Международный журнал информационных технологий и энергоэффективности

Том 7 Номер 3 (25)

2022

Международный журнал информационных технологий и энергоэффективности
Т.7 №3(25) часть 3 2022 г.

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

СОДЕРЖАНИЕ / CONTENT

Применение генетического алгоритма для повышения надежности электроснабжения потребителей / Груздов А.Г.. [и др.] // Международный журнал информационных технологий и энергоэффективности. – 2022. –
Т. 7 № 3(25) часть 3 с. 4–10

Международный журнал информационных технологий и энергоэффективности

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

УДК 62.1

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ ЭЛЕКТРОСНАБЖЕНИЯ ПОТРЕБИТЕЛЕЙ

[1] Груздов А. Г., [2] Пашковская Е. Е., [3] Сивеев Т. М., [4] Цветков А. С.
Национальный исследовательский университет «МЭИ», Москва, Россия (111250, г. Москва, ул. Красноказарменная, 17, стр. 3), e-mail: [1] GruzdovAG@mpei.ru, [2] PashkovskyaYY@mpei.ru, [3] tichonsiveev@gmail.com, [4] sashatsvetkov131202@mail.ru

В данной статье рассматривается проблема снижения показателей надежности электроснабжения потребителей Российской распределительной сети. Очевидным путем повышения надежности электроснабжения потребителей является предотвращение аварийных ситуаций. Это достигается установкой надёжного оборудования и заменой износившихся участков линий электропередачи. К наиболее рациональным способом повышения надежности является, так называемая, децентрализованная автоматизация. Такой подход подразумевает минимизацию последствий аварий с использованием секционирующих устройств нового поколения – реклоузеров. Применение реклоузеров позволяет повысить надежность, качество электроснабжения и снизить ущерб от недоотпуска электрической энергии.

Ключевые слова: Smart Grid, методы оптимизации, генетический алгоритм, реклоузер, надежность, фидер

APPLICATION OF A GENETIC ALGORITHM TO INCREASE RELIABILITY OF ELECTRICITY SUPPLY TO CONSUMERS

[1] Gruzdov A. G., [2] Pashkovskaya E. E., [3] Siveev T. M., [4] Tsvetkov A. S.
National Research University "MPEI", Moscow, Russia (111250, Moscow, Krasnokazarmennaya st., 17, building 3), e-mail: [1] GruzdovAG@mpei.ru, [2] PashkovskyaYY@mpei.ru, [3] tichonsiveev@gmail.com, [4] sashatsvetkov131202@mail.ru

This article discusses the problem of reducing the reliability of power supply to consumers of the Russian distribution network. The obvious way to increase the reliability of power supply to consumers is to prevent emergencies. This is achieved by installing reliable equipment and replacing worn-out sections of power lines. The most rational way to increase reliability is the so-called decentralized automation. This approach implies minimizing the consequences of accidents using a new generation of partitioning devices – reclosers. The use of reclosers makes it possible to increase the reliability, quality of power supply and reduce damage from under-discharge of electric energy.

Keywords: Smart Grid, optimization methods, genetic algorithm, rumber, reliability, feeder.

Актуальность исследования обусловлена направлением развития электроэнергетического комплекса. В последнее время все большее распространение получают проекты, связанные с реализацией концепции Smart Grid, а внедрение такого оборудования, как реклоузер полностью отвечает основным положениям указанной

концепции. Внедрение реклоузеров в распределительных сетях является не только перспективным, но и технологически оправданным мероприятием. Технико-экономическое обоснование применения секционирующих устройств была описана в статье [1].

В зависимости от варианта использования реклоузеров и возможных условий их размещения возникает задача определения оптимальных мест их подключения в распределительной сети. Расстановка в электрической сети реклоузеров является одним из средств увеличения надежности электроснабжения потребителей. При этом, при определении места их установки, предусматриваются определенные условия, конфигурация сети и частота аварийных событий на данном участке ВЛ и время их восстановлений.

Решение такой многовариантной оптимизационной задачи зависит от выбранного критерия оптимизации. В качестве критерия могут быть использованы различные параметры, влияющие на надежность и экономичность работы распределительной сети среднего напряжения. В частности, в [2] в качестве интегрального показателя оценки выбран суммарный годовой недоотпуск электроэнергии. В [3] проблема оптимального секционирования рассмотрена с позиции минимизации потерь в электрической сети и уменьшения токов короткого замыкания.

Для выбора места установки оборудования используется показатель надежности SAIDI. Показатель используется для анализа надежности электрических сетей и используется в соответствующей системе стимулирования повышения надежности и качества, позволяющий достичь повышение тарифа на передачу электрической энергии. Мировой практике рекомендует также использовать SAIFI. Так как показатель SAIDI пропорционально коррелируется с SAIFI, то для выбора места установки реклоузеров достаточно использовать показатель SAIFI.

Прямой перебор мест установки реклоузеров в больших схемах занимает длительное время. При увеличении уровня разветвленности сети число участков сети пригодных для установки реклоузеров также будет расти, что может привести к неразрешимости задачи при использовании классических методов оптимизации без подключения больших вычислительных мощностей и огромного количества времени. Например, в статье [4] указывается, что расчёт в сети, граф которой имеет 42 вершины, для 9 аппаратов занимает больше часа, для 10 – почти 4 часа, для 12 – более 29 часов.

Именно поэтому было решено использовать эвристические алгоритмы, которые не способны гарантировать стопроцентную точность, однако имеют быструю сходимость, что подтверждено авторами в статьях [5].

Как уже было упомянуто выше, генетические алгоритмы являются подтипом быстросходящихся, но не гарантирующих стопроцентной точности эвристических алгоритмов. Генетические алгоритмы используются для решения различных оптимизационных задач, путем случайного подбора, вариации и комбинирования входных параметров с использованием сходных с естественным отбором механизмов. Генетический алгоритм является разновидностью другой группы алгоритмов, именуемых «эволюционными вычислениями» или «эволюционными алгоритмами»

Основным фактором эволюции является естественный отбор, принцип которого «выживает сильнейший». Иными словами, основная идея эволюции заключается в том, что особи с более высоким уровнем приспособленности с большей вероятностью выживут и

оставят потомство. Подразумевается, что потомство, оставленное особями с высоким уровнем приспособленности, также будут более приспособленными.

Эволюционное моделирование используется для решения ряда оптимизационных задач и подразумевает математическое моделирование, процессов эволюции. Другими словами, в основе эволюционных алгоритмов лежат принципы биологической эволюции:

- каждая особь представляет собой набор хромосом (некоторые параметры, например, вектор, строка символов или какой-либо фрагмент данных) и определенной фитнес – функции, которая отображает уровень приспособленности той или иной особи, т.е. ее преимущество перед другими особями в решении поставленной задачи;
- улучшение (максимизация или минимизация в зависимости от цели поставленной задачи) фитнес – функции с применением специальных генетических операторов (отбор, мутация, скрещивание);
- уровень приспособленности особи (значение ее фитнес – функции) определяет вероятность того, насколько будет высока приспособленность потомства, оставленного этой особью [6].

Теоретически процесс эволюции является бесконечным. Через некоторое время он может быть приостановлен наблюдателем, при достижении определённых критериев остановки. Ниже перечислены основные алгоритмы, относящиеся к эволюционным:

- генетический алгоритм, наиболее применимой областью применения которого является оптимизация дискретных функций (с особым упором на оператор скрещивания);
- эволюционная стратегия, наиболее применимой областью применения которого является оптимизация непрерывных функций (с использованием операторов скрещивания);
- эволюционное программирование, наиболее применимой областью применения которого является оптимизация непрерывных функций (без использования операторов скрещивания);
- генетическое программирование, наиболее применимой областью применения которого является оптимизация компьютерных программ (используется только оператор скрещивания) [7].

По сравнению с обычными методами оптимизации, эволюционные алгоритмы имеют следующие отличительные черты:

- наличие параллельного поиска решений;
- наличие понятия случайной мутации и скрещивания полученных решений.

Эволюционные алгоритмы хорошо подходят для оптимизации многомерных, плохо определенных функций.

Генетический алгоритм является одним из самых известных подвидов эволюционных алгоритмов. Он объединяет все основные операции, характерные для генетики (отбор, мутация, кроссинговер). Генетические алгоритмы являются результатом математического описания таких свойств природы, как:

- способность живых организмов приспосабливаться к меняющимся условиям окружающей среды;

- процессы наследования детьми лучших свойств от своих родителей, для повышение своей приспособленности к окружающим условиям;
- наличие естественного отбора, обеспечивающего выживание наиболее приспособленных организмов.

Генетические алгоритмы позволяют решать такие задачи, как оптимизация работы нефтяных трубопроводов, улучшение работы поисковых систем, распределение инструментов в металлообрабатывающих цехах, оптимизацию профилей балок в строительстве и т.д. [6]. Одной из наиболее подходящих для генетических алгоритмов сфер задач являются задачи комбинаторной оптимизации, то есть задач с поиском оптимального решения среди конечного множества ращений (зачастую в подобных задачах, невозможен полный перебор вариантов за оптимальное время).

Ниже перечислены основные генетические операторы, применяемы в процессе оптимизации отбор лучших хромосом от наиболее приспособленных родителей для дальнейшего скрещивания; скрещивание полученных в процессе отбора хромосом с целью получения нового более приспособленного поколения; мутация – случайное изменение некоторых генов с целью недопущения зацикливающихся повторений наборов хромосом в последующих поколениях.

Стоит отметить, что эвристические алгоритмы не могут гарантированно найти наилучшее решение, однако имеют более высокую скорость сходимости к нему, что для некоторых задач гарантирует базисную техническую возможность получения результата.

Авторы работы [8] предлагает методику оптимального определение мест расстановки реклоузеров. Особью представляется комплект ветвей, в которые устанавливаются аппараты. Ген – номер ветви, в которой находится аппарат. Число вероятных номеров генов равно количеству свободных для установки реклоузеров ветвей. Выбранной фитнес-функцией представляется показатель надёжности распределительной сети SAIFI.

Рассмотрим более подробно этапы работы генетического алгоритма. На Рисунке 1 приведена блок – схема работы генетического алгоритма в контексте решаемой задачи.

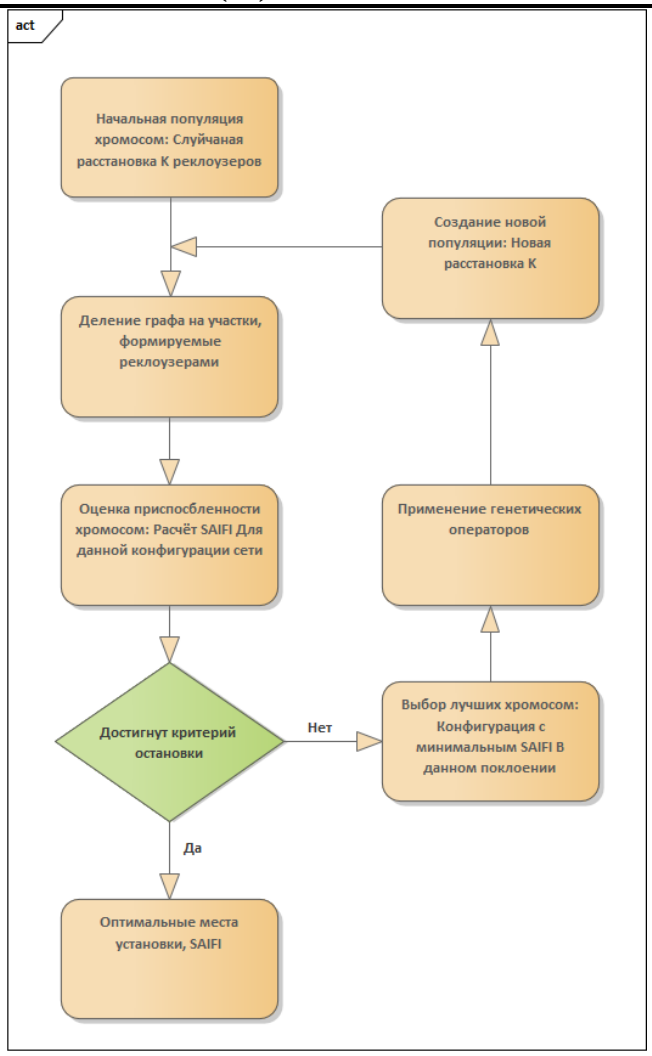


Рисунок 1 – Блок – схема работы генетического алгоритма в контексте решаемой задачи.

На первом этапе алгоритм формирует начальную популяцию хромосом, т.е. создает n хромосом со случайным набором генов (количество которых равно k), где n – размер популяции. Переходя от терминов генетики к терминам электроэнергетики вышесказанное можно переформулировать следующим образом: на первом этапе алгоритм формирует n различных конфигураций схем, в каждой из которой установлено k реклоузеров.

На втором этапе для каждой хромосомы происходит деление графа на участки, формируемые реклоузерами. Каждый реклоузер имеет свою зону действия (участок). Подразумевается, что при возникновении устойчивой аварии в зоне действия реклоузера, будут отключены только потребители, расположенные в узлах, относящихся к данному участку. Этот этап представляет собой моделирование концепции секционирования сети с целью повышения надежности электроснабжения потребителей.

На третьем этапе происходит оценка приспособленности хромосом. Алгоритм, основываясь на рассчитанных для каждой хромосомы значениях фитнесс – функции определяет наиболее приспособленные хромосомы. Иными словами, на данном этапе алгоритм отбирает схемы с наименьшим показателем SAIFI.

На четвертом этапе при условии достижения одного из критериев остановки алгоритм завершает свою работу, предоставляя результаты в виде оптимальных мест для установки реклоузеров и соответствующий показатель SAIFI и программа заканчивается. В противном случае происходит переход следующий этап.

Далее алгоритм отбирает лучшие хромосомы, т.е. хромосомы с наименьшим показателем фитнес – функции, в текущей популяции для их дальнейшего участия в формировании новой популяции.

Следующий этап реализация генетических операторов для создания новой популяции: выбор лучшей хромосомы, мутация, скрещивание.

В конце итерации появляется уже сформированная популяция новых хромосом и алгоритм снова переходит на первый этап.

Для реализации данного алгоритма предлагается разработать алгоритм расчёта, используя высокоуровневый язык программирования Python. В процессе решения будет производится минимизация значения показателя надежности SAIFI для электрической сети с использованием генетического алгоритма.

Предложенный подход может быть использован как на стадии проектирования новых распределительных электрических сетей, так и при модернизации уже существующих.

Список литературы

1. Реклоузер как инструмент повышения надежности / Т. М. Сивеев, А. С. Сорокин, А. Г. Груздов, Д. А. Дегтярев // Столыпинский вестник. – 2022. – Т. 4. – № 5.– С. 12
2. Сазыкин В.Г. Критерии оптимизации места установки реклоузера в распределительной сети 6-10 кВ // Электротехнические системы и комплексы / Кудряков А.Г., Багметов А.А. – Магнитогорск: Изд-во Магнитогорского государственного технического университета им. Г.И. Носова, 2018. – Вып. 1(38). – С. 33-39. 45.
3. Энерго- и ресурсосбережение. Энергообеспечение. Нетрадиционные и возобновляемые источники энергии. Атомная энергетика : материалы Международной научно-практической конференции студентов, аспирантов и молодых ученых, посвященной памяти профессора Данилова Н. И. Екатеринбург, 10–14 декабря 2018 г. / Отв. Ред.: Гаврилова А. Е., Ерошенко С. А. – Екатеринбург : УрФУ, 2018. - С. 151-154. 46.
4. Андрикеева С.А. Оптимизация использования автоматических пунктов секционирования для повышения надёжности распределительной сети и энергоснабжения потребителей //Электрические станции, №8, 2016. – С. 30–34.
5. Sourabh K. A review on genetic algorithm: past, present and future // Multimedia Tools and Applications / Sumit S. Ch., Vijay K. – Heidelberg, Netherlands: Springer Netherlands, 2021. – Vol. 80. – pp. 8091-8126.
6. Климко Е.Г. Генетический алгоритм как разновидность эволюционного алгоритма // журнал «Российские Исследования» №2, 2002, С. 125 – 128 27.
7. Генетическое программирование URL: https://ru.wikipedia.org/wiki/Гентическое_программирование.

References

1. Siveev T. M., Sorokin A. S., Gruzdov A. G., Degtyarev D. A. Recloser as a tool for improving reliability // Stolypinskiy vestnik. - 2022. - T. 4. - No. 5. - p. 12
2. Sazykin V.G. Criteria for optimizing the installation site of a recloser in a 6-10 kV distribution network // Electrical systems and complexes / Kudryakov A.G., Bagmetov A.A. - Magnitogorsk: Publishing House of the Magnitogorsk State Technical University. G.I. Nosova, 2018. - Issue. 1(38). -pp. 33-39. 45.
3. Energy and resource saving. Energy supply. Non-traditional and renewable energy sources. Nuclear power: materials of the International scientific-practical conference of students, graduate students and young scientists, dedicated to the memory of Professor Danilov N. I. Ekaterinburg, December 10–14, 2018 / Ed. Ed.: Gavrilova A. E., Eroshenko S. A. - Yekaterinburg: UrFU, 2018. - pp. 151-154. 46.
4. Andrikeeva S.A. Optimization of the use of automatic sectioning points to improve the reliability of the distribution network and power supply to consumers // Electric Stations, No. 8, 2016. - pp. 30–34.
5. Sourabh K. A review on genetic algorithm: past, present and future // Multimedia Tools and Applications / Sumit S. Ch., Vijay K. - Heidelberg, Netherlands: Springer Netherlands, 2021. - Vol. 80.-pp. 8091-8126.
6. Klimko E.G. Genetic algorithm as a kind of evolutionary algorithm // Journal "Russian Research" №2, 2002, pp. 125 – 128 27.
7. Genetic programming URL: https://ru.wikipedia.org/wiki/Genetic_programming.
8. Akimov D.A. Optimization of the placement of reclosers in distribution networks. Izvestia of the Scientific and Technical Center of the Unified Energy System / Grunina O.I., Karpov A.I., Shkitina N.O. - M.: Publishing House of the Scientific and Technical Center of the Federal Grid Company of the Unified Energy System, 2017. - Issue. 1(76) - pp. 102-113.

Исследование видов дифференциальных защит линий электропередач / Сивеев Т.М. [и др.] // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 11–15

Международный журнал информационных технологий и энергоэффективности

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

УДК 62.1

ИССЛЕДОВАНИЕ ВИДОВ ДИФФЕРЕНЦИАЛЬНЫХ ЗАЩИТ ЛИНИЙ ЭЛЕКТРОПЕРЕДАЧ

[1] Сивеев Т. М., [2] Цветков А. С., [3] Груздов А. Г., [4] Пашковская Е. Е.
Национальный исследовательский университет «МЭИ», Москва, Россия (111250, г. Москва, ул. Красноказарменная, 17, стр. 3), e-mail: [1]tichonsiveev@gmail.com, [2] sashatsvetkov131202@mail.ru, [3] GruzdovAG@mpei.ru, [4] PashkovskyaYY@mpei.ru

Энергетическая система представляет собой совокупность электроустановок, предназначенных для производства, передачи, распределения и потребления электроэнергии. В настоящее время неотъемлемой частью объектов энергосистемы являются устройства релейной защиты и автоматики. Релейная защита – это совокупность автоматических устройств, которые позволяют выявлять повреждения в системе энергообъектов и отключать поврежденные участки, не позволяя наносить ущерб энергосистеме. В связи с этим, к релейной защите предъявляются следующие требования: селективность, чувствительность, надежность и быстродействие. Под селективностью в данном случае понимается способность релейной защиты определять поврежденный объект и отключать именно его от исправно работающей части системы. Чувствительность характеризует способность РЗ включаться в работу при малейших отклонения от нормальных режимах. Быстродействие обосновано рядом существенных негативных последствий, возникающих в системе при коротких замыканиях. В данной статье анализируются наиболее эффективные виды релейной защиты линий электропередач, а также возможность применения метода цепей Маркова, для исследования функционирования канала связи релейной защиты.

Ключевые слова: высокочастотные (ВЧ) защиты линий, канал связи релейной защиты, дифференциально-фазные защиты (ДФЗ), направленные защиты с высокочастотной блокировкой (НВЧЗ), короткое замыкание (КЗ).

INVESTIGATION OF TYPES OF DIFFERENTIAL PROTECTION OF POWER LINES

[1] Siveev T. M., [2] Tsvetkov A. S., [3] Gruzdov A. G., [4] Pashkovskaya E. E.
National Research University "MPEI", Moscow, Russia (111250, Moscow, Krasnokazarmennaya st., 17, building 3), e-mail: [1]tichonsiveev@gmail.com, [2] sashatsvetkov131202@mail.ru, [3] GruzdovAG@mpei.ru, [4] PashkovskyaYY@mpei.ru

An energy system is a set of electrical installations designed for the production, transmission, distribution and consumption of electrical energy. Currently, relay protection and automation devices are an integral part of the power system facilities. Relay protection is a set of automatic devices that allow detecting damage in the system of power facilities and disconnecting damaged areas, preventing damage to the power system. In this regard, the following requirements are imposed on relay protection: selectivity, sensitivity, reliability and performance. Selectivity in this case refers to the ability of relay protection to detect a damaged object and disconnect it from a properly functioning part of the system. Sensitivity characterizes the ability of the RS to be included in the operation at the slightest deviation from normal modes. The performance is justified by a number of significant negative consequences that occur in the system during short circuits. This article analyzes the most effective types of relay protection of power lines, as well as the possibility of using the Markov circuit method to study the functioning of the relay protection communication channel.

Keywords: high-frequency line protection, relay protection communication channel, differential-phase protection, directional protection with high-frequency blocking, short circuit.

Широко известные ступенчатые (токовые и дистанционные) защиты линий электропередач используются для защиты линий с односторонним питанием и не могут использоваться для защиты линий с двухсторонним питанием, поскольку в данном случае не обеспечивают селективность отключения, решить проблему позволяет применение дифференциальных защит.

Главное отличие дифференциальных защит линий от ступенчатых заключается в том, что они имеют связь между комплектами защитных устройств, установленных по концам линии и поэтому обладают абсолютной селективностью. Для этого в защитах применяется канал связи, с помощью которого осуществляется постоянный обмен данными между комплектами РЗ, установленных по концам защищаемой линии.

Исследование процесса работы канала связи целесообразно проводить с помощью метода математического моделирования, математическая модель позволяет спрогнозировать поведение реальной системы объектов и получить аналитические выражения для определения ее параметров. Применительно к системе релейной защиты и автоматики особенно важно создание математической модели ее функционирования, что позволит провести исследование работы РЗ в разных режимах (особенно в случае аварийных режимов), а так же получить аналитические выражения, определяющие показатели надежности ее работы и вероятности отказа различных элементов системы. Одним из таких методов является метод цепей Маркова, при котором вероятность последующего состояния в любой момент времени определяется состоянием в настоящий момент, независимо от прошлого. Для описания возможности применения данного метода необходимо подробно разобраться в особенностях функционирования канала связи релейной защиты ЛЭП.

Обращаясь к СТО «Каналы связи РЗА» [1, с.15], можно выделить следующие виды защит линий электропередач 35-330 кВ, использующие канал связи: дифференциально-фазные защиты, направленные высокочастотные защиты, продольные дифференциальные токовые защиты линий. Необходимо провести сравнение данных видов защит и выявить преимущества и недостатки каждого из них.

Дифференциально-фазные защиты (ДФЗ) – используется в качестве основной защиты от всех видов повреждений линий 110-330 кВ с двусторонним питанием необходимо в случаях, когда для сохранения устойчивости системы необходимо отключение повреждений на всем протяжении защищаемой линии без замедления, а также когда применение других видов защит невозможно и нецелесообразно. [2,с.7]. Данная защита имеет следующие преимущества: правильно работает в неполнофазных режимах; при качаниях; асинхронном ходе; имеет однотипные органы приемопередатчика, действующие на пуск и на отключение, что значительно облегчает их согласование по чувствительности. Принцип действия основан на сравнении фаз токов по концам линии. Это сравнение осуществляется с помощью высокочастотных сигналов, которые, генерируются приемопередатчиком на одном конце защищаемой линии и принимаются на другом. Для управления высокочастотным сигналом применяется ток манипуляции. ДФЗ состоит из следующих органов: орган манипуляции, орган сравнения фаз, пусковой орган.

Орган манипуляции (ОМ) формирует ток манипуляции – синусоидальный сигнал. Если напряжение данного сигнала будет ниже порога чувствительности манипуляции, орган

манипуляции будет выдавать сплошной сигнал. При превышении напряжения чувствительности манипуляции на определенное нормированное значение, к примеру, в случае короткого замыкания на защищаемой линии, срабатывает защита. При внешних коротких замыканиях в канале присутствует непрерывный ВЧ сигнал.

Орган сравнения фаз (ОСФ) – определяет разность фаз токов, сравнивая длительности пауз между сигналами, приходящими с приемопередатчиков. При длительности паузы больше значения, заданного уставкой, линия отключается.

К пусковым органам (ПО) относятся токовые органы, способные реагировать на обратной и нулевой последовательности, тем самым обеспечивая чувствительность защиты ко всем видам коротких замыканий. Пусковые органы делятся на блокирующие и отключающие.Блокирующие ПО осуществляют пуск приемопередатчика, а отключающие разрешают работу органа сравнения фаз [3,с.5-6].

Направленные защиты с высокочастотной блокировкой – применяются в случаях, когда для сохранения работоспособности системы, необходимо незамедлительное действие защиты. Принцип действия данной защиты заключается в сравнении направления мощностей по концам защищаемой линии. При внутреннем коротком замыкании потоки мощности концов линии направлены навстречу друг другу, что является сигналом, для срабатывания защиты. В данном случае органом, регистрирующим направление мощности, является реле мощности. В момент КЗ на защищаемой линии, реле мощности срабатывает и блокирует работу приемопередатчиков, которые обмениваются сигналами тока высокой частоты, сигнал прекращается и защита срабатывает. Таким образом, НВЧЗ имеет в своем составе *высокочастотную часть*, по которой замыкаются токи высокой частоты и *релейную часть,* регистрирующую направление мощности в линии.

Пусковой орган выполняется при помощи двух комплектов реле, один из которых пускает в работу высокочастотный передатчик, а второй отключает защиту. Для срабатывания защиты при междуфазных коротких замыканиях применяется реле тока, включенные на фазный ток, при недостаточной их чувствительности применяют реле сопротивления.

Данная система, по сравнению с дифференциально-фазной, имеет ряд существенных недостатков: может излишне срабатывать в неполнофазных режимах, для предотвращения излишних срабатываний в схемах (НВЧЗ) используют дополнительные цепи, снижающие надежность системы; может излишне срабатывать при качаниях и асинхронном ходе, в связи с чем так же усложняется ее устройство; затруднения в согласовании пусковых органов, действующих на пуск и на отключение; несколько большее время срабатывания, связанное с наличием промежуточных реле.[4,с.4].

Продольная дифференциальная токовая защита – предназначена служить основной защитой линий электропередач небольшой протяженности (до 15 км) в сетях с большими и малыми токами замыкания на землю. [5]. Принцип работы, как и в случае с дифференциально-фазной защитой, основан на сравнении фаз токов по концам линии, однако возможно также и сравнение значений токов, протекающих по вспомогательным элементам защиты. К таким элементам относятся соединенные между собой проводами обмотки трансформаторов тока, расположенных по концам защищаемой линии. Ток в соединительном проводе равен сумме токов обмоток. Соответственно, при равенстве коэффициентов трансформации трансформаторов тока, сумма этих токов равна нулю, поскольку они имеют встречное направление. Реле тока в данном случае блокирует защиту от срабатывания. При

возникновении короткого замыкания в линии токи через реле совпадут по фазе и равенство суммарного тока нулю перестанет выполняться, реле даст сигнал на отключении линии.

