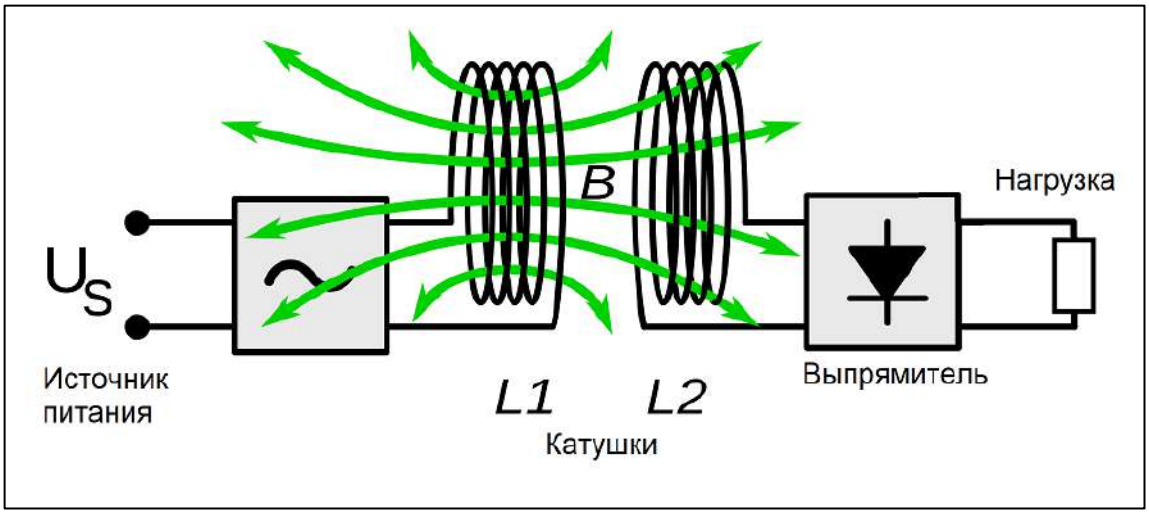


Рисунок 2 – Схема передачи электроэнергии методом электромагнитной индукции

Самым простым примером является электрический трансформатор. Обмотки электрически не связаны между собой, а передача энергии переходит с помощью взаимной индукции. Для повышения взаимодействия катушек между собой в трансформаторе используют металлические сердечники. Но использование металла для передачи электроэнергии на расстоянии будет неудобно в повседневной жизни, поэтому увеличение взаимодействия катушек достигают другим способом.

Большая эффективность в данном способе достигается путем тесного взаимодействия, но и на близких расстояниях такой метод становится неэффективным. Основные потери этого метода связаны с расстоянием между катушками. Как раз это и является минусом данного метода. Если увеличивать расстояние между катушками, то потеря энергии будет увеличиваться, так как действие переменного магнитного поля на вторичную катушку будет уменьшаться. Энергия ближнего поля сама по себе не является излучающей, однако какая-то

часть радиационных потерь происходит. Кроме этого, происходят и резистивные потери. Из-за таких проблем использование данного способа может усложниться.

Однако, возможность увеличения расстояния между катушек может достигаться путем использования резонанса колебательного контура. При резонансной индукции приемник и передатчик настроены на одну частоту. Как пример можно рассмотреть трансформатор с последовательным резонансом. В теории при последовательном резонансе колебательный контур в цепи закорачивается, из-за этого через этот контур будет проходить максимальный ток. На практике, если используется последовательный резонанс в трансформаторе, то нужно установить сопротивление, которое ограничит ток. В результате такая конструкция дает возможность создать в первичном контуре ток выше, чем при нерезонансном режиме. Следовательно, по законам Кирхгофа напряжение на вторичной катушке будет выше, так как магнитное действие первичной катушки увеличится из-за увеличения тока в ней.

Другим способом является использование резонансного колебательного контура отдельно от источника (Рисунок 3). Но действие от такого расположения катушек не меняется, так как и в этом случае будет максимальный ток в контуре, который будет создавать переменное магнитное поле, а это поле – переменный ток во вторичной катушке. [6, с. 1-3]

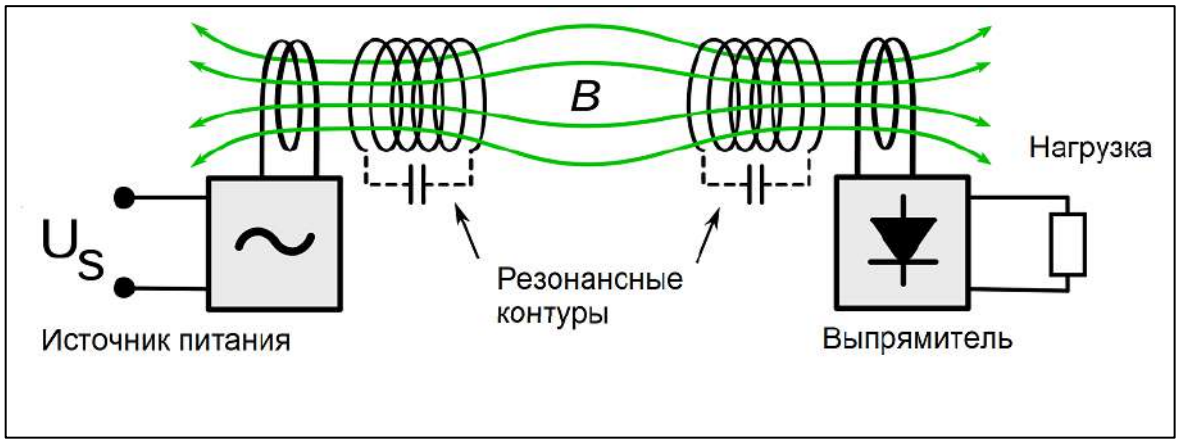


Рисунок 3 – Схема передачи электроэнергии методом резонансной электромагнитной индукции [3, с. 1-3]

Метод электростатической индукции

Данный метод основан на прохождении энергии через диэлектрик. Такой процесс называют электростатической или ёмкостной связью. На практике – это градиент электрического поля между двумя или более клеммами, пластинами, электродами или узлами. Электрическое поле создается за счет заряда пластин переменным током высокой частоты и высокого потенциала, а ёмкость между двумя электродами и питаемым устройством создает разницу потенциалов.

Самым простым примером могут являться конденсаторы (Рисунок 4). В такой схеме также использую переменный источник напряжения, в результате создается переменное электрическое поле, причем на двух конденсаторах оно имеет разное направление. Точнее, одно направлено к приемнику, а другое от приемника. [3, с. 3-4]