Однако, применение соединительных проводов, выполненных на всю протяженность линии, вносят определенные ограничения в работу защиты. Во первых, они обладают внутренним сопротивлением, превышающим, допустимую нагрузку для трансформаторов тока, что вносит необходимость дополнительного включения промежуточных трансформаторов тока. Во вторых, для подключения протяженных линий, одного реле оказалось недостаточным, и возникла необходимость установки отдельного реле на каждом конце линии. В третьих, подключение двух реле повлекло за собой неравномерное распределение токов (токи распределялись обратно пропорционально сопротивлениям цепей). Как итог: возникла необходимость снижения чувствительности защиты.

Таким образом, проведя анализ дифференциальных видов защит линий электропередач, можно утверждать, что наиболее эффективной является дифференциально-фазная защита, поскольку она обладает выраженным превосходством в реализации предъявляемых к ней требований, по сравнению с другими видами. Однако, стоит отметить, что в определенных случаях, применение направленной защиты с высокочастотной блокировкой или продольно-дифференциальной токовой защиты может быть более целесообразным.

Соотнося проведенное исследование, с действительным практическим применением видов дифференциальных защит, стоит отметить наиболее широкое распространение дифференциально-фазных защит линий электропередач в современной системе релейной защиты и автоматики. Данная защита обеспечивает абсолютную селективность отключения, повышенную чувствительность ко всем видам коротких замыканий, высокую скорость срабатывания, наряду с этим она так же способна работать в несимметричных режимах и при этом исключать излишние срабатывания.

Исследование функционирования канала связи РЗ целесообразно проводить с помощью метода цепей Маркова. Применение данного метода дает возможность определить несовершенство конкретного вида релейной защиты при работе в различных режимах, а именно: вероятности излишних или ложных срабатываний, отказа в срабатывании системы защиты. В конечном итоге данный метод позволит составить аналитические выражения для определения показателей надежности конкретного вида защиты линий электропередач.

Список литературы

1. Каналы связи для РЗА. Технические решения для сетей 35-220 кВ: СТО 34.01-9.2-004-2019 – Введ.28.06.2019 – ПАО Россети, 2019 – 15 с.
2. Руководящие указания по релейной защите. Выпуск 9. Дифференциально-фазная защита линий 110-330 кВ. Москва, «Энергия», 1972 г.
3. Дифференциально-фазная защита линий 110-220 кВ: СТО ДИВГ-053-2019 – Взамен СТО ДИВГ-053-2012 Линии электропередач 110-220 кВ. Дифференциально-фазная защита. – Введ.21.08.2019 – ООО НТЦ Механотроника, 2019 – С. 5-6.
4. Руководящие указания по релейной защите. Выпуск 10. Высокочастотная блокировка дистанционной и токовой направленности нулевой последовательности защит линий 110-220 кВ, Москва, «Энергия», 1972 г.
5. Руководящие указания по наладке, проверке и эксплуатации продольной дифференциальной защиты типа ДЗЛ-1. Я.М. Смородинский, В.М. Волков, 1962 г.

References

1. Communication channels for relay protection and automation devices. Technical solutions for networks 35-220 kV: STO 34.01-9.2-004-2019 - Introduced. 06/28/2019 - PJSC Rosseti, 2019 - p.15.
2. Guidelines for relay protection. Issue 9. Differential-phase protection of 110-330 kV lines. Moscow, Energia, 1972
3. Differential-phase protection of 110-220 kV lines: STO DIVG-053-2019 - Instead of STO DIVG-053-2012 Power lines 110-220 kV. Differential-phase protection. - Introduced.21.08.2019 - STC Mechatronics LLC, 2019 – pp. 5-6
4. Guidelines for relay protection. Issue 10
5. Guidelines for the adjustment, testing and operation of longitudinal differential protection type DZL-1. Ya.M. Smorodinsky, V.M. Volkov, 1962.

Исследование регенеративных теплообменников с различными типами насадок / Шацких Ю.В. [и др.] // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 16–21

Международный журнал информационных технологий и энергоэффективности

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

УДК 66.045.13

ИССЛЕДОВАНИЕ РЕГЕНЕРАТИВНЫХ ТЕПЛООБМЕННИКОВ С РАЗЛИЧНЫМИ ТИПАМИ НАСАДОК

[1] Шацких Ю.В., [2] Шарапов А.И., [3] Арзамасцев А.Г., [4] Юнусова М.А.
[1,4]Национальный исследовательский университет «МЭИ», Москва, Россия (111250, Москва, Красноказарменная, 14), e-mail: [1] shatskih_jv@mail.ru [4] YunusovaMA@mpei.ru
[2,3] Липецкий государственный технический университет, Липецк, Россия (398600, Липецк, Московская, 30), e-mail: [2]sharapov-lipetsk@yandex.ru, [3]arzamastcev-ag@mail.ru

В работе представлены результаты расчетного исследования режимов работы регенеративного теплообменного аппарата. Расчеты проводились на основе математической модели регенеративного теплообмена. Ранее показывалось, что оптимальным для регенеративного теплообменника является режим, обеспечивающий линейное распределение температуры теплоносителя и насадки по высоте аппарата. Показано, что в рамках регулярного режима снижение продолжительности периодов нагрева/охлаждения насадки сопровождается увеличением коэффициента использования тепла. Также показано, что границу реализации регулярного режима можно оценить с помощью критериев подобия, сочетающих в себе конструктивные и режимные характеристики регенеративного теплообменника. Проведенные расчеты показали, что имеет смысл повышать коэффициент теплоотдачи насадки только при установленном диапазоне изменения расходов теплоносителей и времени периодов нагрева и охлаждения и режимных параметров работы теплообменников.

Ключевые слова: регенеративные теплообменники, теплообменный аппарат.

STUDY OF REGENERATIVE HEAT EXCHANGERS WITH DIFFERENT TYPES OF PACKINGS

[1] Shatskikh Yu. V., [2] Sharapov A. I., [3] Arzamastsev A.G., [4] Yunusova M.A.
[1,4]National Research University MPEI, Moscow, Russia (111250, Moscow, Krasnokazarmennaya 14), e-mail: [1] shatskih_jv@mail.ru [4] YunusovaMA@mpei.ru
[2,3]Lipetsk State Technical University, Lipetsk, Russia (398600, Lipetsk, Moskovskaya, 30), e-mail: [2]sharapov-lipetsk@yandex.ru, [3]arzamastcev-ag@mail.ru

The paper presents the results of a computational study of the operating modes of a regenerative heat exchanger. The calculations were carried out on the basis of a mathematical model of regenerative heat transfer. Previously, it was shown that the optimal mode for a regenerative heat exchanger is the mode that provides a linear distribution of the temperature of the coolant and packing along the height of the apparatus. It is shown that, within the framework of the regular regime, a decrease in the duration of the heating/cooling periods of the packing is accom-panied by an increase in the heat utilization coefficient. It is also shown that the boundary of the implementation of the regular mode can be estimated using similarity criteria that combine the design and operating characteristics of a regenerative heat exchanger. The calculations performed showed that it makes sense to increase the heat transfer coefficient of the packing only for the established range of changes in the flow rates of heat carriers and the time of heating and cooling periods and the operating parameters of the heat exchangers.

Keywords: regenerative heat exchangers, heat exchanger.

Выбор оптимального режима работы регенеративного теплообменника

Регенеративные теплообменные аппараты широко применяются в технологии и промышленности. Этот тип теплообменников отличается большим разнообразием [1-3]. Но для любого регенеративного теплообменника общим является взаимосвязь конструктивных характеристик и режимных параметров [4].

Теплообмен в регенеративном аппарате в период охлаждения насадки можно описать системой дифференциальных уравнений [5], численное решение которых позволяют получить распределение температуры насадки и теплоносителей по высоте теплообменника. Проведенные расчеты показывают, что при соответствующем подборе соотношения приведенных расходов и времени периодов охлаждения и нагрева можно получить линейное распределение температуры насадки по высоте при квазистационарном режиме. В этом случае мы имеем регулярный режим нагрева (охлаждения) насадки, так как линейное распределение температуры насадки сохраняется в течении всего времени периода [6]. Анализ существующих исследований показывает, что в действующих регенеративных воздухоподогревателях котельных установок и доменных воздухонагревателях распределение температуры насадки и теплоносителей по высоте действительно близко к линейному.

Для регулярного режима можно перейти от дифференциальной формы записи уравнений к интегральной, а затем привести к критериальному виду [4] с использованием критериев подобия.

Критерий $\mathrm{Kp1}_f = \dfrac{C_f Q_f^* \tau}{Cm\rho^* H}$ определяет соотношение между тепловоспринимающей способностью холодного теплоносителя (f=1) или горячего теплоносителя (f=2) и теплоаккумулирующей способностью насадки.

Критерий $\mathrm{Kp2}_f = \dfrac{C_f Q_f^*}{\alpha_f \rho^* f_0 H}$ – соотношение между тепловоспринимающей способностью холодного теплоносителя (f=1) или горячего теплоносителя (f=2) и интенсивностью конвективного теплообмена.

Здесь C – теплоемкость насадки, Дж/(кг·К);

C_f – теплоемкость теплоносителей, Дж/(м3·К);

f_0 –удельная поверхность насадки, м2/кг;

H – высота насадки, м;

m –коэффициент массивности насадки;

Q_f^* – приведенный расход теплоносителей, м3/(м2·с);

α_f – коэффициент теплоотдачи, Вт/(м2□К);

ρ* – плотность насадки, кг/м3;

τ – время, с.

Индекс f – номер теплоносителя: f=1 – холодный теплоноситель, f=2 – горячий теплоноситель.

Удельная поверхность насадки $f_0 = H' / \rho^*$

Коэффициент массивности насадки [3] $m = 1 + \mathrm{Bi}/3,$ где Bi –число Био.

Приведенный расход теплоносителей $Q_f^* = Q_f / S$, где S – полное сечение насадки, м.

Полученные критерии включают в себя как конструктивные, так и режимные характеристики регенеративного теплообменника. Используя эти критерии, можно для имеющихся аппаратов подобрать рациональный режим работы.

Можно решить и обратную задачу. Используя полученные критерии, можно, задаваясь температурой нагрева холодного теплоносителя, получить необходимые значения конструктивных и режимных параметров. Разумеется, полученные результаты будут приближенными, но они позволят оценить эффективность внедрения новых конструкций насадок и подобрать соответствующий режим работы.

Анализ критериальных уравнений для регулярного режима регенеративного теплопереноса позволяет выявить связи между всеми теплофизическими, конструктивными и режимными параметрами регенеративного теплообменного аппарата. Обобщенная, безразмерная форма критериальных уравнений дает возможность выбора требуемых параметров любых РТА в зависимости от предъявляемых требований и оптимизации как характеристик насадки, так и режимов работы. Решение критериальных уравнений [4] в заданных условиях однозначности (начальные и конечные температуры теплоносителей) дает конкретные значения критериев Kp1 и Kp2 , которые могут быть получены при различных комбинациях входящих в них параметров. В частности, критерий показывает соответствие между длительностью периодов и высотой насадки, позволяет определить необходимый приведенный расход теплоносителей *Q**, м3/(м2*с). Причем один и тот же результат можно получить при разных характеристиках насадки за счет соответствующего подбора режимных параметров.

Регулярный режим можно реализовать для любых значений времени нагрева и охлаждения при условии линейного повышения температуры греющего теплоносителя в период нагрева и линейного снижения до минимальной температуры холодного теплоносителя в течении периода охлаждения. При постоянных температурах теплоносителей на входе в насадку с ростом продолжительности периода происходит переход к нерегулярному режиму.

Проиллюстрируем на примере как можно применить критериальный анализ. По программе [7] выполнена серия расчетов доменного воздухонагревателя при следующих исходных данных:

1. Высота насадки H= 40,6 м.
2. Полное сечение насадки S= 42 м2.
3. Живое сечение насадки F= 14,07 м2.
4. Удельное живое сечение насадки f= 0,335 м2/м2.
5. Удельная поверхность нагрева H'= 32,7 м2/м3.
6. Эквивалентная полутолщина слоя δ=0,02035 м.
7. Гидравлический диаметр $d_э$=0,041 м.
8. Удельная масса насадки ρ*=1415,8 кг/м3.
9. Удельная поверхность насадки f_0= 0,0231 м2/кг.
10. Длительность периода нагрева τ_1=7200 с.
11. Длительность периода охлаждения τ_2= 3000 с.
12. Расход холодного теплоносителя Q_1=92 м3/с.
13. Приведенный расход холодного теплоносителя Q_1^*=2,1905 м3/(м2·с).
14. Температура холодного дутья t_{11}= 70 °С.

15. Температура дымовых газов на входе в насадку t_{21}= 1300 °С.

В расчетах менялось время периодов нагрева и охлаждения при прочих неизменных условиях.

Проведённые расчеты, во-первых, дают распределение температуры насадки и теплоносителей по высоте, т.е. позволяют судить о том насколько выбраны режим работы аппарата обеспечивает линейное распределение температуры по высоте насади. Во-вторых, программа рассчитывает значения средних коэффициентов теплоотдачи теплоносителей и теплопроводности насадки.

Расчеты показывают, что для насадки 4 при приведенном расходе Q^*_1 =2,1905 м3/(м2·с) регулярный режим можно реализовать при продолжительности периода охлаждения не более 50 мин. Результаты расчета следующие:

1. Расход топлива 15,031 м3/с, ему соответствует расход дымовых газов $Q_2 = 36{,}5283\ м^3/с$ и приведенный расход горячего теплоносителя Q_2^*=0,875 м3/(м2·с).
2. Температура газа (°С) на выходе из насадки:

   Период нагрева насадки:

   - в начале периода: 143,78;
   - в конце периода: t_{22}= 400,05;
   - средняя за период: 275,73.

Период охлаждения насадки:

- в начале периода: 1248,25;
- в конце периода: t_{12}=1143,91;
- средняя за период: 1198,26.

Средняя теплоемкость кладки С=1220,1241 Дж/(кг·К).

Средний коэффициент теплоотдачи:

- период нагрева α_2=21,7634 Вт/(м2·К);
- период охлаждения α_1=28,3951 Вт/(м2·К).

Данному режиму работы регенеративного теплообменника соответствует значение критерия =0,1.

Распределение температуры насадки и теплоносителя по высоте аппарат показано на рисунке 1.

Допустим, что мы решили поменять насадку теплообменника на более эффективную и обеспечить тот же уровень нагрева теплоносителя. Выясним, какой должен быть режим работы теплообменника и его конструкция, чтобы обеспечить наиболее эффективную его работу. Анализ на основе критерия показывает, что при той же температуре нагрева холодного теплоносителя и той же продолжительности нагрева (охлаждения) необходимо на 4 м уменьшить высоту насадки. Такое сравнительно небольшое изменение в габаритах объясняется сравнительно низкой аккумулирующей способностью насадки по сравнению с более развитой поверхностью нагрева.

Чтобы использовать данную насадку более эффективно необходимо использовать материал с большей плотностью, теплопроводностью и теплоемкостью, например вместо динаса использовать муллитокорундовые огнеупоры. В этом случае при сохранении той же температуры нагрева холодного теплоносителя и продолжительности нагрева при условии =0,1 можно сократить высоту насадки на 10 м, т.е. на 25%.

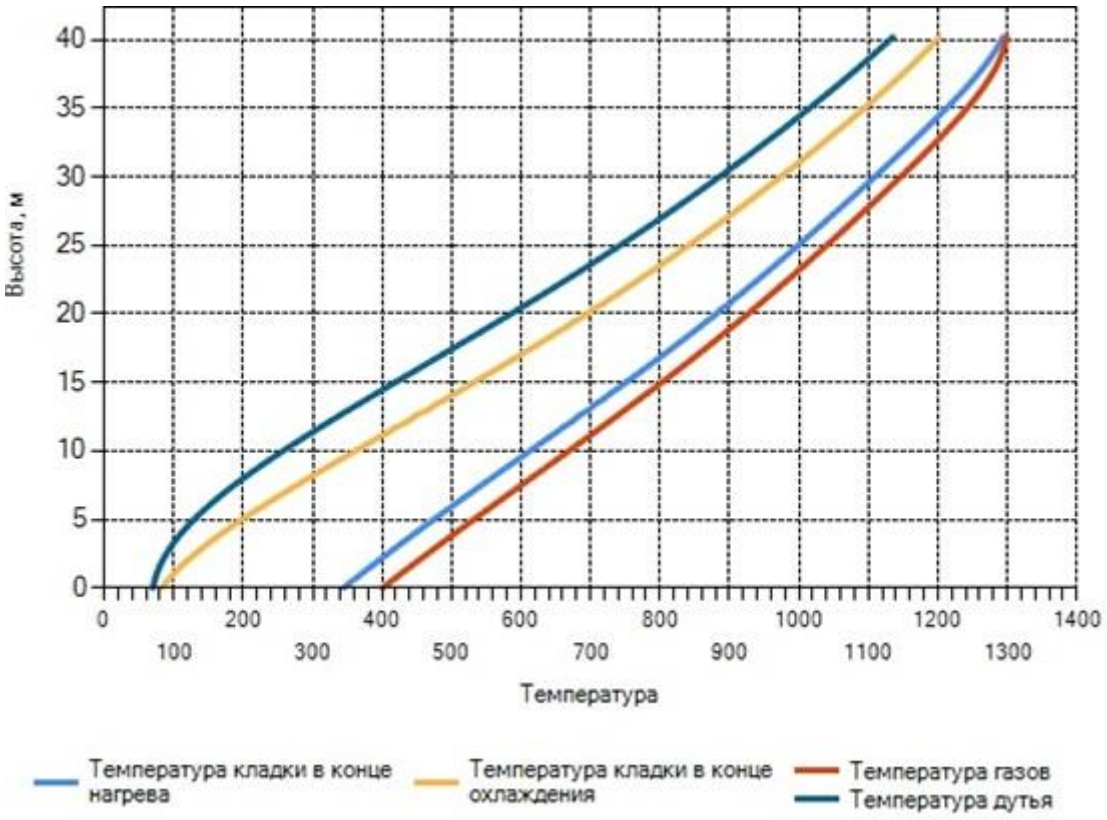


Рисунок 1 – Изменение температуры по высоте насадки при реализации регулярного режима

Учитывая обобщенный характер критерия Kpl_1, его значение 0,1 является границей реализации регулярного режима для любого типа насадки. Снижение расхода теплоносителя сопровождается увеличением временного диапазона реализации регулярного режима, например, при приведенном расходе нагреваемого теплоносителя 1,4 м3/(м2·с) регулярный режим реализуется при продолжительности 80 мин. В рамках регулярного режима снижение продолжительности периода охлаждения и приведенного расхода сопровождаются увеличением температуры дутья, снижением температуры дымовых газов и увеличением коэффициента использования тепла.

Заключение

Расчеты, выполненные с помощью программы, показали, что наиболее рациональным для работы регенеративного теплообменника является режим, обеспечивающим линейное распределение температуры по высоте насадки. Добиться такого распределения возможно при определенном сочетании конструктивных параметров насадки и режимных параметров работы теплообменного аппарата. С помощью критериев подобия определена граница существования режима, обеспечивающего линейное распределение температуры по высоте насадки.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-08-01078 А

Список литературы

1. Кирсанов Ю.А. Циклические тепловые процессы и теория теплопроводности в регенеративных воздухоподогревателях. М.: ФИЗМАТЛИТ –2007, 240 с.
2. Самарин О.Д. Температурная эффективность пластинчатых и роторных теплоутилизаторов при различных расходах воздуха // Сантехника, Отопление, Кондиционирование, 2014, № 1 (145). – С. 118-119.
3. Шкляр Ф.Р. Доменные воздухонагреватели (конструкции, теория, режимы работы) / Шкляр Ф.Р., Малкин В.М., Каштанова С.П., Калугин Я.П., Советкин В.Л.– М.: Металлургия, 1982. – 176 с.
4. Yu. V. Shatskikh, A. I. Sharapov, A. G. Arzamassev and Yu. A. Geller. Optimization of the operation mode of regenerative heat exchangers / Published under licence by IOP Publishing Ltd Journal of Physics: Conference Series, Volume 2119, The XXXVII Siberian Thermophysical Seminar (STS37), 2021 J. Phys.: Conf. Ser. 2119 012156.
5. Соломенцев С.Л. Рациональные типы насадок и доменных воздухонагревателей. Липецк: ЛГТУ., 2001. 432 с.
6. Кондратьев Г.М. Регулярный тепловой режим. М.: ГИТТЛ, Гостехиздат, 1954. 408 с.
7. Свидетельство о государственно регистрации программы для ЭВМ № 2021668760 «Программа для расчета регенеративных теплообменников с неподвижной насадкой».

References

1. Kirsanov Yu.A. Cyclic thermal processes and the theory of heat conduction in regenerative air heaters. M.: FIZMATLIT -2007, 240 p.
2. Samarin O.D. Temperature efficiency of plate and rotary heat exchangers at different air flow rates // Sanitary engineering, Heating, Air conditioning, 2014, No. 1 (145). - S. 118-119.
3. Shklyar F.R. Blast furnaces (designs, theory, modes of operation) / Shklyar F.R., Malkin V.M., Kashtanova S.P., Kalugin Ya.P., Sovetkin V.L. - M .: Metallurgy, 1982. – 176 p.
4. Yu. V. Shatskikh, A. I. Sharapov, A. G. Arzamassev and Yu. A. Geller. Optimization of the operation mode of regenerative heat exchangers / Published under license by IOP Publishing Ltd Journal of Physics: Conference Series, Volume 2119, The XXXVII Siberian Thermophys-ical Seminar (STS37), 2021 J. Phys.: Conf. Ser. 2119 012156.
5. Solomentsev S.L. Rational types of nozzles and blast furnaces. Lipetsk: LGTU., 2001. 432 p.
6. Kondratiev G.M. Regular heat. M.: GITTL, Gostekhizdat, 1954. 408 p.
7. Certificate of state registration of the computer program No. 2021668760 “Program for calculating regenerative heat exchangers with a fixed nozzle”.

Шаханова М. В., Кий Ю. А., Шаханова Э. С. Методы анализа защищённости компьютерных сетей // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 22–27

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.7

МЕТОДЫ АНАЛИЗА ЗАЩИЩЁННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Шаханова М. В., Кий Ю. А., Шаханова Э. С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, д.50а), e-mail: marinavl2007@yandex.ru

Повсеместное развитие и интеграция информационных технологий приводит к глобальным трендам цифровой трансформации всех профессиональных областей жизнедеятельности человека. Одним из актуальных вопросов в современных реалиях является обеспечение информационной безопасности используемых на предприятиях компьютерных сетей. Основной целью текущей статьи является исследование методов анализа защищенности компьютерных сетей. Автором предпринимается попытка систематизации знаний, касающихся основных аспектов использования методов анализа защищенности компьютерных сетей. Научная ценность работы заключается в возможности использования полученных материалов в качестве теоретической базы для дальнейших исследований из области разработки методов защиты. В работе применяются теоретические методы исследования, а также используются зарубежные и отечественные научные материалы.

Ключевые слова. Информационные технологии, информационная безопасность, компьютерная сеть, информация, защищенность.

METHODS FOR ANALYZING THE SECURITY OF COMPUTER NETWORKS

Shakhanova M. V., Kiy Yu. A., Shakhanova E.S.

G.I. Nevelsky Maritime State University, Vladivostok, Russia (690003, Vladivostok, st. Verkhneportovaya, 50a), e-mail: marinavl2007@yandex.ru

The widespread development and integration of information technologies leads to global trends in the digital transformation of all professional areas of human activity. One of the urgent issues in modern realities is ensuring information security of computer networks used at enterprises. The main purpose of the current article is to study methods for analyzing the security of computer networks. The author attempts to systematize knowledge concerning the main aspects of using methods of analyzing the security of computer networks. The scientific value of the work lies in the possibility of using the obtained materials as a theoretical basis for further research in the field of developing protection methods. Theoretical research methods are used in the work, as well as foreign and domestic scientific materials are used.

Keywords: Information technology, information security, computer network, information, security.

С помощью информации, непрерывно обрабатываемой и передающейся в различных инфокоммуникационных системах и сетях, происходит обмен конфиденциальными данными, производятся транзакции на различных предприятиях, а также выполняется работа с засекреченной информацией и данными ограниченного доступа. Данный список можно перечислять без конца так как в современном мире все процессы, происходящие в бытовой и

профессиональной сфере жизнедеятельности человека, основываются на использовании информационных технологиях [1].

Ввиду этого, формируется и актуализируется проблема, связанная с обеспечением безопасности работы с информационными ресурсами. Таким образом, вопрос информационной безопасности – это одно из ключевых и приоритетных направлений становления современного технологического прогресса. В современном мире существует большое количество способов и средств защиты информации в различных инфокоммуникационных системах и сетях. Именно способы защиты информации формируют кластер развития средств защиты информации, используемых в современных инфокоммуникационных системах [2].

Исходя из высокой степени необходимости использования компьютерных сетей на современных предприятиях, все большее внимание уделяется в сторону вопросу поддержания их должного уровня информационной безопасности. Непрерывное развитие и повсеместное использование сетей порождает рост уязвимостей программных ресурсов. В свою очередь, широкое распространения средств реализации данных угроз актуализирует применение различных систем анализа защищенности.

Данные системы представляют программно-аппаратные средства, направленные на выявление фактов несанкционированного доступа в компьютерную сеть. При этом выделяется три основных типа атаки. Первый из них является подготовительным и заключается в поиске предпосылок для выполнения той или иной атаки. На данном этапе производится поиск уязвимостей, дальнейшее использование которых и приводит к реализации атаки, что является вторым этапом. На третьем этапе происходит завершение атаки и «заметание» следов. Методы анализа защищенности компьютерных сетей направлены на обеспечение дополнительного уровня защиты компьютерных сетей и разделяются на такие классы относительно позиции в сети, как хостовые и сетевые системы обнаружения вторжений [3].

Необходимо отметить, что обнаружением вторжений занимаются системы анализа защищенности. Таковыми являются различные сканеры безопасности, а также системы поиска уязвимостей. На их основе производятся всесторонние исследования заданных систем для обнаружения уязвимостей, приводящих к нарушениям целостности и информационной безопасности. При этом наибольший уровень угрозы представляют уязвимости проектирования, обнаружение и устранение которых требует большого труда.

Защищенность представляет собой ключевой показатель эффективности функционирования компьютерных сетей, наряду с показателями надежности, отказоустойчивости, производительности и других. Под защищенностью компьютерных сетей обычно понимается степень адекватности реализованных в ней механизмов по обеспечению защиты информации, потенциально подверженной рискам, связанным с осуществлением угроз безопасности. Данные угрозы могут нарушать такие свойства информации, как ее конфиденциальность, целостность и доступность.

На сегодняшний день существует ряд основных методов анализа защищённости компьютерных сетей, предполагающих использование активных и пассивных систем тестирования. В таблице 1 представлен аналитический свод наиболее распространенных методов анализа защищенности сетей [4-5].

Таблица 1 – Методы анализа защищённости компьютерных сетей

Метод	Описание	Преимущества	Недостатки
Анализ механизмов безопасности организационного уровня	Включает в себя анализ политики безопасности организации и документации по обеспечению режима информационной безопасности. Производится оценка их соответствия существующим требованиям и адекватность к реагированию рискам.	Позволяет выявить несоответствия на начальном уровне построения компьютерной сети.	Долгая обработка данных и информации о рисках нарушения безопасности. Недостаточный уровень автоматизации процессов поиска аномалий.
Ручной анализ конфигурационных файлов	Включает в себя анализ межсетевого экрана, прокси-серверов, на основе которых производится управление межсетевыми взаимодействиями, а также иных критических элементов сетевой инфраструктуры.	Может быть полезен при анализе обеспечения информационной безопасности на объектах, где не существует возможности анализа реальных электронно-вычислительных систем.	Низкая эффективность выявления угроз относительно программных методов.
Сканирование внешних сетевых адресов ЛВС из сети Интернет	Основывается на пингах компьютерной сети с целью выявления внешних IP-адресов и отображает распределение типов ресурсов по сети для выявления аномалий.	Позволяет произвести анализ защищенности относительно внешних угроз безопасности. Высокая эффективность и скорость выявления аномалий.	Ограничен сканированием внешних ресурсов. Требует использование платного программного обеспечения.
Сканирование ресурсов ЛВС изнутри	Основывается на пингах компьютерной сети с целью выявления внутренних IP-адресов и отображает распределение типов ресурсов по сети для выявления аномалий.	Позволяет произвести наиболее эффективный анализ защищенности относительно внутренних угроз безопасности.	Ограничен сканированием внутренних ресурсов. Требует использование платного программного обеспечения.

Продолжение Таблицы 1

Метод	Описание	Преимущества	Недостатки
Анализ конфигурации серверов и рабочих станций ЛВС	Производится посредством специализированных программных агентов, выявляющих аномалии и нарушения информационной безопасности сети.	Представляет возможность быстрого и эффективного поиска угроз безопасности на основе использования программных продуктов. Представляет высокую актуальность своего использования для сканирования масштабных и территориально-распределенных компьютерных сетей.	Требует использование дорогостоящего программного обеспечения. Не является рациональным к использованию небольших компьютерных сетей.

Представленные в таблице 1 методы имеют индивидуальные особенности, использование которых в соответствии каждой из них может быть рационально в зависимости от размерности и выполняемых задач компьютерных сетей. Так, к примеру, аппаратные методы анализа защищенности (ручной анализ конфигурационных файлов, анализ механизмов безопасности организационного уровня) являются наиболее эффективным методом сканирования небольших сетей или при решении задач выявления угроз безопасности на этапе проектирования сетей [6-7].

При этом программные методы позволяют произвести более быстрый анализ защищенности масштабных и территориально-распределенных компьютерных сетей, но требуя использование платных программных продуктов. Одними из наиболее распространенных программных продуктов, использующихся при реализации программного анализа защищенности компьютерных сетей являются следующие инструменты, представленные на рисунке 1.

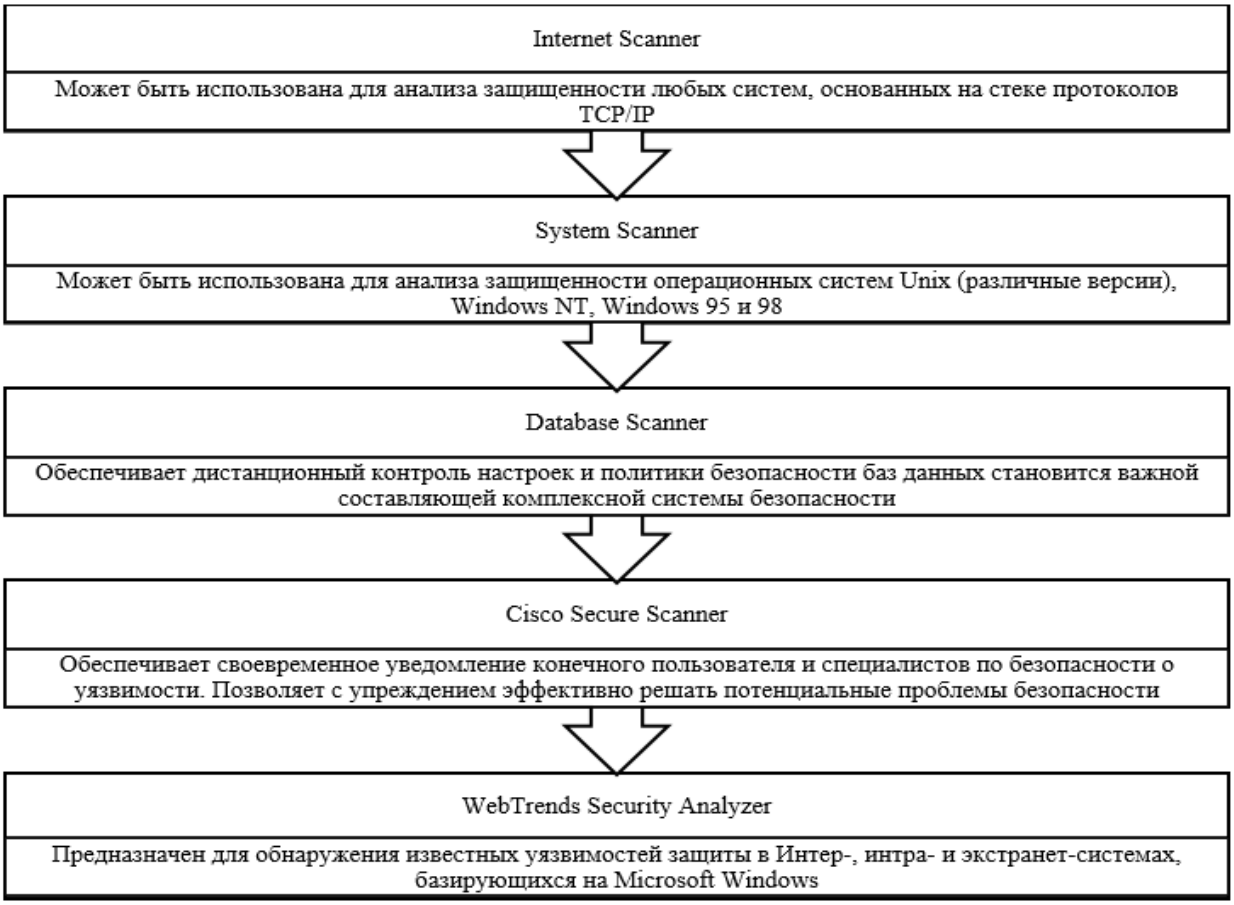


Рисунок 1 – Средства анализа защищенности компьютерных сетей

Таким образом, основной целью представленной статьи являлось исследование методов анализа защищенности компьютерных сетей. В заключение необходимо отметить, что вопрос обеспечения информационной безопасности занимает ключевое место в развитии сегмента информационных технологий. При этом ввиду непрерывного появления новых уязвимостей необходимо разрабатывать новые и повышать эффективность существующих инструментов обнаружения угроз и анализа защищенности компьютерных сетей.

Список литературы

1. Дойникова Е.В., Федорченко А.В., Котенко И.В., Новикова Е.С. Методика оценивания защищенности на основе семантической модели метрик и данных // Вопросы кибербезопасности. 2021.
2. Борзенкова С.Ю., Казарина Е.Е. Анализ методов оценки уровня защищенности информационных систем в процессе их эксплуатации // Известия ТулГУ. Технические науки. 2020.
3. Бутин А.А. Методологии анализа защищенности информации в автоматизированных системах // Достижения науки и образования. 2018.
4. Kotsynyak M.A., Spitsyn O.L., Ivanov D.A. Methodology for assessing network stability in conditions of targeted cybernetic attack // High-tech technologies in Earth space research. 2018.

5. Грушо А. А., Грушо Н. А., Забежайло М. И., Тимонина Е. Е. Методы оценки защищенности компьютерных систем информационной поддержки цифровой экономики // International Journal of Open Information Technologies. 2019.
6. Yuganson A.N., Zakoldaev D.A. An approach to assessing the security of embedded software in the conditions of fuzzy input information. Vestnik AGTU. Series: Management, Computer Engineering and Computer Science. 2020.
7. Шинкаренко А.Ф. Методика оценивания защищенности информационно-телекоммуникационных узлов // Интеллектуальные технологии на транспорте. 2016.

References

1. Doynikova E.V., Fedorchenko A.V., Kotenko I.V., Novikova E.S. Methodology for evaluating security based on the semantic model of metrics and data // Issues of cybersecurity. 2021.
2. Borzenkova S.Yu., Kazarina E.E. Analysis of methods for assessing the level of security of information systems during their operation. Izvestiya TulGU. Technical science. 2020.
3. Butin A.A. Methodologies for analyzing information security in automated systems // Achievements of science and education. 2018.
4. Kotsynyak M.A., Spitsyn O.L., Ivanov D.A. Methodology for assessing network stability in conditions of targeted cybernetic attack // High-tech technologies in Earth space research. 2018.
5. Grusho A. A., Grusho N. A., Zabezhailo M. I., Timonina E. E. Methods for assessing the security of computer systems for information support of the digital economy // International Journal of Open Information Technologies. 2019.
6. Yuganson A.N., Zakoldaev D.A. An approach to assessing the security of embedded software in the conditions of fuzzy input information. Vestnik AGTU. Series: Management, Computer Engineering and Computer Science. 2020.
7. Shinkarenko A.F. Methods for assessing the security of information and telecommunication nodes // Intelligent technologies in transport. 2016.

Хитев А. П., Шиков И. В. Перспективы использования информационных технологий в раскрытии и расследовании преступлений // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 28–31

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Хитев А. П., Шиков И. В.

Владимирский юридический институт Федеральной службы исполнения наказания России, Владимир, Россия (600020, г. Владимир, ул. Б. Нижегородская, 67е), e-mail: hitevap@mail.ru

В России компьютерная криминалистика не имеет широкого распространения, что снижает качество расследования кибератак. С появлением облачных технологий, цифровая криминалистика столкнулась с объективно существующими проблемами. Для решения поставленной проблемы необходимо уделять особое внимание развитию науки компьютерной криминалистики, установлению стандартов деятельности при расследовании таких преступлений и повышению компьютерной грамотности населения.

Ключевые слова: Компьютерная криминалистика, специалист, кибератака, киберпреступление, информация, цифровизация.

PROSPECTS FOR THE USE OF INFORMATION TECHNOLOGY IN THE DETECTION AND INVESTIGATION OF CRIMES

Khitev A. P., Shikov I. V.,

Vladimir Law Institute of the Federal Penitentiary Service of Russia, Vladimir, Russia (600020, Vladimir, B. Nizhegorodskaya st., 67e), e-mail: hitevap@mail.ru

In Russia, computer forensics is not widely used, which reduces the quality of cyberattack investigations. With the advent of cloud technologies, digital forensics has faced with objectively existing problems. To solve this problem, it is necessary to pay special attention to the development of computer forensics science, the establishment of standards for the investigation of such crimes and the improvement of computer literacy of the population.

Keywords: Computer forensics, specialist, cyberattack, cybercrime, information, digitalization.

В век информационных технологий, проблема кибербезопасности приобрела особое значение. Компьютерные науки с каждым годом выходят на новый уровень развития, технологии совершенствуются и внедряются в повседневную жизнь, сохраняя все данные о пользователе. По этой причине человек начинает задумываться о безопасности собственной информации. Однако технологии злоумышленников также «не стоят на месте», и как следствие совершаются киберпреступления нового масштаба.

Оптимизация расследования – это проблема, которая постоянно стоит перед теорией криминалистики. Она обусловлена практикой установления обстоятельств совершения преступлений. То, насколько успешно данная проблема будет разрешена, во многом зависит от средств, которые используются в ходе расследования.

В России компьютерная криминалистика не имеет широкого распространения, что снижает качество расследования кибератак. Так, при расследовании взлома квартиры, следователь имеет чёткое понимание поэтапности своих действий. Поступил звонок, выезд на место преступления, осмотр места преступления, сбор вещественных доказательств, допрос потерпевших и свидетелей и т.п. При расследовании преступлений, связанных с хищением денежных средств с расчетных счетов или персональных данных, обнародованием порочащей честь и достоинство граждан информации, необходимы специальные знания порядка возникновения и движения информации в киберпространстве. В такой момент расследование становится невозможным без специалиста-форензика.

Возникновение информационной среды способствовало возникновению цифровой следовой информации, позволяющей не только расследовать и раскрывать преступления, но и пресекать совершения возможных преступлений, таким примером может служить АИС «Безопасный город» и интегрированных в нее подсистем, видеофиксации, геопозиционирования и др. Создаваемые на основе этой системы центры обработки и хранения информации позволяют выявлять и пресекать преступления [2, с. 150].

Эволюция способов совершения преступлений и орудий преступлений не всегда требует эволюции науки криминалистики и появления ее разновидностей. Надо просто оценить перспективы экстраполяции способов и методик доказывания обстоятельств совершения преступлений в эпоху цифровизации общественных отношений с точки зрения положений современной криминалистики и всего криминального научного блока. Вместе с тем криминалистика признает наличие такой науки, как информатика, под которой понимается техническая наука, систематизирующая приемы создания, хранения, обработки и передачи информации средствами электронно-вычислительной техники, а также принципы функционирования этих средств и методы управления ими.

За рубежом во многих англоязычных странах она также называется computer science – компьютерная наука. Теоретической основой информатики является группа фундаментальных наук, основанных на физике и высшей математике [1, с. 19].

В Российской Федерации, с появлением облачных технологий, цифровая криминалистика столкнулась с объективно существующими проблемами. Несмотря на имеющиеся немногочисленные исследования по цифровой криминалистике в облачных структурах, эта тема все еще в значительной степени не исследуется, и ученым предстоит проделать огромный объем работы [3, с. 75].

В настоящее время количество составленных нормативных правовых актов и научных доктрин об информации и её защите недостаточно для достижения поставленных целей в области обеспечения информационной безопасности. Для решения данной проблемы необходимо составить методические рекомендации, которые будут подробно описывать действия следователей и специалистов в различных областях науки и техники при расследовании киберпреступлений с учётом их вариативности.

Кроме того, необходимо сформировать максимально возможный список преступлений, связанных с движением информации в компьютерном пространстве, сгруппировав их по схожим признакам и индивидуальным особенностям.

Первоначальные действия специалиста должны быть связаны с собиранием и сохранением имеющихся данных, классификацией противоправных деяний, оценкой ущерба

и оставшихся потенциальных рисков. В зависимости от вида преступления способ и объем указанных данных будет отличаться.

Необходимо помнить, что сведения, полученные с компьютера нематериальны, а значит привычные следователям варианты раскрытия преступлений в большинстве случаев будут неэффективны. После чего, необходимо определить круг лиц, который имел доступ к объекту защиты информации, а также перекрыть потенциальные каналы утечки информации, обезопасив оставшиеся данные.

Следующим этапом является анализ полученных сведений, а также моделирование ситуации и восстановление хронологии событий по зафиксированным сохраненным данным с использованием специальных ПО (например: AccessDataForensicToolkit, BrowserForensicTool, EncryptedDiskDetector и т.д.). Набор базовых программ также необходимо отразить в специальной документации. Последующие действия связаны непосредственно с установлением лица, совершившего преступление, которое будет проходить по индивидуальной схеме в зависимости от киберпреступления.

Актуальность проблемы компьютерной криминалистической методики указывает на необходимость развития области компьютерной криминалистики на документальном и официальном уровне. Преимуществом создания предложенных документаций является универсальность данного порядка действий. Общая последовательность действий для криминалиста будет актуальна и полезна для каждого преступления.

Постоянное улучшение методов кибератак и повышение квалификации криминалистов требует постоянного обновления и дополнения нормативных правовых документов, для поддержания уровня и продолжения раскрытия усовершенствованных киберпреступлений.

Постоянного развития сферы компьютерной криминалистики на документальном уровне недостаточно для повышения уровня развития форензики в России. Необходимым дополнением является введение новых предметов при обучении криминалистов и следователей или добавление новой специальности.

Таким образом, при росте совершаемых в век информационных технологий преступлений, связанных с движением информации в компьютерном пространстве, усложнение алгоритмов вредоносных программ, отсутствие достаточного количества нормативных правовых и научных источников, закрепляющих поэтапный и подробный ход расследования таких преступлений, существенно влияет на предотвращение и раскрываемость последних. Для решения поставленной проблемы необходимо уделять особое внимание развитию науки компьютерной криминалистики, установлению стандартов деятельности при расследовании таких преступлений и повышению компьютерной грамотности населения.

В заключении хочется еще раз подчеркнуть, что обеспечения безопасности общества является приоритетной задачей, как государства в целом, так и правоохранительных органов в частности, построение правового общества и государства не возможно, без контроля над преступностью и неотвратимости наказания. А информационные технологии способны стать теми информационно-технологическими средствами, которые облегчат достижения задач по раскрытию расследованию преступлений и станут теми инструментами, теми драйверами модернизации процессов профилактики и борьбы с преступностью.

Учитывая специфику облачных структур, для всего мирового сообщества, вовлеченного в цифровизацию, видится целесообразным интеграция научных криминалистических знаний, накопленных в РФ с целью:

- разработки специальных юридических средств и методов, регулирующих сферу предоставления облачных услуг;
- разработки и введения общего международного стандарта для развертывания и функционирования облачных инфраструктур, обеспечивающего возможность криминалистического сбора информации в соответствии с тремя компонентами, описанными выше;
- введения стандартов по применяемым инструментам и методам, используемым в цифровой криминалистике, с целью не допустить исключения собранных доказательств в суде;
- обмена практическими рекомендациями, выполненными исследователями, с целью развития и совершенствования применяемых криминалистических средств и методов.

В этой связи, безусловно, необходимо внедрение передовых достижений науки и техники в цифровую криминалистику, которая постепенно занимает лидирующие позиции в раскрытии и расследовании преступлений во всем мире.

Таким образом, актуальность цифровой криминалистики и разработка ею различных методов в целях раскрытия, расследования и предупреждения преступлений с каждым годом будет увеличиваться. Это обусловлено тем, что цифровизация проникает во все сферы человеческой жизни.

Список литературы

1. Кучин О.С. К вопросу о дефиниции «цифровая криминалистика» // Современные технологии и подходы в юридической науке и образовании: Сборник 157 материалов международного научно - практического форума, Калининград, 2021. С. 19.
2. Морозова Н.В. Криминалистические методики расследования преступлений. Основания и принципы формирования // Закон и право. 2020. № 8. С. 150.
3. Шевченко А.С. Методы цифровой криминалистики в расследовании преступлений // Современные вызовы и перспективы развития молодежной науки. 2021. С. 75.

References

1. Kuchin O.S. On the question of the definition of "digital forensics" // Modern technologies and approaches in legal science and education: Collection of 157 materials of the international scientific and practical forum, Kaliningrad, 2021. p. 19.
2. Morozova N.V. Forensic methods for investigating crimes. Foundations and principles of formation // Law and law. 2020. No. 8. p. 150.
3. Shevchenko A.S. Digital Forensics Techniques in the investigation of crimes // Modern challenges and prospects for the development of youth science. 2021, p. 75.

Василевский К. А, Андреева Я. А., Гаранин Т. Д. Сферы применения нейронных сетей в современном мире и их будущее // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть3 с. 32–42

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.8

СФЕРЫ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ В СОВРЕМЕННОМ МИРЕ И ИХ БУДУЩЕЕ

[1] Василевский К. А, [2] Андреева Я. А., [3] Гаранин Т. Д.
Московский технический университет связи и информатики, Москва, Россия (111024, Москва, улица Авиамоторная, д.8а), e-mail: [1] alaxtver@yandex.ru, [2] andreevaya.00@mail.ru [3] Veneriec@gmail.com

Статья посвящена актуальной теме исследования, поскольку нейронные сети - одна из самых востребованных для изучения в сфере информационных технологий. Нейронные сети на сегодняшний день весьма популярны, сферы их применения с каждым днем только расширяются.
В качестве предмета исследования выступают нейронные сети.
Данное исследование посвящено сферам применения нейронных сетей в современном мире и их будущему.
Методы исследования – теоретические методы: анализ источников, систематизация и обобщение.
В результате был сделан вывод о том, что нейронные сети созданы для того, чтобы оказывать людям максимальную помощь в решении любых задач. Обладая большим объемом информации, нейронные сети можно научить чему угодно. Возможности поистине огромны, и каждый день открываются новые области применения. Нейронные сети – это будущее, они перевернут наш мир и создадут множество дополнительных направлений в профессиональной деятельности.

Ключевые слова: Нейронная сеть, изображение, распознавание, движение, мимика.

NEURAL NETWORKS IN THE MODERN WORLD AND THEIR FUTURE

[1] Vasilevskii K.A., [2] Andreeva Y.A., [3] Garanin T.D.
Moscow Technical University of Communications and Informatics, Moscow, Russia (111024, Moscow, Aviamotornaya st, 8a), e-mail: [1] alaxtver@yandex.ru, [2] andreevaya.00@mail.ru [3] Veneriec@gmail.com

Article is devoted the actual theme of research as neural networks are one of the most demanded for studying in the field of information technologies. Neural networks today are very popular, the scope of their application is only expanding with each passing day.
The subject of the research is neural networks.
This research is devoted to the spheres of neural networks application in the modern world and their future.
The research methods are theoretical methods: analysis of sources, systematization and generalization.
As a result it was concluded that neural networks are created to help people to solve any problems as much as possible. Possessing a large amount of information, neural networks can be taught anything. The possibilities are truly enormous, and new applications are being discovered every day. Neural networks are the future, they will turn our world upside down and create many additional areas of professional activity.

Keywords: Neural network, image, recognition, motion, facial expressions.

Введение

Большинство сфер человеческой деятельности нуждаются в постоянном изменении и совершенствовании. С каждым годом увеличивается объем информационных данных и скорость их динамики. Использование человеческого интеллекта приводит к уменьшению количества решаемых задач. В этих случаях целесообразно использовать нейронные сети для решения нестандартных задач. Одной из самых популярных тем в области информационных технологий в настоящее время являются нейронные сети. В этой области ведутся интенсивные исследования, в их развитие вкладываются значительные средства. Нейронные сети незаметно для рядового потребителя проникают в нашу повседневную жизнь.

Цель статьи – изучить сферы применения нейронных сетей в современном мире и их будущее.

Научная новизна работы состоит в том, что на сегодняшний день сфер применения нейронных сетей в современном мире наблюдается большое количество. Однако стоит отметить, что есть еще сферы, в которых необходимо применение нейронных сетей в будущем (например, сельское хозяйство). Данное требуют дальнейшего их изучения.

Обзор литературы.

На сегодняшний день по данной тематике много разного рода исследований, имеющие практическую ценность. Нейронные сети анализируются в работах таких авторов, как Ю. В. Орлик, А. А. Арбузова, А. В. Ольховников, Д. А. Сапрыкин, А. Н. Цаунит и т.д.

Однако факт наличия достаточно большого количества исследований по данной тематике не исключает необходимости дальнейших исследований и разработок.

Материалы и методы. В качестве методологической и теоретической основы исследования выступили труды отечественных и зарубежных ученых в области нейронных сетей.

Информационную базу исследования составили материалы периодической печати, материалы сайтов Интернет, а также результаты исследований авторов.

Применялись общенаучные методы познания, такие как дедукция, сравнение, аналогия, синтез.

Результаты.

Целесообразно начать с рассмотрения трактовки понятия «нейронная сеть». На Рисунке 1 приведем трактовки разных авторов.

А. Н. Цаунит	• Искусственная нейронная сеть – это машина, моделирующая способ обработки мозгом определенной задачи. Данная сеть как правило реализуется с помощью электронных компонентов или моделируется компьютерной программой. Для достижения высокой производительности нейронные сети используют многочисленные связи между элементарными вычислительными ячейками - нейронами. Искусственная нейронная сеть – это огромный распределенный параллельный процессор, состоящий из элементарных единиц обработки информации, которые накапливают экспериментальные знания и делают их доступными для дальнейшей обработки [10, с.114].
А. К. Кулаченок, Д. А. Сапрыкин	• Искусственная нейронная сеть – это математическая модель и программно-аппаратная реализация, основанная на принципах организации и функционирования сетей нервных клеток живого организма (биологические нейронные сети) [3, с.136]

Рисунок 1 – Понятие «нейронная сеть»

Таким образом, рассмотрев трактовки разных авторов, можно сделать вывод о том, что нейросети – это математические модели и их программная реализация, основанная на структуре нервной системы человека.

Нейронные сети могут применять различные типы данных (рисунок 2)

Рисунок 2 – Типы данных, применяемые нейросетями [4, с.169]

На рисунке 3 проиллюстрируем схему простой нейросети

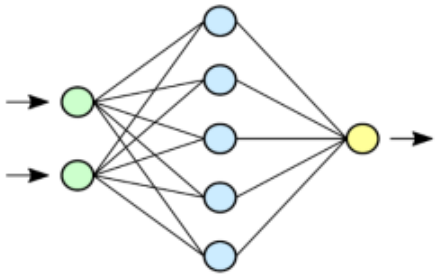


Рисунок 3 – Схема простой нейросети. (Зеленым цветом обозначены входные нейроны, голубым — скрытые нейроны, желтым — выходной нейрон) [2, с.114]

А. В. Ольховников, Д. А. Сапрыкин подчеркивают, что «нейронные сети обучаются, а не программируются в привычном понимании. Способность к обучению выступает в качестве одного из главных преимуществ нейронных сетей перед обычными алгоритмами. Технически обучение заключается в нахождении коэффициента связи между нейронами» [8, с.154].

На рисунке 4 проиллюстрируем задачи нейросетей в современном мире, их три.

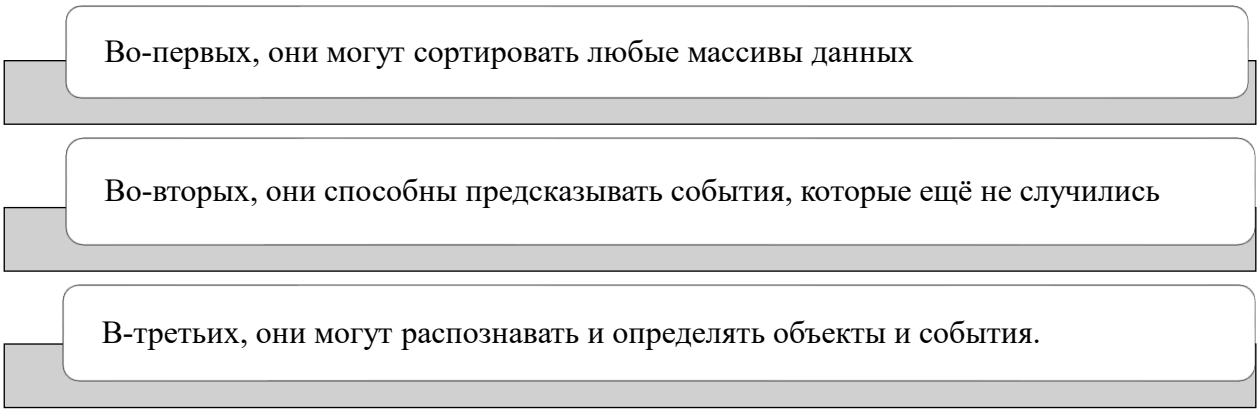


Рисунок 4 – Задачи нейросетей в современном мире

Итак, основная задача нейронной сети – сбор, обработка и анализ информации в режиме самообучения.

Нейронные сети призваны помочь людям выполнить любую задачу как можно лучше. Обладая большим объемом информации, их можно научить чему угодно. Нейронные сети занимают все больше ниш в бизнесе: они ведут подсчет посетителей, следят за соблюдением норм качества и безопасности, считывают номерные знаки автомобилей и т.д. Возможности поистине огромны, и с каждым днем им находят все новые и новые применения.

Стоит отметить о том, что самым распространенным применением нейронных сетей сегодня является распознавание визуальных образов, аудио- и видеоизображений. Нейросети в современном мире встречаются везде - от роботов-автоответчиков в банке до спецэффектов на TikTok, от анализа нефтепроводов до подсчета брака на заводе. Благодаря нейронным сетям труд человека намного облегчается. Помимо прочего, компании, использующие их, экономят миллионы человеко-часов в год.

Сфера применения нейронных сетей растет с каждым годом. По данным компании Allied Analytics, рыночный объем нейросетей в 2023 году будет 39 миллиардов долларов. Данный показатель почти в шесть раз больше, чем в 2016 году.