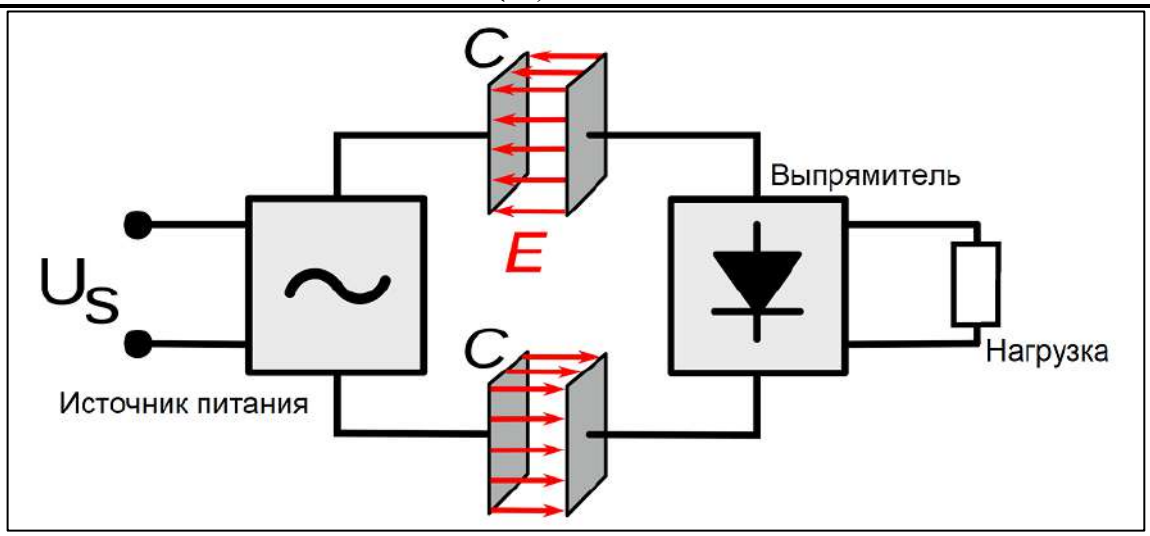


Рисунок 4 – Схема передачи электроэнергии методом электростатической индукции

Лазерный метод

Лазер является в современном мире удобный устройством. Он преобразует энергию накачки в энергию узконаправленного потока электромагнитного излучения. Лазеры могут является очень мощным устройством. С помощью этого устройства можно получать не только пучок света, но и тепло, с помощью которого можно обрабатывать разные материалы. Из-за такой мощности ему нашли применение и в электротехнике.

Если длина волны электромагнитного излучения приближается к видимой области спектра, то энергию можно передать путём её преобразования в луч лазера, который затем может быть направлен на фотоэлемент, тем самым преобразовывая энергию луча в электроэнергию. [4, с. 2-4]

Лазерная передача энергии по сравнению с другими методами беспроводной передачи обладает разными преимуществами. Во-первых, передача энергии может производится на большие расстояния, так как угол расходимости у лазера очень мал, что позволяет пучку точно дойти до приёмника. К тому же это позволит применять лазер для небольших устройств, не используя никаких дополнительных оптических приборов. Во-вторых, лазерное излучение не создает помех для существующих средств связи, таких, как Wi-Fi и сотовые телефоны.

Однако, такая беспроводная передача электроэнергии обладает и недостатками. Лазерный пучок всё же является видимым излучением, поэтому для использования такой передачи нужен фотоэлемент. А эффективность такой установки будет очень мала, так как КПД фотоэлемента достигает 40-50%. К тому же при использовании данного метода на большие расстояния есть потери в атмосфере и нужна прямая видимость между передатчиком и приемником. [3, с. 5-6]

Ультразвуковой метод

Ультразвуковой метод является лишь примером беспроводной передачи электричества, так как такой метод максимально неэффективный. Суть метода была изобретена студентами университета Пенсильвании и впервые представлена в 2011 году. В данном методе также использовался передатчик и приёмник. Передатчик излучал ультразвук, а приемник, в свою очередь, преобразовывал слышимое в электричество. На момент показа этого метода

расстояние передачи достигало от 7 до 10 метров, и была необходима прямая видимость приёмника и передатчика. Передаваемое напряжение достигало 8 вольт. Использование ультразвука никак не действует на человека. [3, с. 1-3]

Практическое применение этого метода невозможно из-за очень низкого КПД, ограничений во многих государствах на максимальный уровень звукового давления и другие причины [4, с. 1]

Микроволновый метод

Радиоволновую передачу энергии можно сделать более направленной. Это достигается за счет уменьшения длины волны электромагнитного излучения до микроволнового диапазона. Для обратного преобразования микроволновой энергии в электричество может быть использована ректенна, эффективность преобразования которой превышает 95%. Данный способ рассматривался как вариант передачи энергии из космоса с орбитальных солнечных электростанций на Землю и питания космических кораблей, покидающих земную орбиту.

Однако, есть проблема в этом методе. Чтобы использовать такую технику в космических программах, необходима диафрагма большого размера. Например, для получения с такой электростанции микроволнового луча частотой 2,45 ГГЦ понадобится передающая антенна диаметром в 1 километр, а принимающая ректенна диаметром в 10 километров. Размеры можно уменьшить путем уменьшения длины передаваемой волны, но из-за этого уменьшения будет большее поглощение атмосферой. Поэтому для очень больших расстояний такой метод не эффективен, однако, этот метод всё же может преодолеть большие расстояния, в отличие от методов электромагнитной и электростатической индукции.