В современном мире искусственные нейронные сети используются практически во всех областях, где видеонаблюдение (рисунок 5)

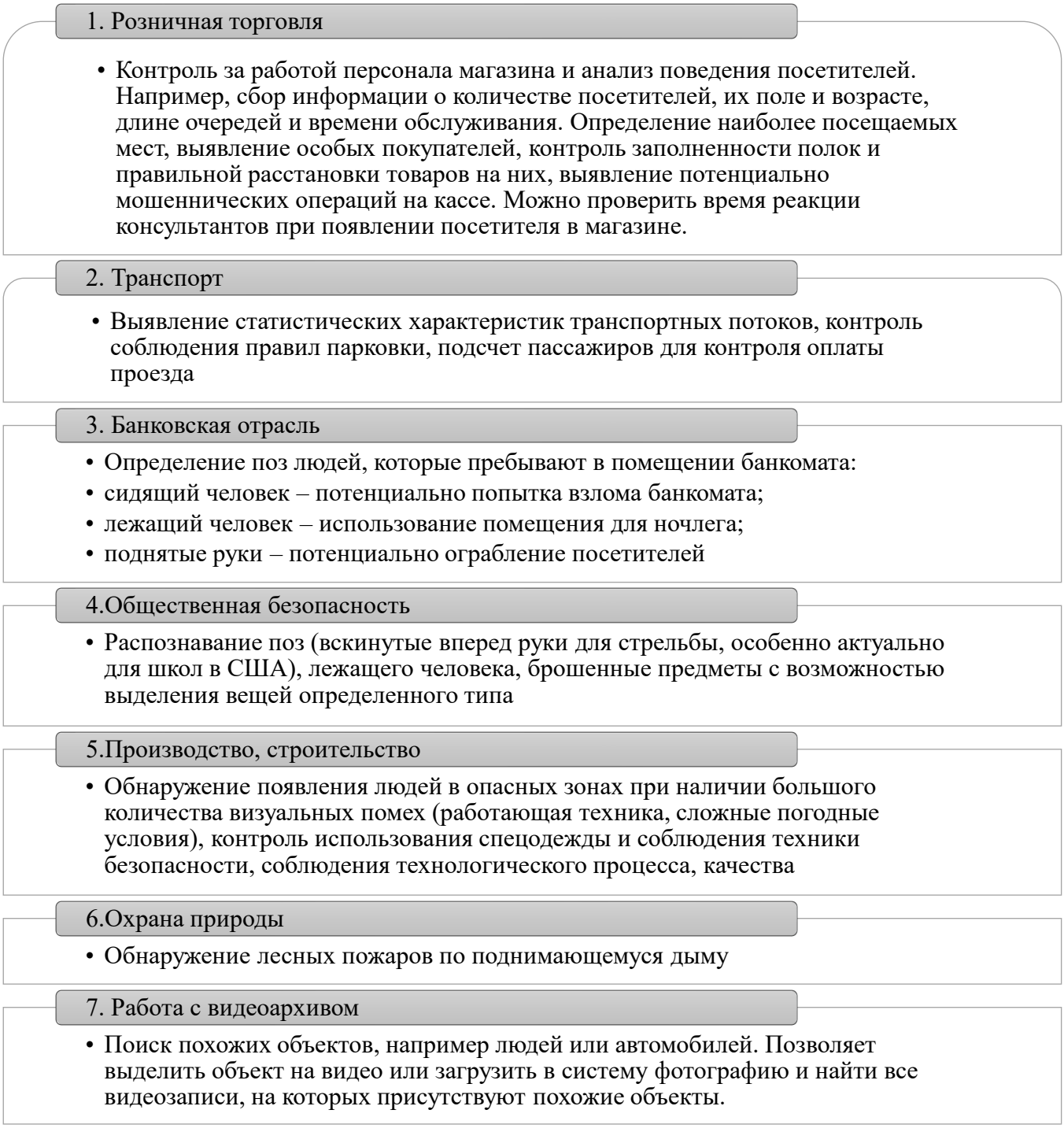


Рисунок 5 – Сферы применения нейронных сетей

Нейросети уже превзошли человека во многих областях. К примеру, распознавание текста при выполнении узкого рода задач, классификация изображений (конкурс ImageNet); программа AlphaGo, применяющая нейронные сети, в 2016 году выиграла матч у одного из сильнейших игроков в истории Го.

Они окружают людей в повседневной жизни: в голосовых помощниках, таких как Алиса и Siri, в VR-масках в социальных сетях и мессенджерах, в автоматическом улучшении изображений в смартфонах.

Даже в мире бизнеса нейронные сети вышли далеко за рамки голосовых роботов, которые звонят в банк. К примеру, благодаря внедрению нейронной сети для управления системой рекомендаций в компании Amazon наблюдалось увеличение продаж на 35%. Brain ANN, разработанная для YouTube, оказалась еще более эффективной: по статистике компании, почти 70 процентов всех видео, просмотренных пользователями, были найдены на основе рекомендаций нейросети.

Помимо прочего, нейронные сети обрели фундаментальную для современного бизнеса способность: предсказывать отказ от покупки еще до того, как она произойдет, благодаря анализу огромного количества данных о поведенческих реакциях клиентов.

Нейронные сети иногда находят применение в самых неожиданных областях. Недавний и необычный пример – анализ юридических документов касаемо корректности их заполнения. Не так давно было даже проведено соревнование между нейронными сетями и американскими юристами, которое выиграла нейронная сеть. Однако нейронные сети и искусственный интеллект лучше подходят для приложений, требующих монотонного повторения одних и тех же операций, то есть для рутинной работы. В случае с видеонаблюдением, которым занимается Ivideon, огромный потенциал нейронных сетей используется для анализа видео. Просмотр многочасового видео - утомительное занятие, в котором человеческий фактор может играть решающую, даже критическую роль. Благодаря нейронным сетям данного рода проблема будет решена намного эффективнее.

Нейросеть также актуальна для сектора здравоохранения: анализ снимков МРТ и рентгеновских снимков, поиск раковых опухолей и т.д. В области косметологии модель используется для мониторинга состояния кожи, а в качестве решения нейронная сеть предлагает способы борьбы со старением кожи.

К примеру, в период заболеваемости COVID-19 была создана нейронная сеть, благодаря которой можно обнаружить коронавирус на основе звуков кашля. Стоит заметить, что результаты 98,5-процентной точности в определении людей с COVID-19, включая тех, у кого нет симптомов Данную нейронную сеть создали американские исследователи из Массачусетского технологического университета. На рисунке 6 продемонстрируем модель COVID-Net

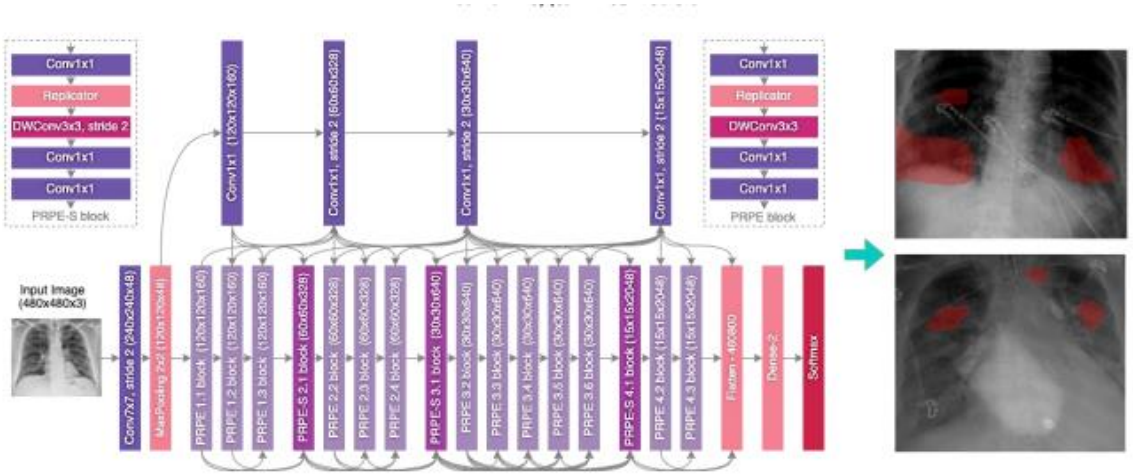
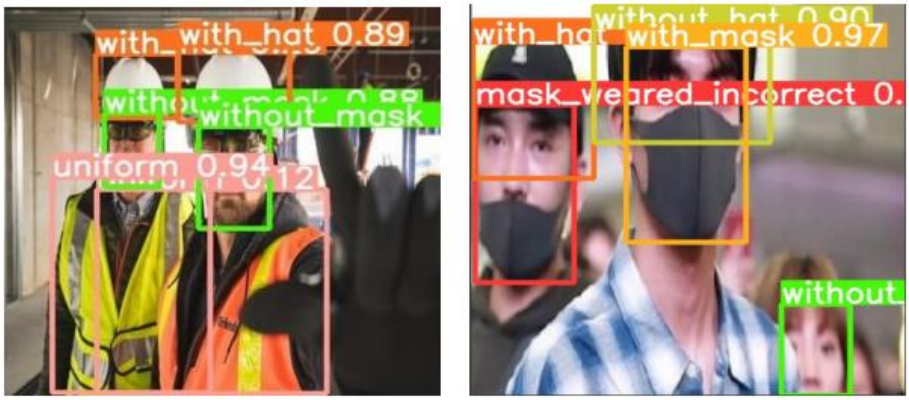


Рисунок 6 – Модель COVID-Net [5, с.245]

Также с помощью нейронной сети YOLO (You Only Look Once) возможно распознавание средств индивидуальной защиты (рисунок 7)



а *б*

Рисунок 7 – Пример распознавания объектов на изображениях [9, с.65]

Разработанная интеллектуальная система с высокой точностью распознала у людей: наличие (with_hat) и отсутствие головного убора (without_hat), наличие спец. одежды (uniform), наличие (with_mask) и отсутствие масок (without_mask), а также неправильное ношение маски (mask_weared_incorrect)

Стоит отметить, что взрывному росту сложности и количества задач, решаемых нейронными сетями, способствует тот факт, что исследователям и разработчикам сегодня доступно большое количество инструментов, позволяющих быстро создать (или использовать готовый продукт), обучить, протестировать и развернуть нейронную сеть любой сложности. Некоторые из них могут быть надстройками, которые накладываются на другие, поэтому прямое сравнение всех со всеми не очень уместно.

Таким образом, как отмечают Ю. В. Орлик, А. А. Арбузова, «благодаря широкому кругу задач, которые могут выполнять нейронные сети, и высокой эффективности выполнения этих задач, эта область искусственного интеллекта является одной из наиболее востребованных областей исследований в информационных технологиях» [7, с.693].

В процессе развития нейронные сети были разделены на множество видов, которые переплетаются в различных задачах. В настоящее время сложно классифицировать сеть на основе какой-то одной характеристики. Это можно сделать в зависимости от области применения, типа входной информации, типа обучения, типа связей и области применения.

Таблица 1 – Виды нейронных сетей, принципы и сферы применения [6]

Нейронная сеть	Принцип применения	Обучение с учителем (+) или без (-) или смешанное (с)	Сфера применения
•1. Перцептрон Розенблатта	•1.Распознание образов, принятие решений, прогнозирование, аппроксимация, анализ данных	•1.+	•1.Практически любая сфера применения, кроме оптимизации информации
•2.Хопфилда	•2.Сжатие данных и ассоциативная память	•2. -	•2.Строение компьютерных систем
•3.Кохонена	•3.Кластеризация, сжатие данных, анализ данных, оптимизация	•3.-	•3.Финансы, базы данных
•4.Радиально-базисных функций (RBF-сеть)	•4.Принятие решений и управление, аппроксимация, прогнозирование	•4.с	•4.Управленческие структуры, нейроуправление
•5.Свёрточная	•5.Распознание образов	•5.+	•5.Обработка графических данных
•6.Импульсная	•6.Принятие решение, распознавание образов, анализ данных	•6. с	•6.Протезирование, робототехника, телекоммуникации, компьютерное зрение

В 2023 году и в последующие 5-10 лет будет большой интерес к сферам метавселенных и виртуальной реальности. Снова потребуются нейронные сети, которые смогут использовать компьютерное зрение для создания 3D-персонажей, определения движения, выражения лица и т.д.

Беспилотники – одна из основных областей применения компьютерного зрения. Некоторые автопроизводители уже готовы заменить водителей. Tesla Chrysler - хороший тому пример. Успешное распознавание лиц может заменить настоящих продавцов. Amazon Go, например, сканирует содержимое тележки с покупками с помощью нейронной сети и автоматически списывает оплату, когда человек покидает магазин.

Тенденция развития и применения компьютерного зрения в строительной отрасли актуальна для 2023 года. Это связано с большим количеством смертей строителей на рабочем месте. Согласно статистике, количество смертей в строительной отрасли в пять раз выше, чем в других профессиях. Это может быть вызвано ударами, падениями, поражением электрическим током и другими причинами. Нейронные сети в данной области и методы машинного обучения позволят использовать «умные» камеры для обеспечения безопасности людей. Установив такие устройства на строительной площадке, можно будет передавать

непрерывный поток видео на отдельные серверы. Весь отснятый материал будет разделен на кадры, после чего нейронная сеть начнет его анализировать. Эта технология позволяет:

1. Быстро найти очаг возгорания.
2. Определить сотрудников, не использующих средства защиты.
3. Выявлять нарушения пропускного режима.
4. Следить за передвижением специальных транспортных средств.

На рынке уже существует несколько систем такого типа, способных идентифицировать конкретного сотрудника и предупреждать его о нарушениях или опасностях через микрофон. Этот тип инноваций позволяет застройщиков автоматизировать многие процессы, связанные с безопасностью сотрудников.

Нейронные сети способны не только создавать изображение из текста, но и анализировать содержание текста, чтобы предоставить варианты целевой аудитории, для какого возраста такая реклама будет актуальна.

СМС или изображение для рекламы с большей вероятностью будут созданы людьми на основе личного опыта и других факторов. Нейронные сети могут предсказать CTR такого сообщения для конкретного человека или группы людей. Зная потенциальный коэффициент конверсии, нейронную сеть можно обучить давать рекомендации по улучшению текста или изображения, а затем написать алгоритмы для самостоятельного составления креативов и рекламных текстов. Это облегчает создание сотен сообщений, особенно при создании индивидуальных предложений. Роботы будут использовать алгоритмы для быстрой адаптации к конкретному клиенту, что будет полезно не только в 2023 году, но и в будущем.

Сегодня аналитика Всемирного банка свидетельствует о том, что с целью поддержки растущего населения планеты, необходимо увеличение продуктов питания на 50% к 2050 году. В настоящее время мы можем наблюдать за тем, как меняется климат. Это приводит в свою очередь к тому, что снижается урожайность на открытом воздухе приблизительно на 25%. Подходящие территории для выращивания культурных растений сегодня как правило уже используются. Сегодня сложность состоит в поиске новых территорий, на которых будет возможно достичь высокого прироста урожайности.

На качество и количество урожая, увеличение поголовья скота оказывают влияние достаточно большое количество факторов. Человек, какой бы опыт у него не был, не может все факторы учесть с целью принятия верного решения. Тут в качестве альтернативы как раз и будут нейросети. Нейросети обучаемы. Они могут быть помощниками для фермеров (сбор урожая, построение различного рода прогнозов и т.д.). Стоит отметить также, что сегодня уже есть ряд успешных разработок в данной области. Что еще раз свидетельствует о важности нейросетей в сельском хозяйстве.

В Интернете постоянно появляются исследования о том, что нейронные сети в будущем заменят людей. Это действительно пугает многих людей.

Однако независимые эксперты отмечают, что это заблуждение. Да, нейронные сети называют искусственным интеллектом, но в реальном мире они, конечно, ни сегодня ни завтра не смогут заменить настоящего человека и принимать осмысленные решения. Дело в том, что любая нейронная сеть имеет очень узкую специализацию и не может быть расширена именно из-за принципа построения.

Большинство считают, что, наоборот, активное развитие нейронных сетей перевернет наш мир и создаст множество дополнительных профессиональных сфер деятельности. В ближайшем будущем они станут новым способом реализации даже самых смелых идей.

Выводы и дальнейшие перспективы исследования.

На основе всего вышеизложенного, можно сделать следующие выводы:

1. Проанализировав имеющиеся научные исследования по применению нейронных сетей в современном мире, можно сделать вывод, что нейронные сети были созданы для того, чтобы помочь людям решить как можно больше задач. Благодаря обилию доступной информации их можно научить всему. Возможности поистине огромны, и каждый день открываются новые области применения.
2. Нейронные сети – это будущее, они произведут революцию в нашем мире и создадут множество дополнительных направлений в профессиональной деятельности. Однако как справедливо отмечает С. А. Грязнов, «чрезмерная зависимость от автоматизированного принятия решений имеет также и существенные недостатки, и по мере того, как машины тестируются в реальном мире, появляется много вопросов (доверие, этика), которые еще предстоит решить» [1, с.159].

Список литературы

1. Грязнов С. А. Эволюция искусственной нейронной сети / С. А. Грязнов // Актуальные проблемы гуманитарных и естественных наук: Сборник статей VI Международной конференции профессорско-преподавательского состава, Казань, 18 марта 2022 года / Гл. редактор Е.А. Астраханцева. – Чебоксары: Общество с ограниченной ответственностью «Издательский дом «Среда», 2022. – С. 156-159
2. Дворянкин О. А. Использование нейронных сетей для розыска автомобилей на примере системы "Паутина" / О. А. Дворянкин, А. С. Абрамов // Тенденции развития науки и образования. – 2022. – № 85-7. – С. 113-116
3. Кулаченок А. К. Области применения искусственных нейронных сетей / А. К. Кулаченок, Д. А. Сапрыкин // Моя профессиональная карьера. – 2021. – Т. 2. – № 31. – С. 135-140
4. Козак Е. Нейронные сети как инструмент прогнозирования в экономике / Е. Козак // Modern Economy Success. – 2022. – № 1. – С. 168-172.
5. Катермина, Т. С. Использование нейронных сетей для определения COVID-19 / Т. С. Катермина, В. И. Туманов, С. С. Зинченко // Современное программирование : Материалы IV Международной научно-практической конференции, Нижневартовск, 08 декабря 2021 года / Под общей редакцией Т.Б. Казиахмедова . – Нижневартовск: Нижневартовский государственный университет, 2022. – С. 243-247
6. Нейросеть и Искусственный интеллект [Электронный источник]//Режим доступа: https://mif-mira.ru/akademicheskie-sredy/post/nejroset-i-iskusstvennyj-intellekt (Дата обращения: 30.10.2022)
7. Орлик Ю. В. Нейронные сети в современной жизни / Ю. В. Орлик, А. А. Арбузова // Молодые ученые - развитию Национальной технологической инициативы (ПОИСК). – 2021. – № 1. – С. 692-693
8. Ольховников А. В. Искуственные нейронные сети в области информационных технологий / А. В. Ольховников, Д. А. Сапрыкин // Моя профессиональная карьера. – 2021. – Т. 2. – № 31. – С. 153-158

9. Филичкин С. А. Применение нейронной сети YOLOv5 для распознавания наличия средств индивидуальной защиты / С. А. Филичкин, С. В. Вологдин // Интеллектуальные системы в производстве. – 2022. – Т. 20. – № 2. – С. 61-67
10. Цаунит А. Н. Перспективы развития и применения нейронных сетей / А. Н. Цаунит. – Текст: непосредственный // Молодой ученый. – 2021. – № 23 (365). – С. 114-117

References

1. Gryaznov S. A. Evolution of an artificial neural network / S. A. Gryaznov // Actual problems of the humanities and natural sciences: Collection of articles of the VI International Conference of the faculty, Kazan, March 18, 2022 / Ch. editor E.A. Astrakhantsev. - Cheboksary: Limited Liability Company "Publishing House "Sreda", 2022. - pp. 156-159
2. Dvoryankin O. A. Using neural networks to search for cars on the example of the "Web" system / O. A. Dvoryankin, A. S. Abramov // Trends in the development of science and education. - 2022. - No. 85-7. – pp. 113-116
3. Kulachenok A. K. Scope of application of artificial neural networks / A. K. Kulachenok, D. A. Saprykin // My professional career. - 2021. - V. 2. - No. 31. - pp. 135-140
4. Kozak E. Neural networks as a forecasting tool in the economy / E. Kozak // Modern Economy Success. - 2022. - No. 1. - pp. 168-172.
5. Katermina, T. S. Using neural networks to determine COVID-19 / T. S. Katermina, V. I. Tumanov, S. S. Zinchenko // Modern programming: Proceedings of the IV International Scientific and Practical Conference, Nizhnevartovsk, 08 December 2021 / Edited by T.B. Kaziakhmedov. - Nizhnevartovsk: Nizhnevartovsk State University, 2022. - pp. 243-247
6. Neural Network and Artificial Intelligence [Electronic source] // Access mode: https://mif-mira.ru/akademicheskie-sredy/post/nejroset-i-iskusstvennyj-intellekt (Date of access: 10/30/2022)
7. Orlik Yu. V. Neural networks in modern life / Yu. V. Orlik, A. A. Arbuzova // Young scientists - the development of the National Technology Initiative (POISK). - 2021. - No. 1. - pp. 692-693
8. Olkhovnikov A. V. Artificial neural networks in the field of information technology / A. V. Olkhovnikov, D. A. Saprykin // My professional career. - 2021. - V. 2. - No. 31. - pp. 153-158
9. Filichkin S. A. The use of the YOLOv5 neural network to recognize the presence of personal protective equipment / S. A. Filichkin, S. V. Vologdin // Intelligent systems in production. - 2022. - T. 20. - No. 2. - pp. 61-67
10. Tsaunit A. N. Prospects for the development and application of neural networks / A. N. Tsaunit. – Text: direct // Young scientist. - 2021. - No. 23 (365). – pp. 114-117

Шаханова М. В., Сидоров М.М, Шаханова Д.С. Проектирование системы защиты персональных данных организации // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 43–50

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.53

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНИЗАЦИИ

Шаханова М. В., Сидоров М.М., Шаханова Д.С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, д.50а), e-mail: marinavl2007@yandex.ru

В современном мире сложно найти человека совершеннолетнего возраста, персональные данные которого не хранились бы на каком-нибудь сервере на необъятных просторах всемирной паутины. Это и социальные сети, и данные заемщиков / вкладчиков в банки, и порталы государственных услуг. Персональные данные человека мошенники используют в своих корыстных неблаговидных целях. За последние годы в разы увеличились случаи компрометации баз данных с персональными данными клиентов банков, социальных учреждений и т.д. Основной способ компрометации персональных данных пользователей состоит во взломе баз данных аккаунтов или компрометации паролей пользователей. В настоящей статье изложены основные концептуальные решения проекта системы защиты аккаунтов пользователей от компрометации персональных данных.

Ключевые слова. Защита данных, персональные данные, информационная система, авторизация, пароль, управление данными, хеширование, модель, UML.

DESIGNING THE ORGANIZATION'S PERSONAL DATA PROTECTION SYSTEM

Shakhanova M. V., Sidorov M.M., Shakhanova D.S.
G.I. Nevelsky Maritime State University, Vladivostok, Russia (690003, Vladivostok, st. Verkhneportovaya, 50a), e-mail: marinavl2007@yandex.ru

In the modern world, it is difficult to find a person of legal age whose personal data would not be stored on some server on the vast expanses of the World Wide Web. These are social networks, data of borrowers /depositors to banks, and portals of public services. Fraudsters use a person's personal data for their own selfish, unseemly purposes. In recent years, the cases of compromising databases with personal data of customers of banks, social institutions, etc. have increased significantly. The main way to compromise users' personal data is to hack account databases or compromise user passwords. This article outlines the main conceptual solutions for the project of a system for protecting user accounts from compromising personal data.

Keywords: Data protection, personal data, information system, authorization, password, data management, hashing, model, UML.

Введение.

Персональные данные являются неотъемлемой частью современных информационных систем практически любой сферы (банковские, образовательные, социальные, здравоохранения, сервисы распространения и оказания услуг и торговли и т.д.). Все персональные данные охраняются Федеральным законом РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных». Данный закон регулирует отношения, связанные с обработкой персональных данных, осуществляемой, в частности, поликлиникой [3]. Целью Федерального

закона № 152-ФЗ является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В соответствии с ФЗ персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). В соответствии со ст. 5 № 152-ФЗ хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

В соответствии со ст. 6 № 152-ФЗ обработка персональных данных субъекта возможна только с его письменного согласия. При этом операторы, обрабатывающие персональные данные, обязаны не раскрывать их третьим лицам в любых случаях, не предусмотренных законом.

Анализ полного состава документа № 152-ФЗ «О персональных данных» показывает, что персональные данные пациентов поликлиники должно храниться в защищенном хранилище, недоступном третьим лицам. Хранилище должно предусматривать прямую защиту от компрометации техническими и социальными методами. Пользователи, имеющие доступ к персональным данным в хранилище, должны быть строго разграничены в доступе к тем данным, которыми они будут оперировать при выполнении своих прямых обязанностей.

Таким образом, над хранилищем персональных данных требуется служба верхнего уровня, отвечающая за делегирование полномочий доступа пользователей к персональным данным. Такой службой может быть административная оболочка базы данных в СУБД, либо клиентское приложение, которое будет организовывать работу с персональными данными. Таким образом, защита информации от угроз реализуется процедурой авторизации пользователей и ограничений их прав доступа к функциям и данным и определяется следующими правилами, которые являются частью политики информационной безопасности:

- операторские компьютеры, работающие с персональными данными, рекомендуется заблокировать паролем, известный только компетентным лицам;
- применение на операторских компьютерах антивирусного программного обеспечения;
- блокировка свободных портов коммутаторов и свитчей, входящих в состав сетевой инфраструктуры поликлиники;
- защита СУБД;
- проверка введенных пользователем данных на корректность;
- резервное создание дампа БД.

Проектирование системы защиты персональных данных организации.

Основа защиты персональных данных состоит в использовании надежной и эффективной системе хранения паролей пользователей информационных систем.

Первый аспект создания надежных паролей состоит в создании и введение в действие системы администрирования паролей пользователей. По-другому, пользователей необходимо обязать создавать наиболее защищенные пароли, которые будут в наименьшей степени поддаваться простому угадыванию и подбору. Очевидно, что пароль «123456» подобрать в разы легче, чем, например, «_0Rtk+!93=q». Для построения эффективной системы администрирования паролей должны быть предусмотрены следующие правила их формирования:

- ограничение пароля по минимальной длине;
- требование к паролю содержания символов из различных групп (буквы, заглавные и строчные, цифры, спецсимволы);
- установка максимального срока действия пароля, по истечении которого пароль необходимо заменить;
- ведение журнала истории паролей и слежение за несовпадением нового пароля с ранее использованными;
- автоматическая генерация пароля в соответствии с вышеперечисленными правилами.

Подсистема авторизации в информационной системе, также должна предусматривать средства для защиты от компрометации, попыток подбора пароля. Например:

- использование задержки (5-10 секунд) при вводе неправильного пароля;
- использование «капчи»;
- ограничение количества попыток на ввод пароля;
- блокировка пользователя после, например, трех попыток неправильного ввода пароля (распространено в банкоматах).

В соответствии с текущими задачами информационных систем, их спецификой, может быть предложена подсистема администратора (ответственного за информационную безопасность), в которой тот будет иметь инструмент гибкой настройки правил установки и использования паролей пользователей. Пример макета интерфейса такой подсистемы приведен на рисунке 1 (рисунок выполнен в редакторе визуальных форм среды разработки Microsoft Visual Studio 2015).