Простой вид схемы данного метода состоит из передатчика и приёмника (Рисунок 5). Передатчиком является передающая антенна, а приёмником – приёмная рентенна. Их размеры будут зависеть от расстояния между ними и от нужной мощности. [7, с. 1-3]

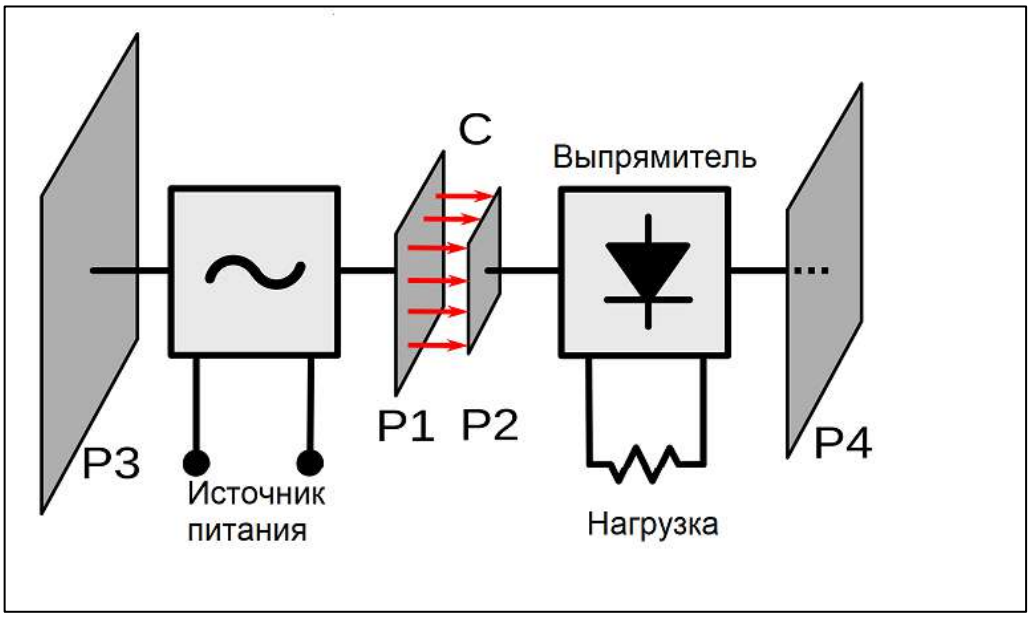


Рисунок 5 – Схема передачи электроэнергии методом микроволнового излучения [3, с. 3-5]

Применение беспроводной передачи электроэнергии

Всем методам беспроводной передачи электроэнергии можно найти применение. В современном мире подобные технологи могут быть особенно полезны. Рассмотрим для применение некоторых методов беспроводной передачи электроэнергии.

Рассмотрим метод электромагнитной индукции. В повседневной жизни применение этого метода можно встретить чаще, чем другие. Этот метод удобен для приборов, которые можно зарядить на близком расстоянии, а таких устройств в настоящее время очень много.

Первым устройством, которое приходит на ум, является телефон. Обычная зарядка от телефона имеет провод, но люди решили сделать более удобное приспособление для зарядки телефона. Этим приспособлением является та же зарядка, но беспроводная (Рисунок 6). Основана она на электромагнитной индукции. [1, с. 4-5]

Рисунок 6 – Беспроводная зарядка

Помимо телефона есть и другие устройства, которые имеют аккумулятор, например, электротранспорт, а в частности общественный. Ранее уже были изобретены машины, которые работают от электричества, но они питаются от контактных проводов. А в новом типе общественного транспорта – электробусы, стоят аккумуляторы, следовательно, они и питают электродвигатель. Чтобы каждый раз не подключать машины на электродвигателях, придумали специальные места с беспроводной зарядкой (Рисунок 7). Эти места могут быть расположены как на остановках, так и на стоянках. [2, с. 354]

Рисунок 7 – Зарядная площадка электробуса [3, с. 1-2]

Применение лазерного метода

Лазерный метод является довольно неэффективным способом передачи электроэнергии на расстояния, но из-за свойств луча этот метод можно использовать в некоторых устройствах.

Лазерную подзарядку для беспилотного самолета-модели продемонстрировали в Драйденском летно-исследовательском центре НАСА. Теперь стало возможным подзарядить летающие аппараты прям в воздухе. Этот метод обходит обычные солнечные батареи, так как эффективность лазерного луча выше, чем солнечного, а также есть возможность использования этого метода в ночное время.