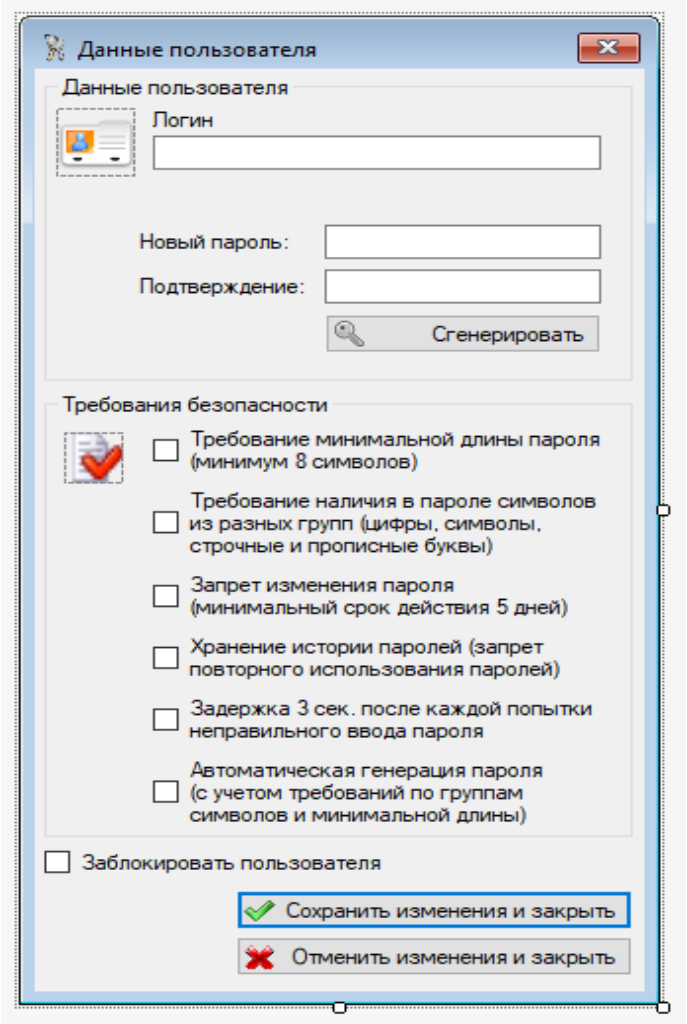


Рисунок 1 – Пример макета интерфейса подсистемы гибкой настройки правил установки и использования паролей пользователей

Атаки злоумышленников не всегда направлены на попытке подбора пароля. Нередки случаи, когда злоумышленник получает доступ к базе данных аккаунтов пользователей. В этом случае все пароли становятся доступными ему. Поэтому в современных системах давно уже не принято хранить пароли пользователей в открытом виде. Наиболее распространенный способ защиты пароля – хеширование.

Одним из ключевых требований для криптографических хеш-функций является условие, при котором при атомарном (то есть самом малом) изменении аргумента функции ее выходное значение менялось кардинально. Такое условие при его соблюдение обеспечит невозможность утечки информации по значению хеш-функции при незначительном изменении аргумента. Среди множества существующих хэш-функций принято выделять криптографически стойкие, применяемые в криптографии. Как правило, криптографическая стойкость хэш-функции обеспечивается следующими свойствами [1]:

- стойкость к коллизиям первого рода (необратимость): для заданного сообщения M должно быть практически невозможно подобрать другое сообщение M` имеющее такой же хэш. Это свойство также называется необратимостью хэш-функции;
- стойкость к коллизиям второго рода: должно быть практически невозможно подобрать пару сообщений (M, M`) с одинаковым хэшем.

Для увеличения устойчивости хешированных паролей к взлому перед хешированием к исходному паролю добавляется случайная последовательность символов, которая на сленге криптографии получила название «соль». Соль (модификатор входа хэш-функции) — строка данных, которая передаётся хеш-функции вместе со входной строкой (прообразом) для вычисления хэша (образа) [4]. Цель использования «соли» – усложнение определения прообраза хэш-функции методом перебора по словарю возможных входных значений (прообразов), включая атаки с использованием «радужных» таблиц.

При использовании одинаковых паролей «соль» сгенерирует различные хеши, что должно добавить дополнительную сложность для злоумышленников. На практике лучше применять статическую и динамическую «соль». Статическая «соль» – постоянная случайная строка, которая добавляется ко всем паролям. Динамическая «соль» генерируется индивидуально по заданному алгоритму для каждого пароля [2]. Использование динамической составляющей «соли» имеет дополнительное преимущество в случае, когда пользователь использует одинаковый пароль на нескольких ресурсах сразу, а злоумышленнику стал известен из его хешей. В этом случае использование динамической соли позволяет избежать компрометации аккаунтов пользователя на нескольких веб-сервисах сразу [5]. Для построения эффективной защиты пароля предлагается:

- использование алгоритма хеширования, например, SHA256;
- для повышения устойчивости пароля к взлому перед хешированием добавлять «соль» из трех компонентов.

Первым компонентом соли (SALT1) будет являться динамическая константа, которая будет генерироваться при каждом изменении пароля в виде десяти случайных символов. Данная константа будет записываться в базу данных в открытом виде рядом с хешем пароля. Основное назначение данной части «соли» – ввести в заблуждение злоумышленника, у которого получилось скомпрометировать базу аккаунтов пользователей: он будет ошибочно полагать, что «соль» ему известна, хотя это далеко не так.

Второю часть «соли» (SALT2), которая также будет динамической, можно формировать по следующему алгоритму:

- перевод даты создания аккаунта пользователя (должен храниться в таблице аккаунтов в БД) в строку Sdate формата «dd.mm.yyyy hh:MM» (dd – день в виде числа из двух знаков, mm – месяц в виде числа из двух знаков, yyyy – год в четырехзначном формате, hh, MM – соответственно, часы и минуты в формате двух знаков);
- получение строки Slog путем поочередной конкатенации символов (выбираются по одному), составляющих логин пользователя (хранится в таблице аккаунтов), и компонентов строки Sdate (день, месяц, год, часы, минуты); например, если логин пользователя – LOGIN, а дата создания его аккаунта – 11.04.2021 11:04, то полученная строка Slog будет иметь вид «M11Y04L2021O11G04IN»;
- шифрование полученной строки Slog методом таблиц Вижинера, причем для ключа шифрования по таблицам будет использоваться третий компонент «соли» (SALT3).

Таким образом, динамическая часть «соли» будет иметь достаточно сложный алгоритм формирования и, соответственно, хорошую защищенность от компрометации. Последний компонент «соли» (SALT3) будет являться системной константой (12 символов), которая будет храниться не в базе данных, а локально (например, в конфигурационном файле системы). Итоговая «соль» будет являться конкатенацией всех трех компонентов. Таким

образом, перед хешированием в конец пароля будет подмешиваться «соль» общей длиной не менее 42 символов, которая будет формироваться по сложному алгоритму и будет более, чем надежной. Полученный пароль перед помещением в базу данных будет хешироваться методом SHA256. На рисунке 2 показана схема создания хеша пароля перед помещением его в таблицу аккаунтов базы данных.

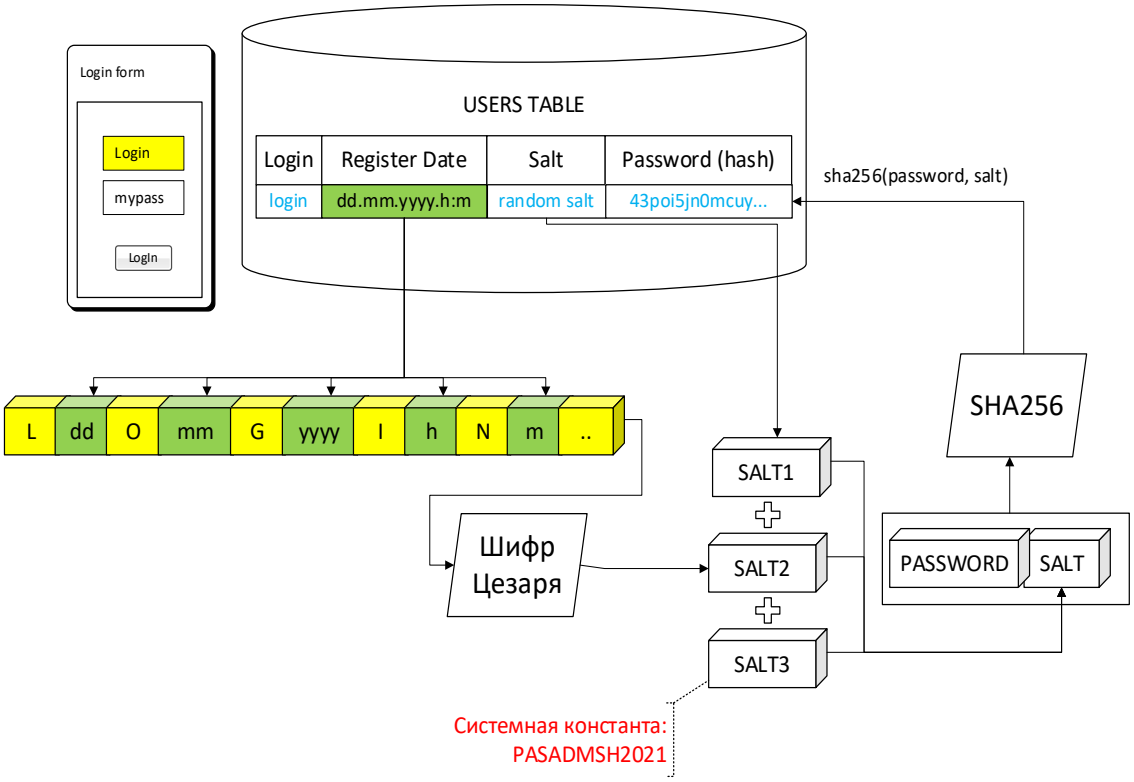


Рисунок 2 – Схема хеширования пароля

Таким образом, описанная концептуальная схема защиты паролей пользователей будет обеспечивать дополнительную надежность и высокую устойчивость к компрометации персональных данных злоумышленниками. На Рисунке 3 приведена UML-диаграмма активности, в соответствии с которой можно реализовывать прецедент авторизации пользователя в информационной системе.

Заключение.

Таким образом, предложенный проект системы защиты персональных данных пользователей способен защитить от:

- методов подбора пароля как ручным способом, так и с использованием специализированных программ;
- получения авторизационных данных пользователей при успешной компрометации базы аккаунтов.

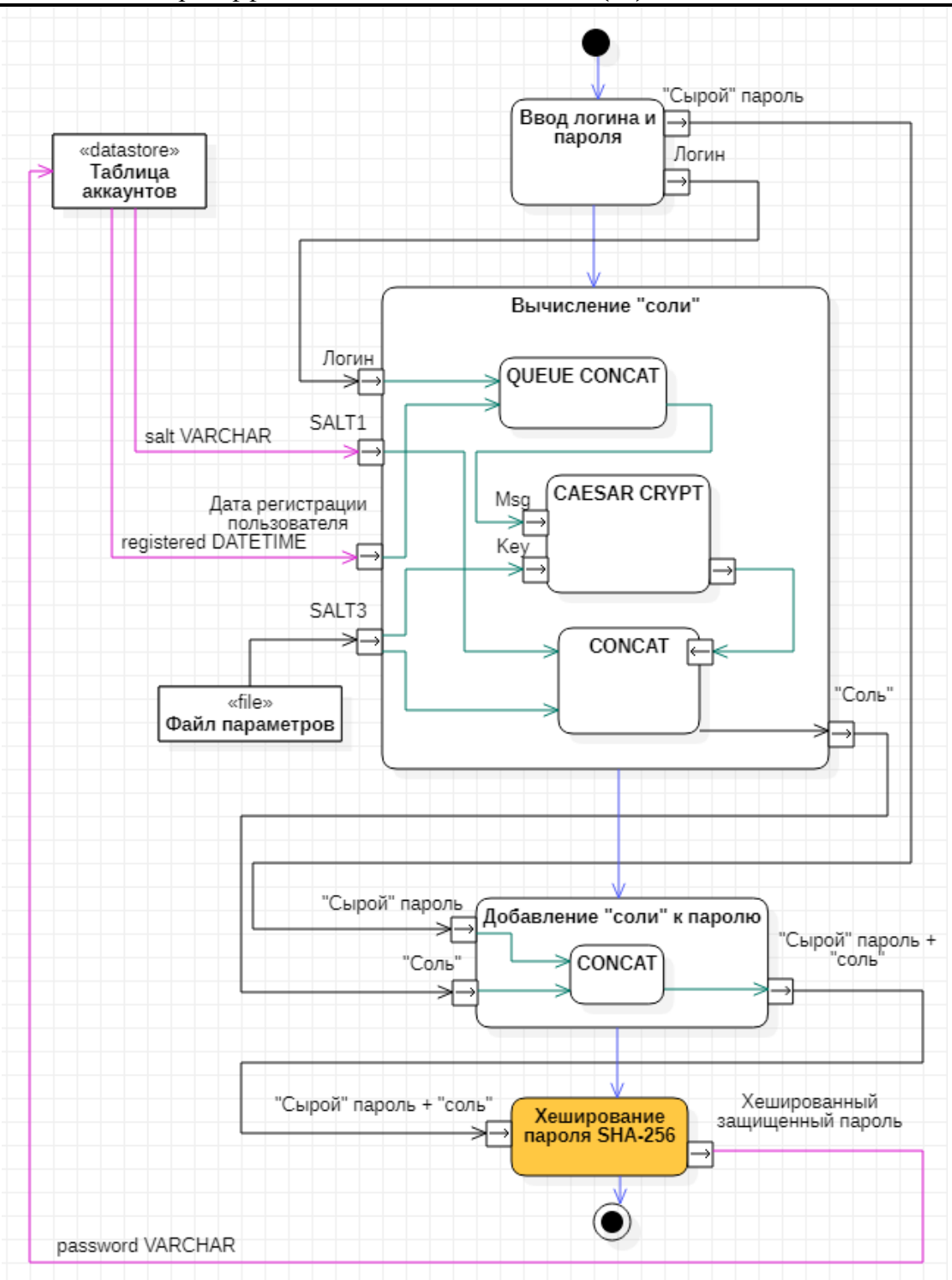


Рисунок 3 – Диаграмма активности прецедента авторизации пользователя в информационной системе

Список литературы

1. ГОСТ Р 34.11-94. Информационная технология (ИТ). Криптографическая защита информации. Функция хеширования / М.: Издательство стандартов, 1994
2. Интернет-технологии.ру. «Солёное» хеширование паролей: делаем правильно [Электронный ресурс] URL: https://www.internet-technologies.ru/articles/solenoe-

heshirovanie-paroley-delaem-pravilno.html (дата обращения: 01.10.2022 г.)
3. Российская Федерация. Законы. О персональных данных. Федеральный закон от 27.07.2006 N 152-ФЗ [принят Государственной Думой 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г.]
4. Ященко, В.В. Введение в криптографию / изд. 4-е доп. – М.: МЦНМО, 2012. – 341 с.
5. Club.CNews.ru. 52% пользователей используют одинаковые пароли на разных сайтах [Электронный ресурс] URL: https://club.cnews.ru/ blogs/entry/52_polzovatelej_ispolzuyut_odinakovye_paroli_na_raznyh_sajtah (дата обращения: 01.10.2022 г.)

References

1. . GOST R 34.11-94. Information technology (IT). Cryptographic protection of information. Hash function / M.: Publishing house of standards, 1994
2. Internet technologies.ru. "Salted" password hashing: doing it right [Electronic resource] URL: https://www.internet-technologies.ru/articles/solenoe-heshirovanie-paroley-delaem-pravilno.html
3. Russian Federation. Laws. About personal data. Federal Law No. 152-FZ of July 27, 2006 [adopted by the State Duma on July 8, 2006: approved by the Federation Council on July 14, 2006]
4. Yashchenko, V.V. Introduction to cryptography / ed. 4th add. – M.: MTsNMO, 2012. – 341 p.
5. Club.CNews.ru. 52% of users use the same passwords on different sites. Club.CNews.ru. 52% of users use the same passwords on different sites [Electronic resource] URL: https://club.cnews.ru/ blogs/entry/52_polzovatelej_ispolzuyut_ odinakovye_paroli_na_raznyh_sajtah (date of access: 01.10.2022)

Интеллектуальные технологии управления и автоматики в энергосистеме / Балаев П.А. [и др.] // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 51-58

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.896

ИНТЕЛЛЕКТУАЛЬНЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ И АВТОМАТИКИ В ЭНЕРГОСИСТЕМЕ

[1] Балаев П. А., [2] Сивеев Т. М., [3] Груздов А. Г., [4] Пашковская Е. Е.
Национальный исследовательский университет «МЭИ», Москва, Россия (111250, г. Москва, ул. Красноказарменная, 17, стр. 3), e-mail: [1]mr.balaev2002@gmail.com, [2]tichonsiveev@gmail.com, [3] GruzdovAG@mpei.ru, [4] PashkovskyaYY@mpei.ru

В данной статье рассматривается функционал современных технологий автоматического управления энергосистемой, имеющей в своём составе электростанции на основе возобновляемых источников энергии. Приводится оценка эффективности упомянутых технологий и выгоды от внедрения интеллектуальных систем в России и странах ЕС.

Ключевые слова: Интеллектуальные технологии, Smart Grid, Micro Grid, АИИС КУЭ

INTELLIGENT TECHNOLOGIES OF CONTROL AND AUTOMATION IN THE POWER SYSTEM

[1] Balaev P. A., [2] Siveev T. M, [3] Gruzdov A. G., [4] Pashkovskaya E. E.
National Research University "MPEI", Moscow, Russia (111250, Moscow, Krasnokazarmennaya st., 17, building 3), e-mail: e-mail: [1]mr.balaev2002@gmail.com, [2]tichonsiveev@gmail.com, [3] GruzdovAG@mpei.ru, [4] PashkovskyaYY@mpei.ru

This article discusses the functionality of modern technologies for automatic control of the power system, which incorporates power plants based on renewable energy sources. An assessment of the effectiveness of the mentioned technologies and the benefits from the introduction of intelligent systems in Russia and the EU countries is given.

Keywords: Intelligent technologies Smart Grid, Micro Grid, Automated information and measuring system for commercial accounting of electricity.

В наши дни нет ни одной другой отрасли экономики со столь широким спектром взаимосвязей, как электроэнергетика. Расходы на питающую все жизненно необходимые объекты электроэнергию составляют колоссальную долю различного вида ресурсов. Основой развития экономики всех стран мира становится эффективное функционирование электроэнергетики и бесперебойное снабжение потребителей.

В этой статье рассмотрим технологии, способствующие достижению оптимального ресурсоиспользования, выясним, какие страны лидируют по числу планов развития «зеленой энергетики», перечислим позитивные последствия внедрения современных технологий в энергетическую сферу.

В России об интеллектуальных технологиях управления и автоматики в энергосистеме особенно серьёзно начали задумываться после июня 2009 года, когда президентом РФ были

определены пять приоритетных направлений модернизации российской экономики, в числе которых было развитие энергетики [1].

Интеллектуальная энергосистема – система, автоматически выполняющая функции распределения и отслеживания потоков электрической энергии, что позволяет максимально эффективно использовать выработанную энергию. Данная энергосистема способна решить перечень следующих задач [2]:

- необходимость использования возобновляемых источников энергии при производстве электрической энергии;
- увеличение эффективности, надёжности и безопасности электроэнергетической системы;
- оперативное реагирование на изменение рабочего режима сети;
- уменьшение затрат на производство, хранение и передачу электрической энергии.

Определим, какие компоненты включает в себя интеллектуальная энергосистема, на базе каких технологий реализуется автоматическое управление энергетической сетью страны.

Интеллектуальная энергосистема состоит из генерирующего, распределительного, передающего, трансформирующего и потребляющего энергию оборудования. А также в технологический состав системы входят новейшие коммуникационные и информационные технологии, взаимодействующие друг с другом.

Использование информационно-коммуникационных технологий позволяет собирать информацию с оборудования, оперативно анализировать её, полученные результаты применять для оптимизации использования электроэнергии, вследствие чего наблюдается снижение затрат, увеличение эффективности, надёжности и безопасности энергосистемы.

В наши дни существуют несколько технологий, реализующих работу интеллектуальной электроэнергетической системы:

- Smart Grid;
- Micro Grid;
- АИИС КУЭ, АИИС ТУЭ;

Более подробно рассмотрим указанные выше технологии, выясним какие преимущества даёт использование той или иной технологии, какие smart системы активно используются в странах ЕС.

Энергетическая сеть России охватывает практически всю обжитую территорию страны и является крупнейшим в мире централизованно управляемым энергообъединением. Сбой работы подобного масштабного энергетического объекта способен привести к необратимым последствиям не только для экономики страны, но даже для её суверенитета.

Рисунок 1 – Структура сети Smart Grid

Среди преимуществ интеллектуальной технологии Smart Grid (рисунок 1) числится способность к самовосстановлению после сбоев в подаче электроэнергии, что крайне благоприятно для сильно разветвленной энергосистемы. Данная технология входит в состав модернизированных сетей электроснабжения и использует информационные и коммуникационные сети для сбора информации об энергопроизводстве и энергопотреблении [3].

Среди прочих преимуществ Smart Grid значатся:

- устойчивость сети к вмешательству как физическому, так и программному;
- обеспечение требуемого качества передаваемой электроэнергии;
- обеспечение синхронной работы источников генерации и узлов хранения электроэнергии.

Несомненно, Smart Grid – совокупность интеллектуальных технологий, совместное использование которых направлено на достижение оптимального использования ресурсов. Например, внедрение умных счётчиков с функцией дистанционного управления позволит удаленно и оперативно отслеживать динамику изменения нагрузки, а внедрение автоматизированных систем управления производственной деятельностью в энергокомпаниях, обладающих функциями управления техническим обслуживанием и ремонтом, не только снизят энергозатраты, но и повысят безопасность персонала.

С помощью технологии Smart Grid потребитель способен не только управлять потреблением электрической энергии, но и генерацией, благодаря возможности использования маневренных электростанций на основе ВИЭ.

В наши дни Голландия находится на первом месте по числу планов развития «зеленой энергетики» и активно осуществляет энергоэффективные проекты. Один из проектов – Amsterdam Smart City. Он подразумевает внедрение интеллектуальной сети, которая охватит несколько секторов. В основе проектов сектора «Жильё» находится внедрение технологий энергосбережения: тысячи домов должны быть оборудованы системами управления

энергопотреблением. Пользователи в режиме реального времени будут получать от счетчиков данные о потреблении газа и электрической энергии. Направление «Работа» реализует концепцию «умных» зданий с помощью сенсорных датчиков, регистрирующих расход энергии и обеспечивающих оптимальную работу систем отопления, охлаждения, безопасности и освещения. Проекты направления «Транспорт» направлены на переход к использованию экологичных видов транспорта [4].

Некоторые страны ЕС, реализовавшие подобного рода проекты, уже наблюдают за благоприятными последствиями. Наибольшие совокупные выгоды от реализации проектов в сфере смарт-учета природного газа прогнозируются в Австрии (1400 млн Евро) и Испании (1050 млн Евро).

В таблице 1 представлена оценка внедрения smart систем в странах ЕС.

Таблица 1 – Оценка внедрения smart систем в странах ЕС.

Страна	**Совокупные инвестиции, млн. евро**	**Совокупные выгоды, млн. евро**	**Затраты на оснащение 1 точки учёта, евро**	**Выгоды от оснащения 1 точки учёта, евро**
Австрия	3195	3539	590	654
Чехия	4367	2735	766	499
Дания	310	322	225	233
Германия	14466	16968	546	493
Греция	1733	2443	309	436
Ирландия	1040	1212	473	551
Италия	3400	6400	94	176
Литва	254	128	123	82
Нидерланды	3340	4108	220	270
Польша	2200	2330	167	177
Португалия	640	1316	99	202
Румыния	712	552	99	77
Швеция	1500	1677	288	323

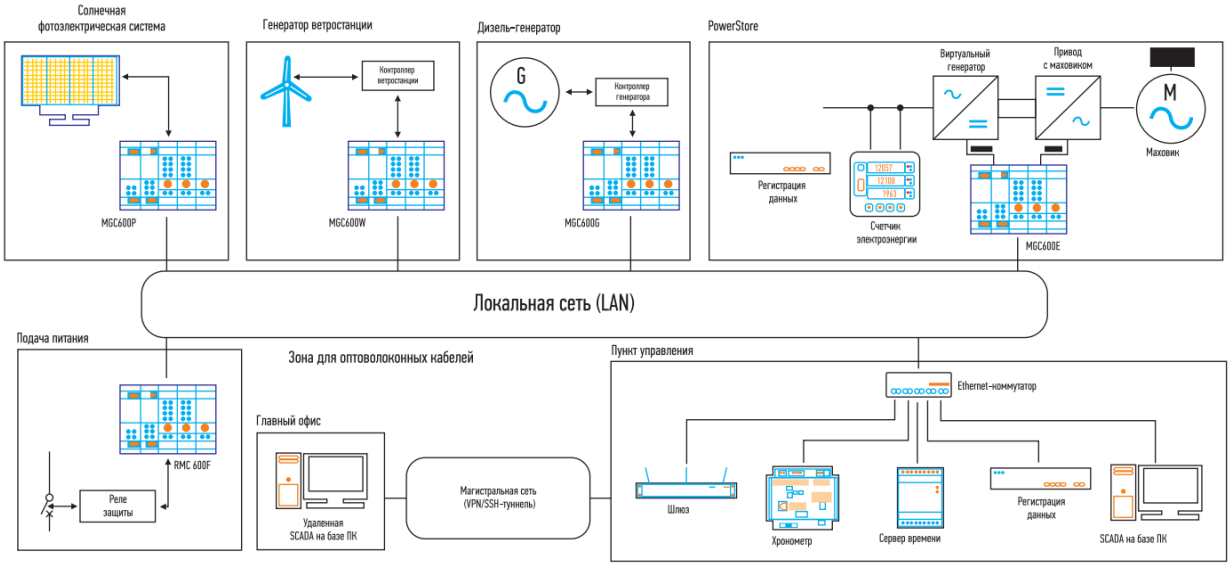


Рисунок 2 – Структура Micro Grid

Следующая интеллектуальная технология – Micro Grid (рисунок 2). В случае отключения от центральной сети оборудование, оснащенное данной технологией, способно задействовать внутренние генерирующие устройства. Micro Grid обладает в том числе следующим функционалом [5]:

- работа как при подключении к общей центральной сети, так и стационарно;
- способность успешно использовать возобновляемые источники энергии;
- повышение эффективности и надёжности энергосистемы в целом.

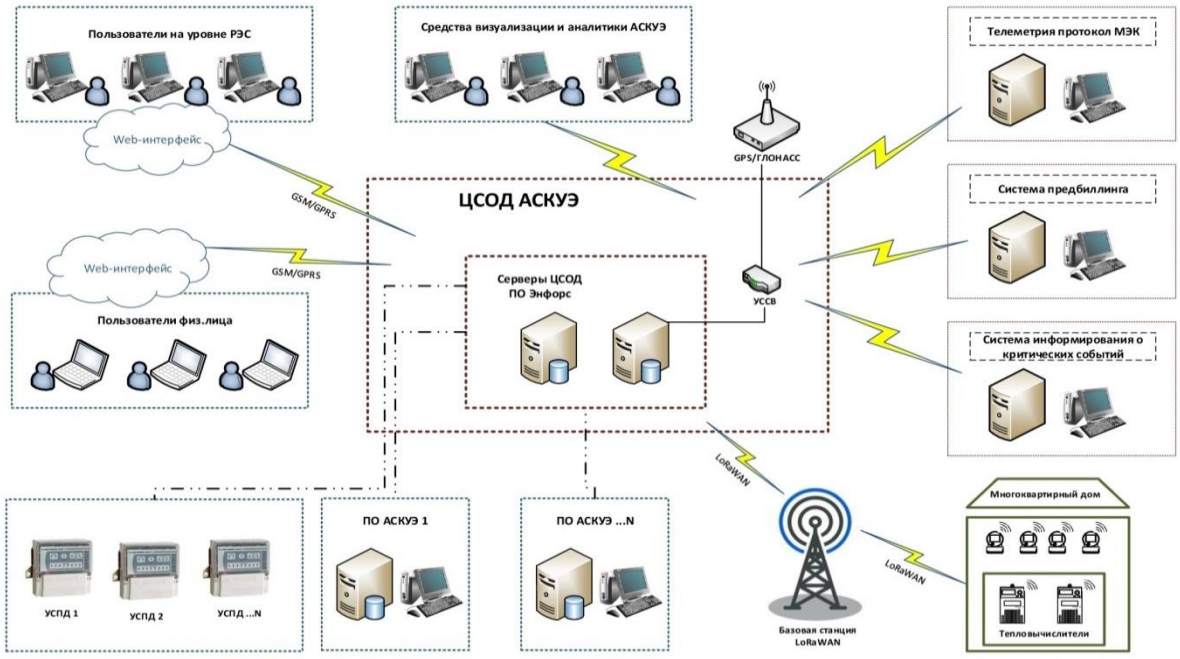


Рисунок 3 – Структура АИИС КУЭ

Последняя интеллектуальная технология, которую мы рассмотрим уже нашла широкое применение в мире. Автоматизированная информационно-измерительная система

коммерческого учёта электроэнергии (АИИС КУЭ, рисунок 3) предназначена непосредственно для осуществления коммерческих расчётов с поставщиками или с потребителями [6].

Автоматизация передачи коммерческой информации в контролирующие организации с обеспечением сохранности информации при стороннем вмешательстве – полезная функция, которая значительно экономит время и средства организаций. Помимо упомянутых функций АИИС способна контролировать потребляемую мощность, отслеживать несанкционированный доступ к энергосистеме и восстанавливать питание устройств системы.

На данном этапе стоит привести несколько конкретных примеров исследований и применений упомянутых интеллектуальных систем. Одной из важнейших составляющих любой технологии является среда моделирования, поэтому рассмотрим исследование Валерия Камаева и его команды [7].

С помощью программного обеспечения PVSOL, моделирующего систему с учетом погодных условий, представители Волгоградского государственного технического университета запрограммировали и протестировали интеллектуальную гибридную систему с ВИЭ. В результате моделирования были выявлены оптимальная конфигурация гибридной энергосистемы и оптимальная стратегия покупки электроэнергии.

Успех упомянутого исследования означает, что и другие программные обеспечения моделирования электроэнергетических систем и релейной защиты, и автоматики могут быть использованы для анализа работы и управления современных систем.

Исследование потока мощности или исследование потока нагрузки является важным методом анализа и проектирования энергосистемы. Именно для этих целей создаются и тестируются программы моделирования.

Далее рассмотрим результаты, полученные при непосредственном применении интеллектуальных технологий на Российских энергетических объектах. Принципы работы интеллектуальной активно-адаптивной сети Smart Grid в своих работах подробно рассматривают представители Иркутского национального исследовательского технического университета [8].

Упомянутая сеть использует современные информационно-коммуникационные технологии, увеличивающие эффективность. После внедрения интеллектуальных сетей в городе Уфа был выявлен ряд позитивных изменений в работе энергетической сети:

- сокращение времени ликвидации аварийных ситуаций с 2,5 ч до 2 мин;
- обнаружение несанкционированных подключений;
- снижение затрат на обслуживание и ремонт оборудования.

Но вместе с позитивными изменениями были замечены факторы, которые препятствуют широкомасштабному использованию интеллектуальной сети Smart Grid:

- широкий спектр требований потребителей к качеству электрической энергии;
- отсутствие надежных накопителей энергии;
- отсутствие мотивации у генерирующих компаний.

Дополнением к упомянутым в статье интеллектуальным технологиям могут служить виртуальные электростанции, основной целью создания которых является интеграция децентрализованных генерирующих мощностей в централизованную электрическую сеть и виртуальное дублирование всей энергосистемы.

Подводя итог, необходимо ещё раз отметить высокую точность и быстродейственность интеллектуальных систем, оснащенных современной автоматикой. Прогнозирование энергопотребления осуществляется благодаря адаптивным компьютерным моделям, работающим с данными, получаемыми от компонентов smart сети. А управление генерацией и потреблением энергии может быть осуществлено посредством использования датчиков на всех этапах энергетического производства.

Наличие более маневренных электростанций на основе ВИЭ, позволяет оптимально распоряжаться ресурсами. Временные сложности в повсеместном введении smart технологий связаны в большей мере с экономическим положением, которое не позволяет дополнить систему недостающими компонентами, например, энергетическими накопителями, скорректировать трудовые соглашения между предприятиями и работниками.

Список литературы

1. Илларионова, А. В. Интеллектуальные энергетические сети как одно из направлений инновационного развития российской экономики / А. В. Илларионова. — Текст: непосредственный // Молодой ученый. — 2010. — № 9 (20). — С. 122-127. — URL: https://moluch.ru/archive/20/2063/
2. Михеев Е.А., Н.Г. Семенова ИНТЕЛЛЕКТУАЛЬНАЯ ЭНЕРГОСИСТЕМА // Международный студенческий научный вестник. – 2015.–№3-1.; URL: http://www.eduherald.ru/ru/article/view?id=12027
3. U.S. Department of Energy. URL: https://www.energy.gov/science-innovation/electric-power/smart-grid
4. Jeremy Rifkin. Leading the Way to the Third Industrial Revolution and a New Distributed Social Vision for the World in the 21st Century, November 2009, Paris. Retrieved from http://www.foet.org//
5. MicroGrid – будущее электросетей. Кейсы, перспективы, возможности // Smart Energy. – 2018.; URL: http://smartenergysummit.ru/novosti/microgrid-%E2%80%93-budushhee-elektrosetej.-kejsyi,-perspektivyi,-vozmozhnosti
6. АСКУЭ – системы автоматизированного коммерческого учёта электроэнергии // АйСиБиКом. – 2015.; URL: https://icbcom.ru/ru/askueaiis-kue
7. Май Н.Т., Ха В.М., Камаев В.А., Щербаков М.В. Моделирование и оптимизация управления интеллектуальной гибридной энергосистемой с источниками возобновляемой энергии // Управление большими системами. – 2013. – №46. – С. 293 – 309.
8. Гаврилова А.А., Кузнецова С.Ю. Повышение энергоэффективности в России: внедрение интеллектуальной сети электроснабжения smart grid // Иркутский национальный исследовательский технический университет. – 2018. – С. 118-121.

References

1. Illarionova, A. V. Intelligent energy networks as one of the directions of innovative development of the Russian economy / A. V. Illarionova. — Text: direct // Young scientist. - 2010. - No. 9 (20). — pp. 122-127. — URL: https://moluch.ru/archive/20/2063/
2. Mikheev E.A., N.G. Semenova INTELLIGENT ENERGY SYSTEM // International Student Scientific Bulletin. – 2015.–№3-1.; URL: http://www.eduherald.ru/ru/article/view?id=12027

3. U.S. Department of Energy. URL: https://www.energy.gov/science-innovation/electric-power/smart-grid
4. Jeremy Rifkin Leading the Way to the Third Industrial Revolution and a New Distributed Social Vision for the World in the 21st Century, November 2009, Paris. Retrieved from http://www.foet.org//
5. MicroGrid is the future of power grids. Cases, prospects, opportunities // Smart Energy. – 2018.; URL: http://smartenergysummit.ru/novosti/microgrid-%E2%80%93-budushhee-elektrosetej.-kejsyi,-perspektivyi,-vozmozhnosti
6. ASKUE - systems for automated commercial accounting of electricity // ICSiBiCom. – 2015.; URL: https://icbcom.ru/ru/askueaiis-kue
7. Mai N.T., Kha V.M., Kamaev V.A., Shcherbakov M.V. Modeling and optimization of the management of an intelligent hybrid energy system with renewable energy sources // Management of large systems. - 2013. - No. 46. - pp. 293 - 309.
8. Gavrilova A.A., Kuznetsova S.Yu. Improving Energy Efficiency in Russia: Implementation of Smart Grid Power Supply // Irkutsk National Research Technical University. - 2018. - pp. 118-121.

Шаханова М. В., Лутов Е. В., Шаханова Э. С. Выявление событий информационной безопасности с помощью индикаторов компрометации // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 59–64

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

ВЫЯВЛЕНИЕ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ

Шаханова М. В., Лутов Е. В., Шаханова Э. С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, д.50а), e-mail: marinavl2007@yandex.ru

Настоящая статья посвящена вопросам, раскрывающим роль индикаторов компрометации, позволяющих предупреждать события информационной безопасности, повысить надежность и информационную безопасность информационной системы предприятия. В статье также рассказывается о необходимости интеграции имеющихся индикаторов в существующие системы слежения и управления информационной безопасностью.

Ключевые слова. Индикатор компрометации, инцидент информационной безопасности, система менеджмента инцидентами информационной безопасности, интеграция, защита данных.

IDENTIFICATION OF INFORMATION SECURITY EVENTS USING INDICATORS OF COMPROMISE

Shakhanova M. V., Lutov E. V., Shakhanova E.S.
G.I. Nevelsky Maritime State University, Vladivostok, Russia (690003, Vladivostok, st. Verkhneportovaya, 50a), e-mail: marinavl2007@yandex.ru

This article is devoted to issues that reveal the role of indicators of compromise, allowing to prevent information security events, improve the reliability and information security of an enterprise information system. The article also talks about the need to integrate existing indicators into existing tracking and information security management systems.

Keywords: Indicator of compromise, information security incident, information security incident management system, integration, data protection

Вмешательство человека в информационное пространство предприятий может оказать существенное влияние на структуру информационной безопасности, вызвать нежелательные события и инциденты. Вмешательство человека может быть случайным и преднамеренным. В последнем случае, как правило, преследуются корыстные интересы, наносится большой вред организации. По данным исследовательского отчета института Ponemon, подсчитанный примерный ущерб от атак на информационные системы розничных магазинов за период только с 2019 по 2020 гг. вырос с 8 млн. $ и превысил значение в 12 млн. $ на каждое большое предприятие. Среди финансовых организаций средний ущерб превышал двадцать млн. $, в технологическом секторе – свыше четырнадцати млн. $, в среднем на одно предприятие [5].

Важно контролировать все попытки вмешательства и структуру информационной системы предприятия, иметь для этого соответствующие средства, которые бы регистрировали все события (инциденты) информационной безопасности, предоставляли бы удобные средства консолидации данных для анализа уязвимостей информационной системы предприятия. Такие средства позволят предупреждать события информационной безопасности, повысить надежности и информационную безопасность технологического сегмента предприятия.

Информация в окружающем мире представляет сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [1]. Для того, чтобы информация, которой оперируют сотрудники в процессе своей деятельности, была пригодной, она должна обладать следующими качествами [2]:

- объективность и субъективность;
- полнота – содержать необходимое и достаточное количество фактов для принятия решения;
- достоверность – соответствовать объективной модели реальности в текущем контексте;
- адекватность – объективная оценка достоверности информации в соответствии с принятым контекстом;
- доступность информации – уровень защиты источников и доступа к информации;
- актуальность – показатели таких характеристик, как достоверность и адекватность относительно настоящего момента времени;
- репрезентативность – уровень отбора свойств информации для представления и описания интересующего объекта / явления / процесса;
- содержательность – отношение количества семантической информации в сообщении к объему обрабатываемых данных;
- точность – характеристика меры схожесть информации с описанием реального объекта / явления / процесса;
- устойчивость – показатель модифицируемости выходных данных в качестве отклика на изменение входных данных;
- преобразуемость – показатель вариативности представления информации в зависимости от контекста.

Важно иметь подробную классификацию угроз ИБ, чтобы в каждом конкретном случае возникающую угрозу можно было соотнести с известным классом и оценить возможное влияние последствий в соответствии с базовыми параметрами, описанными в классе (наработанными в результате опыта). Анализ массива данных по угрозам ИБ по классам позволит систематизировать основные характеристики угроз ИБ и тем самым может способствовать разработке превентивных мер, мер по устранению последствий и т.д.

Так, на Рисунке 1 приведены наиболее опасные угрозы ИБ по данным опроса, проведенного в рамках исследования «Путь к киберустойчивости: прогноз, сопротивление, ответная реакция» [5].

Рисунок 1 – Наиболее опасные угрозы ИБ [5, 2021 г.]

Почти в каждом случае инцидент информационной безопасности не приходит одномоментно. Почти всегда этому предшествуют сопутствующие действия, связанные с выявлением уязвимостей, хищением секретных ключей и т.д. Это, например, шпионаж, социальная инженерия, внедрение троянских программ в инфраструктуру и т.д. Множество таких подготовительных действий злоумышленников можно попытаться распознать на ранних этапах попыток компрометации системы информационной безопасности. Для этого главную роль играют специальные индикаторы компрометации.

Индикаторы компрометации в своем многообразии представляют собой различные методы и средства:

- организационные;
- программно-технические;
- технологические.

Организационные меры обеспечивают документальную и методическую поддержку функционирования индикаторов компрометации. К ним относятся документация на комплексы (например, руководство пользователя), политика информационной безопасности, должностная инструкция службы безопасности. В этих документах должны быть четко прописаны характеристики индикаторов, правила работы с ними, комплекс мероприятий, проводимых для предупреждения, выявления, реакции и последующего устранения угроз информационной безопасности. Таким образом, организационное обеспечение индикаторов компрометации устанавливает правила их использования, а, часто еще устанавливает формы отчетности и протоколы ведения журнала регистрации событий.

Программно-технические средства индикаторов компрометации являются основными рабочими схемами в системе обеспечения информационной безопасности. Так, в их состав входят:

- аппаратные брандмауэры и сетевые экраны, в «прошивку» которых входят функции обнаружения подозрительных абонентов;
- сетевая коммутационная аппаратура с интеллектуальными алгоритмами распознавания попыток вторжения, например, через заблокированные порты;
- системы контроля и управления доступом (СКУД), сигнализирующие о попытках несанкционированного доступа;
- специальное программное обеспечение, отслеживающее подозрительные файлы на компьютерах (например, антивирусы);
- специальное программное обеспечение, контролирующее содержимое трафика сети и сигнализирующее о попытках передачи подозрительных данных и / или попытках высоко загрузить сеть (сервер);
- протоколы, действующие в сети, позволяющие идентифицировать и аутентифицировать цифровые подписи, содержимое электронных писем, электронных сертификатов.

Все эти средства должны работать в комплексе и быть объединены общей базой данных, в которую будут записываться все события, регистрируемые индикаторами.

Назначение индикаторов компрометации системы информационной безопасности состоит в регистрации всех подозрительных событий и попыток несанкционированного вторжения в информационную инфраструктуру. При этом для наиболее эффективного практического применения индикаторов необходимо иметь специальную систему, работающую над всеми индикаторами. Такую систему часто называют системой менеджмента инцидентов информационной безопасности [3]. В рамках такой системы необходима реализация следующих функций:

- ведение базы знаний (справочника) типов инцидентов, их приоритета, оценок критичности, признаков, оценок последствий и т.д.;
- автоматическая классификация всех регистрируемых индикаторами событий в соответствии с группами, выделенными в базе знаний;
- построение аналитических отчетов в виде таблиц, графиков и диаграмм, наглядно показывающих состояние мониторинга безопасности информационных систем предприятия; при этом необходима возможность анализа всех зарегистрированных инцидентов с помощью агрегирующих функций (например, группировка по узлам системы, типам событий, адресам / источникам и т.д.).

Правильное применение системы управления инцидентов информационной безопасности, зарегистрированных индикаторами, позволит прогнозировать, предотвращать и снижать риск повторных компрометаций, найти слабые и уязвимые места в системе ИБ. При этом система управления инцидентов информационной безопасности должна основываться на следующих прецедентах [4]:

- идентификация (система управления);
- сигнализация (индикаторы);
- регистрация (индикаторы);

- выявление причин, оценка влияния, устранение последствий, внесение изменений для устранения причин (анализ и решения);
- разработка превентивных мер (анализ и решения);
- расследование (анализ и решения);
- анализ данных и принятие управленческих решений (анализ и решения).

На Рисунке 2 приведена схема жизненного цикла события компрометации (инцидента), зарегистрированного индикатором, приведенная в руководстве по реагированию от лаборатории Касперского [6].

Рисунок 2 – Этапы управления инцидентом информационной безопасности

Выполнение приведенных на рисунке этапов управления инцидентами информационной безопасности подразумевает интеграцию индикаторов компрометации в систему управления инцидентами, базу знаний, базу данных, специального пакета программного обеспечения, форм ввода данных и форм итоговых документов. Поэтому можно сформировать следующие требования к системе, в которой должны функционировать индикаторы компрометации системы ИБ:

- наличие контролирующей службы ИТ-подразделения, выполняющей слежение за соблюдение политики ИБ на предприятии;
- интеграция специального модуля регистрации инцидентов ИБ;
- ведение базы знаний по видам, типам, характеристикам, признакам и превентивным мерам инцидентов;
- интеграция с экспертной системой, которая будет идентифицировать инциденты и предлагать варианты решения из базы знаний;
- стандартизация индикаторов (как минимум, стандартизация протоколов, по которым будут записываться в хранилище данных зарегистрированные события);
- разработка организационного обеспечения, включающего документы по использованию базы знаний, экспертной системы и индикаторов;
- обеспечение безопасности сетевой инфраструктуры;
- внедрение прикладного программного обеспечения системы менеджмента инцидентов информационной безопасности, интегрированного с экспертной системой, базой знаний и индикаторами.

Список литературы

1. ГОСТ Р 56546-2015. Уязвимости информационных систем п. 3.1
2. ГОСТ Р 56546-2015. Уязвимости информационных систем п. 3.5
3. ГОСТ Р ИСО/МЭК 18044 – 2007. Менеджмент инцидентов информационной безопасности
4. ГОСТ Р ИСО/МЭК 27001 – 2006. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности, ст. 3.6
5. Международное исследование EY в области информационной безопасности «Путь к киберустойчивости: прогноз, сопротивление, ответная реакция» // 2021 г.
6. Руководство по реагированию на инциденты информационной безопасности // Управление технологических решений // АО Kaspersky Lab., – Версия 1.0 (07.03.2022)

References

1. GOST R 56546-2015. Vulnerabilities of information systems p. 3.1
2. GOST R 56546-2015. Vulnerabilities of information systems p. 3.5
3. GOST R ISO / IEC 18044 - 2007. Management of information security incidents
4. GOST R ISO / IEC 27001 - 2006. Information technology (IT). Methods and means of ensuring security. Information security management systems, art. 3.6
5. EY international study in the field of information security "The path to cyber resilience: forecast, resistance, response" // 2021
6. Guidelines for responding to information security incidents // Management of technological solutions // AO Kaspersky Lab., - Version 1.0 (03/07/2022)

Ли Ц., Лю Л., Уласы Б. Анализ и исследование безопасности контейнеров docker // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 65–72

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

АНАЛИЗ И ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ DOCKER

[1] Ли Ц., [2] Лю Л., [3] Уласы Б.
Университет ИТМО, Санкт-Петербург, Россия (197101, г. Санкт-Петербург, Кронверкский пр., 49), e-mail: [1] magiclij@outlook.com, [2] magiclil@outlook.com, [3]magicula@outlook.com

В качестве ключевой технологии облачных вычислений контейнер Docker используется благодаря своим характеристикам упрощения конфигурации, повышения эффективности разработки, изоляции приложений, интеграции серверов, многопользовательской среды и быстрого развертывания. Исследованы проблемы безопасности контейнерной виртуализации, безопасности образа контейнера, безопасности контейнерной сети и стабильной работы контейнерных сервисов, с которыми сталкиваются Docker-контейнеры в процессе эксплуатации, и даны решения для вышеуказанных рисков.

Ключевые слова: Docker; образ; безопасность; риск.

ANALYSIS AND RESEARCH ON DOCKER

[1] Li J., [2] Liu L., [3] Ulas B.
ITMO University, St. Petersburg, Russia (197101, St. Petersburg, Kronverksky pr., 49), e-mail: [1] magiclij@outlook.com, [2] magiclil@outlook.com, [3]magicula@outlook.com

As a key cloud computing technology, Docker containers are used for their simplified configuration, improved development efficiency, application isolation, server integration, multi-tenant environment, and rapid deployment. The problems of container virtualization security, container image security, container network security, and container service stability faced by Docker containers during operation are studied, and solutions for the above risks are given.

Keywords: Docker; image; security; risk.

Введение

В последние годы многие предприятия и научно-исследовательские учреждения отдавали предпочтение облачным вычислениям как центру компьютерной и интернет-индустрии. В качестве ключевой технологии облачных вычислений [1] технология виртуализации быстро развивалась с использованием облачных вычислений. Виртуализация относится к виртуализации компьютера на несколько логических компьютеров с помощью технологии виртуализации [2]. Виртуализация может быть достигнута либо с помощью аппаратной эмуляции, либо с помощью операционной системы. Текущие основные технологии виртуализации, такие как XEN, VMware и KVM, представляют собой технологии виртуализации платформ, основанные на виртуальных машинах [3]. Эти решения, как правило, менее адаптируются к крупномасштабному развертыванию кластера из-за обычно больших образов виртуальных машин, необходимости в собственной независимой полной операционной системе (GuestOS) и большого количества занимаемых аппаратных ресурсов.

Docker — это облачный проект с открытым исходным кодом, основанный на языке Go, который появился на свет в начале 2013 года [4]. Как облегченная технология виртуализации, Docker имеет значительные преимущества перед традиционными виртуальными машинами при запуске приложений [5]: Контейнеры Docker работают очень быстро, а запуск и остановка могут быть достигнуты за секунды, по сравнению с традиционным подходом к виртуальной машине намного быстрее. Контейнеры Docker требуют очень мало ресурсов в системе, и хост может запускать до тысяч контейнеров, что невообразимо на традиционных виртуальных машинах. Docker поддерживает гибкий механизм автоматического создания и развертывания через конфигурационный файл Dockerfile для повышения эффективности [6]. Благодаря широкому использованию контейнерной технологии Docker обеспечение безопасности контейнеров Docker считается ключом к использованию контейнеров Docker.

1. Анализ безопасности докера.

Docker — это реализация виртуализации на уровне операционной системы Linux, и его суть ничем не отличается от процесса, работающего в Linux. В настоящее время безопасность контейнеров Docker существенно зависит от самой системы Linux [7]. Безопасность Docker в основном достигается за счет следующих аспектов: Безопасность изоляции контейнера, обеспечиваемая механизмом пространства имен ядра Linux. Благодаря механизму пространства имен программы в контейнерах Docker, работающие на одном хосте, не могут влиять друг на друга и имеют свои собственные уникальные сетевые стеки, к которым другие контейнеры не могут получить доступ. Возможность управления механизмом группы управления Linux для ресурсов контейнера защищена. Механизм группы управления Linux может гарантировать, что контейнеры на одном хосте справедливо распределяют ресурсы, такие как ЦП, диск и память хоста. Механизм группы управления также гарантирует, что нормальная работа хоста и других контейнеров не будет затронута, когда контейнер нестандартный. Права доступа, предоставленные механизмом возможностей ядра Linux, безопасны. Linux обеспечивает более детальное управление доступом к разрешениям. Чтобы обеспечить безопасность контейнеров, мы будем строго ограничивать разрешения контейнеров при использовании контейнеров Docker, ограничивая их только минимальными разрешениями, необходимыми для функций контейнера.

1.1. Зеркальные риски безопасности

Образ Docker — это статическое представление контейнера Docker, и безопасность среды выполнения контейнера зависит от безопасности образа Docker. Docker Hub — это официальный репозиторий образов Docker, в котором Образам Docker не хватает идеального контроля за загрузчиками, а их версия, качество и безопасность не контролируются пользователями. Если в Dockerfile не указан USER, Docker будет запускать контейнер с привилегиями root, в случае атаки на него могут быть получены привилегии root хоста. Использование паролей, ключей и другой информации в Dockerfile приведет к утечке данных после атаки. Использование образов из небезопасных источников приведет к неконтролируемым рискам безопасности для контейнеров Docker.

1.2. Риски безопасности виртуализации контейнеров

По сравнению с традиционными виртуальными машинами контейнеры Docker не имеют независимой конфигурации ресурсов и изоляции ресурсов на уровне ядра системы, поэтому существуют потенциальные риски изоляции ресурсов и неполных ограничений ресурсов.

Атака с выходом из контейнера означает, что злоумышленник получает полномочия root незаконными средствами и получает возможность выполнения команд с определенными правами хоста или других контейнеров, что влияет на текущую безопасность хоста или других контейнеров.

Контейнер Docker и хост совместно используют ядро операционной системы, и существуют потенциальные риски, связанные с отсутствием изоляции файловой системы, изоляции процессов и изоляции межпроцессного взаимодействия между контейнером Docker и другими контейнерами или хостами на хосте. Проблемы безопасности, связанные с изоляцией контейнера Docker, в основном включают следующие два

Ситуация: Злоумышленник напрямую атакует ядро операционной системы, создавая угрозу безопасности для контейнера Docker на хосте. Злоумышленник незаконно получает данные, управляя контейнером Docker для доступа к хосту или другим контейнерам.

Контейнер Docker и хост совместно используют аппаратные ресурсы, такие как ЦП, память и дисковое пространство. Если контейнер Docker не ограничивает использование ресурсов хоста контейнером Docker, злоумышленник может истощить аппаратные ресурсы хоста, захватив контейнер. или другое назначение контейнера, подвешивающего или даже умирающего.

1.3. Риски кибербезопасности

Безопасность сети контейнеров Docker всегда была одной из самых серьезных проблем, с которыми сталкиваются при использовании контейнеров. Из-за особой сетевой среды сеть Docker более строгая, чем традиционная сетевая безопасность.

Контейнеры Docker имеют различные сетевые режимы, предоставляя такие функции, как взаимодействие между контейнерами, взаимодействие между контейнерами между хостами и сеть кластера контейнеров. Ниже приводится анализ потенциальных рисков сетевой безопасности нескольких основных сетевых режимов. Режим моста заключается в том, что Docker по умолчанию принимает сетевой режим моста. В режиме моста на хосте создается виртуальный мост docker0, и все контейнеры Docker в этом режиме подключаются на хосте к мосту docker0. Все контейнеры Docker взаимно доступны. Хотя режим моста обеспечивает удобство взаимного доступа между контейнерами, из-за отсутствия механизма безопасного управления злоумышленники могут повлиять на безопасность хоста и других контейнеров с помощью широковещательных штормов, сниффинга, мошенничества с ARP и других методов атак. MacVLAN – это решение для виртуализации сетевых карт для контейнеров Docker. В мультитенантном сценарии для каждого арендатора виртуализируется отдельная сеть для обеспечения изоляции. Однако, поскольку контрольный доступ между контейнерами Docker в одной и той же виртуальной сетевой среде отсутствует, злоумышленники по-прежнему могут влиять на безопасность хоста и других контейнеров с помощью широковещательных штормов, сниффинга, мошенничества с ARP и других методов атак. Как наиболее распространенное решение для передачи данных и маршрутизации между хостами, оверлейная сеть в основном используется для построения кластерной сети контейнеров между хостами.

сеть. Как и два вышеупомянутых сетевых режима, оверлей по-прежнему имеет риски безопасности из-за отсутствия контроля доступа. Следовательно, независимо от того, какой сетевой режим используется, существует риск взаимных атак между контейнерами.