Следующее применение продемонстрировала компания PowerBeam. С 2006 года она разрабатывает готовые для коммерческого применения узлы для различных потребительских и промышленных электронных устройств. Эти узлы как раз основаны на лазерном луче. [7, с. 4-5]

Применение микроволнового метода

Микроволновое излучение показало себя, как хороший способ передачи электроэнергии на большие расстояния. Микроволна является направленной волной, что делает микроволновый метод удобным для распространения.

Инженеры стартапа Emord уже разрабатывают систему на микроволнах. Из-за направленности микроволн передатчик не должен находиться вблизи потребителя, следовательно, электроэнергию можно передать со станции сразу к потребителю без проводов. Приёмник может быть совсем небольших размеров (Рисунок 8). [4, с. 4-5]

Рисунок 8 – Приёмник микроволновых волн Emord [7, с. 3-4]

Заключение

Таким образом, использование в настоящее время беспроводной передачи электроэнергии возможна. Методы беспроводной передачи удобны как для дальнего расстояния, так и для ближнего, но в любом найдутся свои минусы.

У идеи беспроводной передачи электричества есть свои проблемы. Во-первых, многие методы добавляют свои минусы, так как физика их работы довольно разная. Будет сложно использовать разные методы в одном доме, а если использовать только один метод, то это не избавит нас от всех проводов. Во-вторых, самый главный минус – экономическая составляющая беспроводной передачи. Во многих методах такая передача уменьшает КПД, и если подсчитать затраты, которые получит потребитель за удобство, то будет выгоднее и удобнее использовать старые методы. К тому же многие идеи требуют средства на развитие, производство новых деталей и проектирование новых систем

Список литературы

1. Бессонов, Л. А. Теоретические основы электротехники / Л. А. Бессонов. – 4-е изд. – М.: Высш. шк., – 1964. – 752 с.
2. Елдышев, Ю. Н. Электричество без проводов – мечта сбывается? / Ю. Н. Елдышев // Экология и жизнь, 2010 – N 4. – С. 58-60.
3. Беспроводная передача электричества [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/Беспроводная_передача_электричества (дата обращения 06.04.2023).
4. Беспроводная передача электроэнергии [Электронный ресурс] – Режим доступа: https://amperof.ru/teoriya/besprovodnaya-peredacha-elektroenergii.html (дата обращения 06.04.2023).
5. Тесла, Никола [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/Тесла,_Никола#Изобретения_и_научные_работы (дата обращения 06.04.2023).

6. Резонансная индуктивная связь [Электронный ресурс] – Режим доступа: https://en.wikipedia.org/wiki/Resonant_inductive_coupling (дата обращения 06.04.2023).
7. Беспроводное электричество: от идеи до реализации [Электронный ресурс] – Режим доступа: https://mentamore.com/covremennye-texnologii/besprovodnoe-elektrichestvo.html#:~:text=Беспроводная%20передача%20электричества%3A%20что%20это.,электрической%20цепи%20из%20токопроводящих%20элементов (дата обращения 06.04.2023).

References

1. Bessonov, L. A. Theoretical foundations of electrical engineering / L. A. Bessonov. - 4th ed. – M.: Higher School, - 1964. – p. 752
2. Eldyshev, Yu. N. Electricity without wires – is a dream coming true? / Yu. N. Eldyshev // Ecology and life, 2010 – N 4. – pp. 58-60.
3. Wireless transmission of electricity [Electronic resource] – Access mode: https://ru.wikipedia.org/wiki/Беспроводная_передача_электричества (accessed 06.04.2023).
4. Wireless transmission of electricity [Electronic resource] – Access mode: https://amperof.ru/teoriya/besprovodnaya-peredacha-elektroenergii.html (accessed 06.04.2023).
5. Tesla, Nikola [Electronic resource] – Access mode: https://ru.wikipedia.org/wiki/Tesla,_Nikola#Invention_and_scientific_work (accessed 06.04.2023).
6. Resonant inductive coupling [Electronic resource] – Access mode: https://en.wikipedia.org/wiki/Resonant_inductive_coupling (accessed 06.04.2023).
7. Wireless electricity: from idea to implementation [Electronic resource] – Access mode: https://mentamore.com/covremennye-texnologii/besprovodnoe-elektrichestvo.html#:~:text=Беспроводная%20передача%20электричества%3A%20что%20это.,электрической%20цепи%20из%20токопроводящих% 20 elements (accessed 06.04.2023).