2. Реализация механизма безопасности Docker

2.1. Механизм защиты образа контейнера

Чтобы обеспечить безопасность образа контейнера Docker, после получения общедоступного минимального базового образа из официального репозитория образов вам необходимо использовать инструмент сканирования безопасности для сканирования загруженного образа на предмет безопасности. В настоящее время используется больше инструментов, включая Docker Security Scanning, Clair and Trivy и т. д. Программное обеспечение в обнаруживаемом образе содержит уязвимости CVE. После создания управляемого образа контейнера, чтобы упростить управление образом, необходимо создать управляемый частный репозиторий образов. Необходимо обеспечить отсутствие доступа к зеркальному складу из внешней публичной сети. В процессе подтягивания зеркала используется механизм проверки содержимого для решения проблемы взлома зеркала контейнера посередине. Чтобы убедиться, что исполняемые файлы и файлы конфигурации в контейнере Docker заслуживают доверия, проверка CRC32 выполняется для исполняемых файлов и файлов конфигурации перед каждым запуском контейнера Docker, и контейнер Docker может быть запущен только после успешной проверки. Предполагая, что исполняемые файлы и файлы конфигурации ключей имеют значения F1, F2... Fn соответственно, после развертывания программы-контейнера Docker контрольное значение C1 всех исполняемых файлов и файлов конфигурации ключей вычисляется один раз, а контрольное значение шифруется. и сохранен. Перед запуском контейнера Docker снова вычисляется проверочное значение C2 для всех исполняемых файлов и ключевых файлов конфигурации, и проверочные значения сравниваются дважды. Схема процесса показана на рисунке 1:

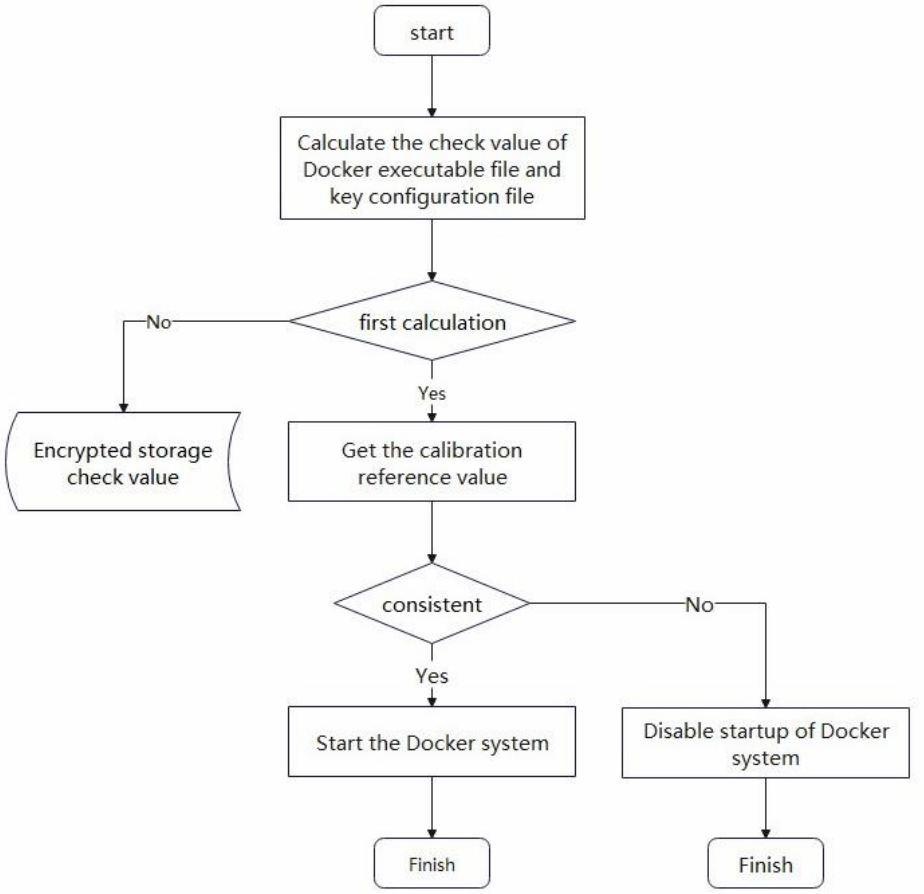


Рисунок 1 – Процесс запуска образа контейнера

2.2. Механизм безопасности виртуализации контейнеров

В архитектуре контейнера, основанной на существующих механизмах Cgroups, Namespace и возможностей ядра, управление ресурсами безопасности контейнера Docker может быть достигнуто за счет улучшения соответствующих механизмов на уровне ядра операционной системы.

Cgroups наложили ограничения на элементы ресурсов, такие как ЦП, память и скорость дискового ввода-вывода контейнеров Docker, чтобы контейнер не исчерпал аппаратные ресурсы на хосте. Когда контейнер запускается, параметры CPU, Memory и Device можно использовать для ограничения использования CPU, использования памяти и скорости чтения/записи диска. Ограничьте объем использования диска, создайте отдельного пользователя для каждого контейнера и ограничьте объем использования диска для каждого пользователя. Используйте каталоги файловой системы, такие как XFS, для ограничения использования диска. Создайте виртуальную файловую систему фиксированного размера для каждого контейнера.

Для ограничения доступа Docker-контейнера к ресурсам хоста используется механизм SELinux. При запуске Docker-контейнера SELinux можно запустить с использованием docker daemon --selinux-enabled = true.

2.3. Механизм безопасности контейнерной сети

В производственной среде хост обычно развертывает сотни или тысячи контейнеров Docker для предоставления услуг для мультитенантности. Чтобы отдельные контейнеры не занимали большую часть пропускной способности и делали другие службы контейнеров Docker недоступными, контроллер трафика модуля управления трафиком Linux используется в сети контейнеров для регулирования трафика.

Чтобы предотвратить злонамеренные сетевые атаки и обеспечить сетевую безопасность контейнеров Docker, можно реализовать контроль доступа к сети, настроив политику белого списка. Политика доступа к белому списку может быть реализована с помощью механизма брандмауэра, который поставляется с Linux.

Когда контейнеры Docker предоставляют услуги самостоятельно, не требуя, чтобы несколько контейнеров Docker формировали микросервисы. Для предотвращения вредоносных атак между контейнерами Docker необходимо запретить межконтейнерное взаимодействие, что можно установить командой dockerd --icc=false.

2.4. Механизм безопасности программы обслуживания контейнеров

Основная функция контейнеров Docker — предоставление надежных и стабильных облегченных сервисов виртуализации. Чтобы обеспечить стабильность сервисной программы в контейнере Docker, программа-сторож может выполнять регулярные проверки в контейнере. В то же время можно создать центр управления контейнером для регулярного получения данных пульса, отправляемых программой пульса в контейнере, и обработки их в соответствии с ситуацией приема.

Программа «watchdog» в основном используется для запуска и проверки сервисов в Docker. Его основной рабочий процесс показан на рисунке 2.

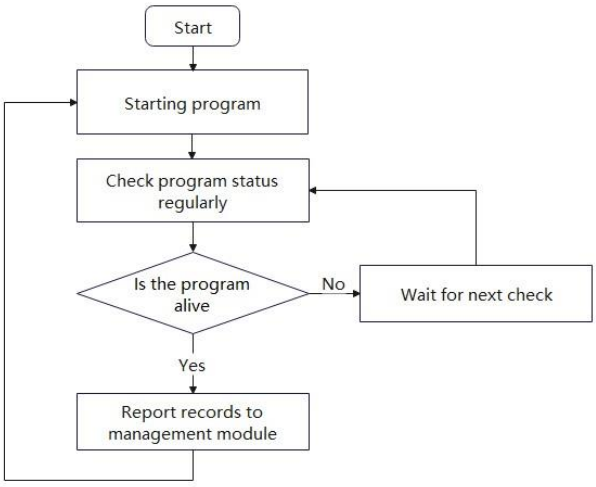


Рисунок 2 – Поток выполнения сторожевой программы

Шаг 1: запустите сервисную программу в контейнере.

Шаг 2: регулярно проверяйте статус сервисной программы. После того, как сервисная программа окажется зависшей, сообщите о проблеме в модуль управления и перезапустите сервисную программу.

Шаг 3: Дождитесь следующей проверки.

При реализации процесса пульса в контейнере Docker пульсация и рабочие данные регулярно отправляются в центр управления, чтобы достичь цели мониторинга ресурсов в контейнере. Его основной процесс показан на рисунке 3.

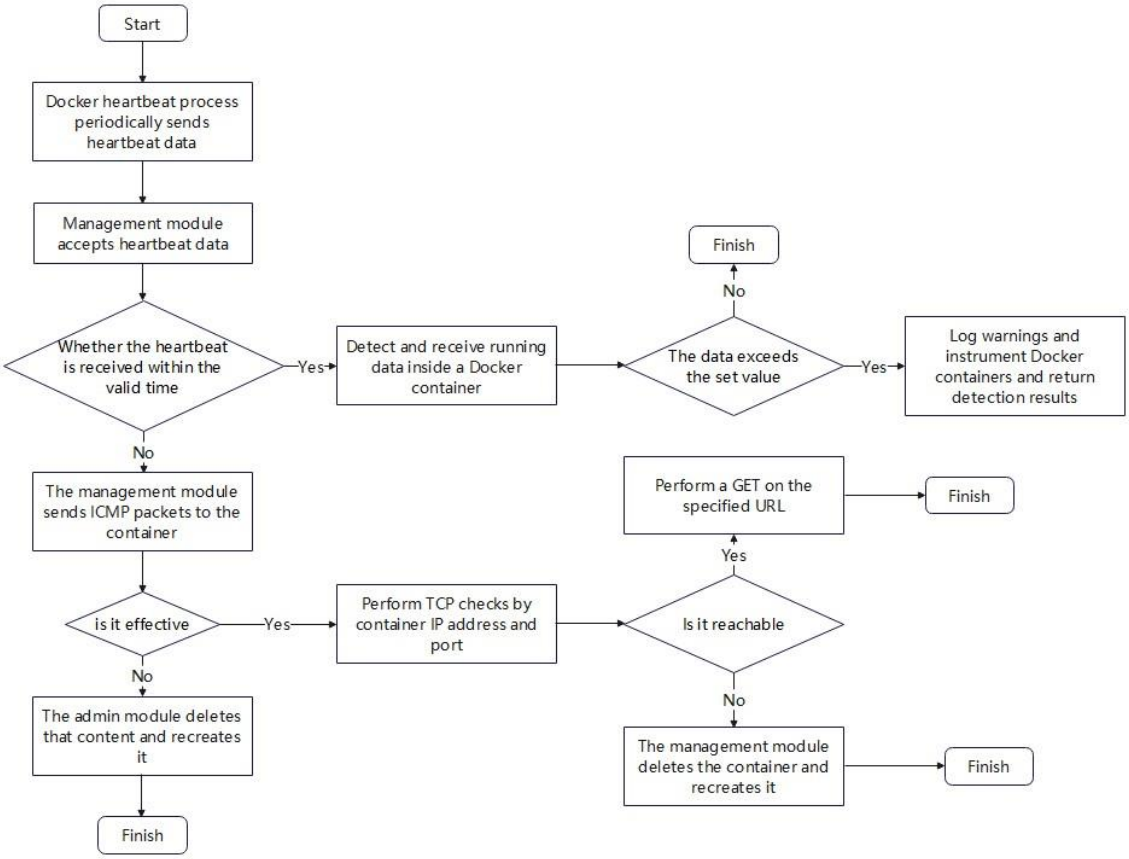


Рисунок 3 – Поток обработки пульса

Шаг 1: Процесс пульса в контейнере Docker периодически отправляет данные, такие как использование ЦП и памяти контейнера Docker, в центр управления.

Шаг 2: Центр управления получает данные, отправленные Docker, и записывает их. Если ЦП контейнера, память и другие данные превышают установленное безопасное значение в течение длительного времени, необходимо проверить контейнер Docker и перераспределить ресурсы.

Шаг 3: Центр управления не получает данные, отправленные процессом пульса в контейнере Docker, в течение периода ожидания. Отправьте ICMP-пакет в контейнер Docker, если контейнер не возвращается, уведомите хост о необходимости удалить контейнер и создать его заново.

Шаг 4: когда ICMP-пакет возвращается, выполняется проверка TCP по IP-адресу и порту и принимается возвращенный результат проверки. Если результат проверки успешен, это означает, что контейнер Docker доступен. В противном случае хост получает уведомление об удалении контейнера и его воссоздании.

ЗАКЛЮЧЕНИЕ

В этой статье представлены решения путем анализа угроз безопасности, с которыми могут столкнуться контейнеры Docker при использовании. Во время производства и

развертывания контейнеров Docker следует полностью учитывать возможные риски безопасности и проводить соответствующий анализ требований безопасности в соответствии со сценариями развертывания. В сочетании с решениями безопасности контейнеров Docker должны формироваться.

Список литературы

1. Zhang Y. Cloud Computing and Virtualization Technology // Computer Security – 2011. – №5. – С. 80–82.
2. Luo J. Cloud computing: architecture and key technologies / J. Jin, A. Song // Journal on Communications – 2011. Vol. 32. № 07. – С.3–21.
3. Библиотека программиста [Электронный ресурс]: Что такое Docker, и как его использовать? URL: https://proglib.io/p/docker (дата обращения 11.03.2020).
4. 1. Блог компании RUVDS.com [Электронный ресурс]: Изучаем Docker URL: https://habr.com/ru/company/ruvds/blog/438796/ (дата обращения 11.03.2020).
5. Каталог облачных служб Azure | Microsoft Azure [Электронный ресурс] URL: https://azure.microsoft.com/ru-ru/services/ (дата обращения: 11.02.2020).
6. Comparing Virtual Machines vs Docker Containers [Электронный ресурс] URL: https://clck.ru/MEwKH (дата обращения: 11.02.2020).
7. И.В.Подорожный, А.Н.Светличный, А.В.Подлеснов. Введение в контейнеры, виртуальные машины и docker // Молодой ученый. 2016. №19. С. 49-53. URL: https://moluch.ru/archive/123/33873/ (дата обращения: 02.07.2018).

References

1. Zhang Y. Cloud Computing and Virtualization Technology // Computer Security - 2011. - No. 5. – pp. 80–82.
2. Luo J. Cloud computing: architecture and key technologies / J. Jin, A. Song // Journal on Communications - 2011. Vol. 32. No. 07. – pp.3–21.
3. Programmer's Library [Electronic resource]: What is Docker and how to use it? URL: https://proglib.io/p/docker (Accessed 03/11/2020).
4. 1. RUVDS.com company blog [Electronic resource]: Exploring Docker URL: https://habr.com/ru/company/ruvds/blog/438796/ (accessed 03/11/2020).
5. Azure Cloud Services Catalog | Microsoft Azure [Electronic resource] URL: https://azure.microsoft.com/en-us/services/ (accessed 02/11/2020).
6. Comparing Virtual Machines vs Docker Containers [Electronic resource] URL: https://clck.ru/MEwKH (accessed 02/11/2020).
7. I.V. Podorozhny, A.N. Svetlichny, A.V. Podlesnov. Introduction to containers, virtual machines and docker // Young scientist. 2016. No. 19. pp. 49-53. URL: https://moluch.ru/archive/123/33873/ (date of access: 07/02/2018).

Сидоркин А.Д., Панчехин Н. И., Десятов А. Г. Обзор существующих решений на основе методов машинного и глубокого обучения для задач аутентификации при помощи ЭКГ-паттернов // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 73–85

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.52

ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ НА ОСНОВЕ МЕТОДОВ МАШИННОГО И ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ЗАДАЧ АУТЕНТИФИКАЦИИ ПРИ ПОМОЩИ ЭКГ-ПАТТЕРНОВ

[1] Сидоркин А.Д., [2] Панчехин Н. И., [3] Десятов А. Г.
ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана, Москва, Россия (105005, Москва, ул. 2-я Бауманская, д.5, стр.1), e-mail: [1] Sidorkin1556@gmail.ru, [2] 000256789@yandex.ru, [3] Desyatov.a001@yandex.ru

Традиционные методы аутентификации, такие как пароли, токены, отпечатки пальцев сильно подвержены кражам и фальсификации. На замену им разрабатываются новые подходы. Одним из таких подходов является аутентификация при помощи паттернов сердцебиения. Электрическая активность сердца уникальна у каждого человека. Кроме того электрокардиограмму сложно подделать. Эти факты побуждают использовать ЭКГ в биометрических системах. Машинное и глубокое обучение являются наиболее эффективными методами для решения задач аутентификации по ЭКГ. В данной статье рассмотрены современные исследования, в которых применяется машинное и глубокое обучение. Аутентификация, инструментами которой являются эти два метода, включает в себя следующие основные стадии: сбор данных, их обработка, извлечение признаков, классификация. Описание стадий и используемых алгоритмов на каждой из них приведено в этой работе. По результатам литературного обзора сделаны выводы.

Ключевые слова: Аутентификация, ЭКГ, машинное обучение, глубокое обучение, фильтрация, извлечение признаков, классификация, биометрия.

OVERVIEW OF EXISTING SOLUTIONS BASED ON MACHINE AND DEEP LEARNING METHODS FOR AUTHENTICATION TASKS USING ECG PATTERNS

[1] Sidorkin A.D., [2] Panchekhin N. I., [3] Desyatov A. G.
Moscow State Technical University named after N. E. Bauman, Moscow, Russia (105005, Moscow, 2nd Baumanskaya st., 5, building 1), e-mail: [1] Sidorkin1556@gmail.ru, [2] 000256789@yandex.ru, [3] Desyatov.a001@yandex.ru

Traditional authentication methods such as passwords, tokens, and fingerprints are highly susceptible to theft and falsification. New approaches are being developed to replace them. One of these approaches is authentication using heartbeat patterns. The electrical activity of the heart is unique for each person. In addition, an electrocardiogram is difficult to fake. These facts encourage the use of ECG in biometric systems. Machine learning and deep learning are the most effective methods for solving ECG authentication tasks. This article discusses modern research that uses machine learning and deep learning. Authentication, the tools of which are these two methods, includes the following main stages: data collection, processing, feature extraction, classification. A description of the stages and the algorithms used on each of them is given in this paper. Based on the results of the literary review, conclusions are drawn.

Keywords: Authentication, ECG, machine learning, deep learning, filtering, feature extraction, classification, biometrics.

Введение

Биометрические данные, а именно: изображения радужной оболочки глаза, лица или запись голоса, как методы аутентификации, имеют недостатки. Запись голоса нетрудно подделать, а, например, изображения лиц или радужной оболочки глаза, полученные видеокамерами, могут быть повреждены из-за угла наблюдения, а также освещения, разрешения камеры и других параметров. Поэтому рассматриваются новые методы аутентификации, такие как паттерны сердцебиения. В свою очередь, сигналы электрокардиограммы демонстрируют уникальные характеристики строения записи, которые трудно подделать, поскольку основные биометрические параметры скрыты во время аутентификации и могут быть получены только из физических измерений субъекта. С развитием технологий сбора данных появились портативные устройства для снятия электрической активности сердца, такие как смарт-часы Apple, Samsung и т.п. Это облегчает снятие электрокардиограммы для аутентификации.

Аутентификация по ЭКГ не исследована в полной мере. Предлагаемые для аутентификации алгоритмы часто разрабатываются на основе сигналов ЭКГ диагностического класса [1, 2]. Такие сигналы имеют относительно низкий уровень шума. Также на практике для аутентификации необходимо собрать несколько шаблонов электрокардиограммы: в спокойствии, во время физической активности и т.п. На основании изложенных фактов современные методы не могут быть легко адаптированы для практической аутентификации личности. Однако исследуемая область перспективна, и с каждым годом выходит множество работ, предлагаемые решения в которых становятся более точными и оптимизированными.

Стоит отметить, что для аутентификации перспективно использовать и другие биометрические сигналы, например, ЭЭГ или ФКГ, прежде всего из-за их уникального строения у каждого человека, а также из-за высокой трудности воссоздать их искусственно.

Биометрические системы, как правило, состоят из двух основных фаз: регистрация сигнала и фаза аутентификации. На этапе регистрации ЭКГ субъекта записывается для создания шаблона. Далее на этапе аутентификации снимается новое ЭКГ, которое сравнивается с шаблоном для определения разрешения на доступ. Наиболее эффективными инструментами такого сравнения являются модели машинного обучения и модели глубокого обучения. В данной статье приведен литературный обзор таких моделей.

Литературный обзор

1. Электрокардиограмма

Электрокардиограмма представляет собой запись биопотенциалов, связанных с сокращениями сердечной мышцы. Любая ЭКГ состоит из зубцов, сегментов и интервалов (рисунок 1), отражающих процесс небольших электрических изменений, которые являются следствием деполяризации сердечной мышцы с последующей реполяризацией во время каждого сердечного цикла.

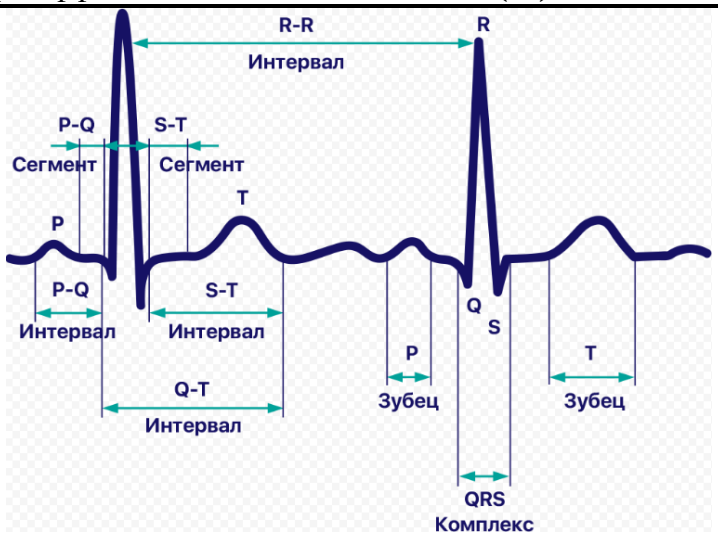


Рисунок 1 – Структурные элементы записи ЭКГ.

Строение записи ЭКГ сильно варьируется у людей из-за различий в размере и расположении сердца, возраста, пола и других факторов. Такая информация, как угол, амплитуда и частота сердечных сокращений, описывает уникальность человека.

2. Предварительная обработка данных

Как для подхода аутентификации по ЭКГ при помощи моделей машинного обучения, так и для подхода, в основе которого лежат модели нейронных сетей, свойственно наличие этапа предварительной обработки данных. Цель предварительной обработки – отделить требуемые биометрические признаки от фонового шума. Сигналы ЭКГ могут быть искажены различными видами шумов. Эти виды включают в себя дрейф изолинии из-за дыхания, возникающий шум из-за движения электродов, а также шумы, создаваемые электронными устройствами, которые используются при снятии ЭКГ. Эти компоненты должны быть удалены или уменьшены до выделения признаков и классификации, поскольку они могут повлиять на биометрическую информацию сигнала. В контексте ЭКГ рассматриваются высокочастотные и низкочастотные компоненты шума. Фильтры нижних частот способны удалять высокочастотный шум. Фильтры высоких частот наоборот.

Для фильтрации ЭКГ сигналов популярны вейвлет-преобразования. В работе [3] сравниваются вейвлеты Хаара и Добеши, а также фильтр нижних частот LPF. Результаты работы показывают, что вейвлет Добеши лучшим образом среди перечисленных сохраняет структурные элементы записи ЭКГ, отделяя ее от шума.

Кроме этого для удаления шума в ЭКГ записи используют фильтр Калмана, фильтр Винера, БИХ-фильтр Баттерворта [4, 5]. В [5] также используется Симлет вейвлет. Аргументируется это тем, что функция похожа на ЭКГ сигнал.

В качестве предварительной обработки во многих работах, например, [5], сегментируют сигналы ЭКГ на удары или интервалы различной продолжительности (например, 2 с и 5 с) перед извлечением признаков.

3. Модели машинного обучения

3.1. Извлечение признаков

Извлечение признаков из сигнала ЭКГ можно разделить на две категории: условно ручное и неручное. Условно ручное извлечение представляет собой интерактивный процесс, включающий ряд автоматических процедур преобразования данных. В свою очередь, условно ручное извлечение делится на нахождение реперных признаков, целостный анализ ЭКГ, гибридный метод. Последний метод является комбинацией первых двух.

Зубцы P, Q, R, S, T, разница во времени между пиками Q и T, а также интервал Q-T, например, считаются реперными признаками. Суть алгоритмов, основанных на таких признаках, состоит в точном обнаружении P, Q, R, S, T зубцов для получения их относительной амплитуды, характерных временных интервалов между ними и ряда других морфологических особенностей. В работах [6-7] использовались некоторые подмножества этих реперных признаков. Временные интервалы и амплитуда пиков каждого отдельного субъекта аутентификации индивидуальны. Однако точное обнаружение структурных элементов записи ЭКГ является очень сложной задачей, поскольку они очень чувствительны к шуму. Более того, алгоритмы, основанные на реперных признаках, не являются универсальными, поскольку у людей с заболеваниями сердца могут отсутствовать те или иные реперные точки, что приводит к значительным ошибкам. Поэтому условно ручное извлечение признаков на основе целостного анализа записи ЭКГ является более предпочтительным.

В основе целостного анализа записи ЭКГ лежит временной или частотный анализ для получения других статистических признаков. Распространенными инструментами для такого анализа являются вейвлет-преобразования [5, 8] и дискретное косинусное преобразование [9].

3.2. Классификация

Перед классификацией нередко производят уменьшение размерности выявленных признаков. Линейный дискриминантный анализ (LDA) [6], анализ главных компонентов (PCA) [6] являются примерами методов уменьшения набора признаков для классификации.

Классификация – это основная составляющая аутентификации субъекта доступа по ЭКГ. Большинство алгоритмов машинного обучения в этой категории реализуют вычисления оценок соответствия на основе сходства и различия между вектором признаков запроса и шаблоном. Во время аутентификации полученная оценка сравнивается с предопределенным порогом. Если оценка сходства предъявленной записи ЭКГ с шаблоном выше некоторого порога, то доступ предоставляется. В современных работах используются различные алгоритмы, такие как метод опорных векторов (SVM) [9-10], наивный баесовский классификатор [11], деревья решений [11], лес решений [8], k-ближайших соседей [12].

Стоит отметить инкрементный метод обучения классификатора SVM [10], при котором сохраняется ранее обученная модель и эффективно обновляется по мере поступления дополнительных входных данных.

4. Модели глубокого обучения

Условно ручные подходы извлечения признаков включают дополнительный этап, а именно нахождение реперных точек или временной и (или) частотный анализ для получения ключевой информации. Нейронные сети способны извлекать признаки автоматически, что

позволяет обходить дополнительные этапы. Это повышает производительность, а также надежность биометрических систем. Надежность повышается в виду того, что при условно ручном извлечении признаков перед исследователями стоит задача оптимизации и правильного подбора механизмов извлечения, при необходимости уменьшения набора признаков. Правильно подобранный комплекс механизмов может хорошо работать на одном наборе данных ЭКГ, но это не означает, что он будет так же работать на другом отличном наборе. В свою очередь, условно ручное извлечение признаков из нескольких наборов данных или при наборе с разными отведениями ЭКГ делает метод еще более сложным.

Распространенными и эффективными моделями нейронных сетей для задачи аутентификации являются сверточная нейронная сеть CNN [1-2, 13-15] и тип рекуррентных нейронных сетей, способный обучаться долгосрочным зависимостям – нейронная сеть с долгой краткосрочной памятью LSTM [13, 16-17].

В работе [18] описываются две модели нейронных сетей, CNN и ResNet. ResNet представляет собой остаточную сеть. Идея заключается в том, чтобы взять несколько сверточных слоев и добавить к ним дополнительные связи, которые проходят мимо этих слоев, пропускают один или несколько слоев. Таким образом решается проблема затухающего градиента. В [18] передавали моделям сигналы ЭКГ без какой-либо обработки и фильтрации. При этом предложенные модели показали высокую точность на тестовых данных. Этот факт говорит о том, что обе модели показывают высокую производительность и хорошую способность к обобщению данных.

В [19] предложили модель BiGRU для задачи аутентификации по ЭКГ. BiGRU представляет собой двунаправленную LSTM с управляемыми рекуррентными блоками. Двунаправленная LSTM запускает входные данные как вперед, так и назад во времени, таким образом, сохраняя контекст как из будущего, так и из прошлого. Это позволяет повышать качество классификации. А управляемые рекуррентные блоки содержат меньше параметров, чем у LSTM, а значит обучать такую сеть можно быстрее. Точность классификации при этом у BiGRU сравнима с BiLSTM [19].

В [20] GRU вводится в сочетании с CNN. Извлечение признаков для классификации в обычной CNN происходит независимо в каждый момент времени. В CNN происходит пространственная корреляция признаков. GRU в сочетании с CNN позволяет лучше извлекать признаки из временного ряда записи ЭКГ. Использование такого сочетания повышает производительность и точность классификации.

В некоторых работах используются ранее обученные известные модели нейронных сетей. Так, например, в работе [14] используется сверточная нейронная сеть Inception, а в [21] используется сверточная нейронная сеть VGG-Net.

5. Результаты литературного обзора

В таблице 1 приведены результаты ранее проделанных работ. В таблице указывается название базы данных, проводили ли в работе фильтрацию, если да, то каким способом. Как выделялись признаки из ЭКГ записи, как происходила классификация, а также метрики для оценки предложенных решений. В Таблице 2 расшифрованы аббревиатуры, используемые в Таблице 1. В обзор вошли работы за последние 5 лет. При этом точность аутентификации

предлагаемых решений свыше 90%, то есть модели перспективно применимы к использованию в биометрических системах.

Таблица 1 – Обзор решений из литературных источников

Источник	Год	База данных	Фильтрация	Выделение признаков	Метод	Метрика
[17]	2017	ECG-ID MITDB	– –	LSTM GRU	LSTM GRU	Acc: 100%, EER: 0 Acc: 96%, EER: 3.5%
[8]	2017	MITDB NSRDB ECG-ID	BP BP BP	НРП/DWT НРП/DWT НРП/DWT	Random Forest Random Forest Random Forest	Acc: 98% Acc: 99% Acc: 91%
[7]	2017	PTB	BW	НРП	SVM	Acc: 97.45%, FAR: 5.71%
[9]	2017	Частная БД	SG	DCT	SVM	Acc: 94.9%, EER: 2.66%
[6]	2017	Частная БД	–	НРП	LDA	Acc: 91.6%
[22]	2018	SIAT-ECG PTB	BW BW	НРП НРП	SVM SVM	Acc: 93.15%, FAR: 11.58% Acc: 100%, FAR: 0
[25]	2018	TEOAE	BP	AC/LDA	SVM	EER: 6.9%
[28]	2018	MIT-BIH	WT	DBLSTM-WS	DBLSTM-WS	Acc: 99,39%
[21]	2019	PTB CYBHi	– –	CNN VGG-Net CNN VGG-Net	QG-MSVM QG-MSVM	Acc: 96.83%, FAR: 3.1% Acc: 97.15%, EER: 2.8
[24]	2019	UofTDB CYBHi	– –	CNN CNN	CNN CNN	EER: 7.86% EER: 15.37%
[2]	2019	MWM-HIT	MD	CNN	CNN	Acc: 96.96%, EER: 4.86%

Продолжение Таблицы 1						
[14]	2019	PTB	–	CNN Inception	CNN Inception	Acc: 98.1%
[1]	2019	PTB	BW	CNN	CNN	EER: 2.9%
[15]	2019	PTB MIT-BIH	BP BP	CNN CNN	CNN CNN	Acc: 98.45% Acc: 99.2%
[26]	2019	ECG-ID MIT-BIH	– –	CNN CNN	SVM SVM	Acc: 98.24% Acc: 95.99%
[19]	2019	ECG-ID MITDB	BW BW	BiGRU BiGRU	BiGRU BiGRU	Acc: 98.6% Acc: 98.4%
[31]	2019	PTB PTB	CWT CWT	AlexNet GoogLeNet	AlexNet GoogLeNet	Acc: 92.50% Acc: 100%
[16]	2020	NSRDB MITDB	DF+MAF DF+MAF	BiLSTM BiLSTM	BiLSTM BiLSTM	Acc: 100%, F1-score: 1 Acc: 99.8%, F1-score: 0.99
[27]	2020	NSRDB FANTASIA	BP BP	Cascaded CNN Cascaded CNN	Cascaded CNN Cascaded CNN	Acc: 91.4% Acc: 99.9%
[29]	2020	FANTASIA MIT-BIH CYBHi	MAF MAF MAF	TCNN TCNN TCNN	TCNN TCNN TCNN	Acc: 100% Acc: 96% Acc: 90%
[30]	2021	ECG-ID MIT-BIH PTB	– – –	HT/FT + PCANet HT/FT + PCANet HT/FT + PCANet	SVM SVM SVM	Acc: 99.44% Acc: 99.66% Acc: 99.77%
[18]	2021	CYBHi CYBHi	– –	CNN ResNet-Attention	CNN ResNet-Attention	Acc: 99.72%, EER: 0.27% Acc: 99.27%, EER: 0.68%

Продолжение Таблицы 1						
[20]	2021	MIT-BIH	WT	CNN-GRU	CNN-GRU	Acc: 99.61%, F1-score: 0.99
[10]	2021	MIT-BIH CYBHi	BP BP	НРП НРП	Инкрементный SVM	Acc: 97.7% Acc: 99.4%
[23]	2022	MIT-BIH + CinC_2017	WT	FRRNet	FRRNet	Acc: 98.97%, F1-score: 0.98
[32]	2022	AFDB NSRDB ECG-ID	BW BW BW	BERT BERT BERT	BERT BERT BERT	Acc: 96.2% Acc: 99.91% Acc: 96.35%
[33]	2022	MIT-BIH	BW	HBF	LS-SVM	Acc: 95%

Таблица 2 – Используемые сокращения

Сокращение	Расшифровка	Сокращение	Расшифровка
Acc	Accuracy	AC	Normalized Autocorrelation
BERT	Bidirectional Encoder Representations from Transformers	DBLSTM-WS	Deep Bidirectional LSTM network-based Wavelet Sequences
EER	Equal Error Rates	LS-SVM	Least Square Support Vector Machine
FAR	False Acceptance Rate	LDA	Linear Discriminant Analysis
CNN	Convolutional Neural Network	QG-MSVM	Q-Gaussian multi support vector machine
BP	Band Pass filter	MD	Median filter
DWT	Discrete Wavelet Transform	CWT	Continuous Wavelet Transform
LSTM	Long Short-Term Memory network	DF	Derivative Filter
GRU	Gated Recurrent Units	MAF	Moving average filter
WT	Wavelet Transform	TCNN	Temporal Convolutional Neural Network
НРП	Нахождение реперных признаков	PCANet	Principal Component Analysis Network

Продолжение Таблицы 2			
SVM	Support Vector Machine	FT	Fourier Transform
BW	Butterworth low-pass filter	HT	Hilbert Transform
SG	Savitzky-Golay filter	FFRNet	Feature Reuse Residual Network
DCT	Discrete Cosine Transform	HBF	Half-Band Filter

В работах, приведенных в таблице 1, используются разные базы данных. Кроме того берутся различные количества записей из этих баз. Некоторые наборы данных содержат только здоровые сигналы ЭКГ, некоторые с различными аритмиями. В некоторых работах используют только одно отведение ЭКГ, в других – несколько. Некоторые авторы используют в своих работах ЭКГ записи, снятые в покое, после физической активности и т.п. Некоторые – только ЭКГ диагностического класса. Исходя из вышеперечисленных фактов, нельзя перечислить решения из Таблицы 1, которые являются наиболее точными и производительными. Для однозначного превосходства одних алгоритмов над другими необходимы равные условия, а также необходимо определить значимость таким критериям, как оценочные метрики, скорость работы и способность адаптации под программное обеспечение. Однако на основе литературного обзора можно подчеркнуть следующие факты:

1) за последние годы в доминирующем количестве работ используют глубокое обучение, в частности для задачи аутентификации наиболее популярными являются сверточные нейронные сети;
2) модели, в основе которых лежат нейронные сети, характеризуются более высокой скоростью аутентификации, поскольку содержат в своей структуре меньше механизмов;
3) сочетание сверточных нейронных сетей для выделения признаков и моделей машинного обучения для классификации дает хорошие результаты;
4) алгоритмы, не использующие предварительную фильтрацию сигнала ЭКГ, показывают хорошие результаты. При этом такие алгоритмы имеют более высокую производительность, а также они более устойчивы к шуму;
5) полосовой фильтр, фильтр Баттерворта, а также вейвлет-преобразования являются популярными методами фильтрации сигнала ЭКГ;
6) в большинстве работ используют базы данных, содержащие сигналы ЭКГ диагностического класса. Эти сигналы сняты в медицинских учреждениях и содержат относительно низкий уровень фонового шума. Алгоритмы, обученные на таких сигналах, менее применимы в биометрических системах. В связи с этим остается актуальной задача сбора записей ЭКГ теми же методами, с помощью которых сигнал будет сниматься в биометрических системах. А также сбора записей ЭКГ в различных состояниях человека.

Заключение

В данной работе приведен литературный обзор методов машинного и глубокого обучения для задач аутентификации при помощи ЭКГ-паттернов. Приведены основные алгоритмы, которые используются в исследуемой теме, и результаты их применения. Описаны основные стадии аутентификации по ЭКГ при помощи нейронных сетей и машинного обучения. На основе литературного обзора сделаны выводы.

Список литературы

1. R. D. Labati, E. Muñoz, V. Piuri, R. Sassi, F. Scotti, Deep-ECG: Convolutional Neural Networks for ECG biometric recognition, Pattern Recognition Letters, Volume 126, 2019, Pages 78-85.
2. M. Hammad, S. Zhang, K. Wang, A novel two-dimensional ECG feature extraction and classification algorithm based on convolution neural network for human authentication, FGCS, Volume 101, 2019, Pages 180-196.
3. A. B. Patwary, M. T. I. Chowdhury and N. Mamun, Comparison Among ECG Filtering Methods for Non-linear Noise, ICAEEE, 2018.
4. Manju B.R., Sneha M.R., ECG Denoising Using Wiener Filter and Kalman Filter, Procedia Computer Science, Volume 171, 2020, Pages 273-281.
5. M. Ingale, R. Cordeiro, S. Thentu, Y. Park and N. Karimian, ECG Biometric Authentication: A Comparative Analysis, IEEE Access, vol. 8, pp. 853-866, 2020.
6. V. Krasteva, I. Jekova, R. Abächerli, Biometric verification by cross- correlation analysis of 12-lead ECG patterns: Ranking of the most reliable peripheral and chest leads, Electrocardiology, vol. 50, pp. 847-854, 2017.
7. J. S. Paiva, D. Dias and J. P. S. Cunha, Beat-ID: Towards a computationally low-cost single heartbeat biometric identity check system based on electrocardiogram wave morphology, PLoS ONE, vol. 12, no 7, 2017.
8. Tan R., Perkowski M., Toward Improving Electrocardiogram (ECG) Biometric Verification using Mobile Sensors: A Two-Stage Classifier Approach. Sensors, vol. 17, pp. 410, 2017.
9. J. Pinto, J. Cardoso, A. Lourenço and C. Carreiras, "Towards a continuous biometric system based on ECG signals acquired on the steering wheel", Sensors, vol. 17, no. 10, pp. 2228, 2017.
10. Kim J., Yang G., Lee S., Kim K., Park C. Efficiently Updating ECG- Based Biometric Authentication Based on Incremental Learning. Sensors, vol. 21, no 5, pp. 1568, 2021
11. Ergin S., Uysal A.K., Gunal E.S., Gunal S., Gulmezoglu M.B. ECG based biometric authentication using ensemble of features; Proceedings of the 9th CISTI, Barcelona. 18–21 June 2014; pp. 1–6.
12. K. A. Sidek, I. Khalil and H. F. Jelinek, ECG biometric with abnormal cardiac conditions in remote monitoring system, IEEE, vol. 44, pp. 1498-1509, 2014.
13. Коннова Н.С., Сафина Д., Биометрическая аутентификация по ЭКГ на основе машинного обучения, ИиТТ 2020, № 48, С. 17 – 24.
14. P.L. Hong, J.Y. Hsiao, C.H. Chung, Y.M. Feng and S.C. Wu, ECG biometric recognition: Template-free approaches based on deep learning, Proc. 41st Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), pp. 2633-2636, 2019.

15. J. S. Kim, S. H. Kim and S. B. Pan, Personal recognition using convolutional neural network with ECG coupling image, J. Ambient Intell. Humanized Comput., pp. 1-10, 2019.
16. Kim B.H., Pyun J.Y., ECG Identification For Personal Authentication Using LSTM-Based Deep Recurrent Neural Networks. Sensors. 2020; 20(11):3069.
17. R. Salloum, C.C.J. Kuo, ECG-based biometrics using recurrent neural networks, Proc. IEEE-ICASSP, pp. 2062-2066, 2017.
18. Hammad M., Pławiak P., Wang K., Acharya U.R., ResNet-Attention model for human authentication using ECG signals. Expert Syst. 2021, 38, E12547.
19. Lynn H.M., Pan S.B., Kim P., A Deep Bidirectional GRU Network Model for Biometric Electrocardiogram Classification Based on Recurrent Neural Networks. IEEE Access 2019,7, 395–405.
20. Yao G., Mao X., Li N., Xu H., Xu X., Jiao Y., Ni J., Interpretation of Electrocardiogram Heartbeat by CNN and GRU. Comput Math Methods Med. Aug 29 2021:6534942.
21. M. Hammad, Y. Liu and K. Wang, Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint, IEEE Access, vol. 7, pp. 527-542, 2019.
22. J. Liu, L. Yin, C. He, B. Wen, X. Hong and Y. Li, A multiscale autoregressive model-based electrocardiogram identification method, IEEE Access, vol. 6, pp. 251-263, 2018.
23. Yang Z., Liu L., Li N., Tian J., ECG Identity Recognition Based on Feature Reuse Residual Network. Processes. 2022; 10(4): 676.
24. J. Pinto and S. J. Cardoso, A end-to-end convolutional neural network for ECG based biometric authentication, IEEE-BTAS, pp. 1-8, 2019.
25. M. Komeili, W. Louis, N. Armanfard and D. Hatzinakos, Feature selection for nonstationary data: Application to human recognition using medical biometrics, IEEE Trans. Cybern., vol. 48, no. 5, pp. 1446-1459, 2018.
26. Y. Chu, H. Shen and K. Huang, ECG authentication method based on parallel multi-scale one-dimensional residual network with center and margin loss, IEEE Access, vol. 7, pp. 598-607, 2019.
27. Y. Li, Y. Pang, K. Wang and X. Li, Toward improving ECG biometric identification using cascaded convolutional neural networks, Neurocomputing, vol. 391, pp. 83-95, 2020.
28. Yildirim Ö. A novel wavelet sequence based on deep bidirectional LSTM network model for ECG signal classification. Comput. Boil. Med. 2018, 189–202.
29. Belo D., Bento N., Silva H., Fred A., ECG Biometrics Using Deep Learning and Relative Score Threshold Classification. Sensors 2020, 20, 4078.
30. Liu X., Si Y., Yang W., A Novel Two-Level Fusion Feature for Mixed ECG Identity Recognition. Electronics 2021, 10, 2052.
31. Byeon Y.H., Pan S.B., Kwak K.C., Intelligent Deep Models Based on Scalograms of Electrocardiogram Signals for Biometrics. Sensors 2019, 19, 935.
32. Chee K.J., Ramli D.A., Electrocardiogram Biometrics Using Transformer's Self-Attention Mechanism for Sequence Pair Feature Extractor and Flexible Enrollment Scope Identification. Sensors. 2022 Apr 30; 22(9):3446.

33. Majeed R.R., Alkhafaji S.K.D., ECG classification system based on multi-domain features approach coupled with least square support vector machine (LS-SVM). Comput Methods Biomech Biomed Engin. 2022 May 13, pp.1-8.

References

1. R. D. Labati, E. Muñoz, V. Piuri, R. Sassi, F. Scotti, Deep-ECG: Convolutional Neural Networks for ECG biometric recognition, Pattern Recognition Letters, Volume 126, 2019, Pages 78-85.
2. M. Hammad, S. Zhang, K. Wang, A novel two-dimensional ECG feature extraction and classification algorithm based on convolution neural network for human authentication, FGCS, Volume 101, 2019, Pages 180-196.
3. A. B. Patwary, M. T. I. Chowdhury and N. Mamun, Comparison Among ECG Filtering Methods for Non-linear Noise, ICAEEE, 2018.
4. Manju B.R., Sneha M.R., ECG Denoising Using Wiener Filter and Kalman Filter, Procedia Computer Science, Volume 171, 2020, Pages 273-281.
5. M. Ingale, R. Cordeiro, S. Thentu, Y. Park and N. Karimian, ECG Biometric Authentication: A Comparative Analysis, IEEE Access, vol. 8, pp. 853-866, 2020.
6. V. Krasteva, I. Jekova, R. Abächerli, Biometric verification by cross- correlation analysis of 12-lead ECG patterns: Ranking of the most reliable peripheral and chest leads, Electrocardiology, vol. 50, pp. 847-854, 2017.
7. J. S. Paiva, D. Dias and J. P. S. Cunha, Beat-ID: Towards a computationally low-cost single heartbeat biometric identity check system based on electrocardiogram wave morphology, PLoS ONE, vol. 12, no 7, 2017.
8. Tan R., Perkowski M., Toward Improving Electrocardiogram (ECG) Biometric Verification using Mobile Sensors: A Two-Stage Classifier Approach. Sensors, vol. 17, pp. 410, 2017.
9. J. Pinto, J. Cardoso, A. Lourenço and C. Carreiras, "Towards a continuous biometric system based on ECG signals acquired on the steering wheel", Sensors, vol. 17, no. 10, pp. 2228, 2017.
10. Kim J., Yang G., Lee S., Kim K., Park C. Efficiently Updating ECG- Based Biometric Authentication Based on Incremental Learning. Sensors, vol. 21, no 5, pp. 1568, 2021
11. Ergin S., Uysal A.K., Gunal E.S., Gunal S., Gulmezoglu M.B. ECG based biometric authentication using ensemble of features; Proceedings of the 9th CISTI, Barcelona. 18–21 June 2014; pp. 1–6.
12. K. A. Sidek, I. Khalil and H. F. Jelinek, ECG biometric with abnormal cardiac conditions in remote monitoring system, IEEE, vol. 44, pp. 1498-1509, 2014.
13. Коннова Н.С., Сафина Д., Биометрическая аутентификация по ЭКГ на основе машинного обучения, ИиТТ 2020, № 48, С. 17 – 24.
14. P.L. Hong, J.Y. Hsiao, C.H. Chung, Y.M. Feng and S.C. Wu, ECG biometric recognition: Template-free approaches based on deep learning, Proc. 41st Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), pp. 2633-2636, 2019.
15. J. S. Kim, S. H. Kim and S. B. Pan, Personal recognition using convolutional neural network with ECG coupling image, J. Ambient Intell. Humanized Comput., pp. 1-10, 2019.

16. Kim B.H., Pyun J.Y., ECG Identification For Personal Authentication Using LSTM-Based Deep Recurrent Neural Networks. Sensors. 2020; 20(11):3069.
17. R. Salloum, C.C.J. Kuo, ECG-based biometrics using recurrent neural networks, Proc. IEEE-ICASSP, pp. 2062-2066, 2017.
18. Hammad M., Pławiak P., Wang K., Acharya U.R., ResNet-Attention model for human authentication using ECG signals. Expert Syst. 2021, 38, E12547.
19. Lynn H.M., Pan S.B., Kim P., A Deep Bidirectional GRU Network Model for Biometric Electrocardiogram Classification Based on Recurrent Neural Networks. IEEE Access 2019,7, 395–405.
20. Yao G., Mao X., Li N., Xu H., Xu X., Jiao Y., Ni J., Interpretation of Electrocardiogram Heartbeat by CNN and GRU. Comput Math Methods Med. Aug 29 2021:6534942.
21. M. Hammad, Y. Liu and K. Wang, Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint, IEEE Access, vol. 7, pp. 527-542, 2019.
22. J. Liu, L. Yin, C. He, B. Wen, X. Hong and Y. Li, A multiscale autoregressive model-based electrocardiogram identification method, IEEE Access, vol. 6, pp. 251-263, 2018.
23. Yang Z., Liu L., Li N., Tian J., ECG Identity Recognition Based on Feature Reuse Residual Network. Processes. 2022; 10(4): 676.
24. J. Pinto and S. J. Cardoso, A end-to-end convolutional neural network for ECG based biometric authentication, IEEE-BTAS, pp. 1-8, 2019.
25. M. Komeili, W. Louis, N. Armanfard and D. Hatzinakos, Feature selection for nonstationary data: Application to human recognition using medical biometrics, IEEE Trans. Cybern., vol. 48, no. 5, pp. 1446-1459, 2018.
26. Y. Chu, H. Shen and K. Huang, ECG authentication method based on parallel multi-scale one-dimensional residual network with center and margin loss, IEEE Access, vol. 7, pp. 598-607, 2019.
27. Y. Li, Y. Pang, K. Wang and X. Li, Toward improving ECG biometric identification using cascaded convolutional neural networks, Neurocomputing, vol. 391, pp. 83-95, 2020.
28. Yildirim Ö. A novel wavelet sequence based on deep bidirectional LSTM network model for ECG signal classification. Comput. Boil. Med. 2018, 189–202.
29. Belo D., Bento N., Silva H., Fred A., ECG Biometrics Using Deep Learning and Relative Score Threshold Classification. Sensors 2020, 20, 4078.
30. Liu X., Si Y., Yang W., A Novel Two-Level Fusion Feature for Mixed ECG Identity Recognition. Electronics 2021, 10, 2052.
31. Byeon Y.H., Pan S.B., Kwak K.C., Intelligent Deep Models Based on Scalograms of Electrocardiogram Signals for Biometrics. Sensors 2019, 19, 935.
32. Chee K.J., Ramli D.A., Electrocardiogram Biometrics Using Transformer's Self-Attention Mechanism for Sequence Pair Feature Extractor and Flexible Enrollment Scope Identification. Sensors. 2022 Apr 30; 22(9):3446.
33. Majeed R.R., Alkhafaji S.K.D., ECG classification system based on multi-domain features approach coupled with least square support vector machine (LS-SVM). Comput Methods Biomech Biomed Engin. 2022 May 13, pp.1-8.

Беляева К. В. Паттерн проектирования для разработки веб-приложений – BFF // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 86–89

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.415.25

ПАТТЕРН ПРОЕКТИРОВАНИЯ ДЛЯ РАЗРАБОТКИ ВЕБ-ПРИЛОЖЕНИЙ – BFF

Беляева К. В.
РТУ МИРЭА – Российский технологический университет, Москва, Россия(119454, Москва, пр. Вернадского, 78), e-mail: kaleriaa@bk.ru

Статья посвящена описанию взаимодействия программ между собой посредством API. С усложнением бэкенда, то есть использование микросервисного подхода, появляются трудности, так как фронтенду необходимо запоминать API каждого микросервиса. Для решения проблемы существует паттерн проектирования для разработки веб-приложений Backend for Frontend (BFF), который описан в данной статье, а также немного затронут паттерн API Gateway.Ключевые Социотехническая система, идентификация кластеров и анализ устойчивости, нечеткая когнитивная модель, нечеткое отношение взаимовлияния.

Ключевые слова: Паттерн, backed for frontend, веб-разработка, интерфейс, фронтенд, бэкенд, API, Gateway.

PATTERN FOR DEVELOPING BACKEND FOR FRONTEND (BFF) WEB APPLICATIONS

Belyaeva K. V.
RTU MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadsky Ave., 78), e-mail: kaleriaa@bk.ru

The article is devoted to the description of the interaction of programs with each other through the API. With the complication of the backend, that is, the use of a microservice approach, difficulties arise, since the frontend needs to remember the API of each microservice. To solve the problem, there is a design pattern for developing Backend for Frontend (BFF) web applications, which is described in this article, and the API Gateway pattern is also slightly affected.

Keywords: pattern, backed for frontend, web development, interface, frontend, backend, API, Gateway.

В современном мире, где технологии развиваются стремительно, каждый третий человек использует информационные технологии в работе и повседневной жизни. С каждым днем появляются новые сервисы, разрабатываются новый функционал и обновляются приложения. По данным Росстата 85% жителей России используют интернет ежедневно. Служба веб-аналитики StatCounter опубликовала рейтинг популярности браузеров за 2022 год. Чаще остальных используют Google Chrome (66,64%), на втором месте Microsoft Edge (10,07%), на третьем – Safari от Apple (9,61%). Результат исследований подтверждает тот факт, что интернет является неотъемлемой частью жизни человека.

Огромное количество веб-сервисов и ресурсов покрывают разные потребности, но, к сожалению, удовлетворить абсолютно все нужды не представляется возможным с экономической и технической точки зрения. Так, благодаря API новые приложения

интегрируются с существующими программными системами, что, в конечном итоге, увеличивает скорость разработки, потому что каждую функцию не требуется писать самостоятельно с нуля. API (Application Programmable Interface) – это программный интерфейс, который позволяют двум программным компонентам взаимодействовать друг с другом, используя набор определений и протоколов. В определении API интерфейс можно рассматривать как контракт между двумя программами, которая одна предоставляет другой.

Так, к примеру, система метеослужбы содержит ежедневные данные о погоде. Приложение погоды на телефоне или интегрированное на главную страницу браузера «обменивается» с этой системой через API и показывает ежедневные обновления погоды на телефоне. API позволяет настроить как разные компоненты программы должны эффективно взаимодействовать и используется повсеместно, что показывает важность данной технологии.

Современные веб-приложения реализуются с помощью графического интерфейса (фронтенда), с которым взаимодействует пользователь, и бэкенда, который скрыт от конечного пользователя и обеспечивает работу всего приложения, обрабатывая запросы от «клиента» и производя соответствующие действия.

В настоящее время частой практикой является разбиение приложения на отдельные небольшие приложения с ограниченной функциональностью – микросервисы, которые реализуют микросервисную архитектуру. Так, изначально данный подход использовали только на стороне бэкенда, но вскоре был реализован и на стороне фронтенда.

Среди многочисленных плюсов миркосервисной архитектуры есть и минусы, один из которых: каждый микросервис реализует уникальный программный интерфейс, поэтому фронтенд должен знать о каждом API, в связи с этим образуется жесткая сцепка между двумя сторонами. Также со стороны сервера могут поступать данные, не подходящие под нужды «клиента», допустим нефильтрованные данные, следовательно, браузер должен затратить больше ресурсов.

Решением данной проблемы является создание единого программного интерфейса, который будет знать о всех микросервисах, а также вынести несложную логику на отдельный уровень, которая обеспечивает контроль над данными. Этим промежуточным уровнем является BFF [3].

Backend for Frontend (BFF) – паттерн проектирования для разработки веб-приложений, основанный на идее API Gateway (единое окно), был разработан в компании SoundCloud. Gateway также является паттерном, так, оба этих шаблона используют один контракт для доступа к разным API. BFF используют в случаях, когда необходимо получать доступ от разных API и когда реализованы микросервисы.

Возможности BFF [4]:

- взаимодействовать с микросервисами и получать от них данные;
- преобразовать данные в соответствии с необходимым представлением;
- отправлять данные «клиенту».

Традиционный подход использует один gateway для всех «клиентов». Благодаря BFF покрываются потребности каждого «клиента», к примеру, мобильного, десктопного приложений, веб-сайта и т.д., так как возможно создать API для каждого. То есть возможность поддерживать несколько BFF позволяет избавиться от ограничений бэкенда и от хранения всего в одном месте. В связи с этим упрощается разработка сервисов, работающих с разными «клиентами».

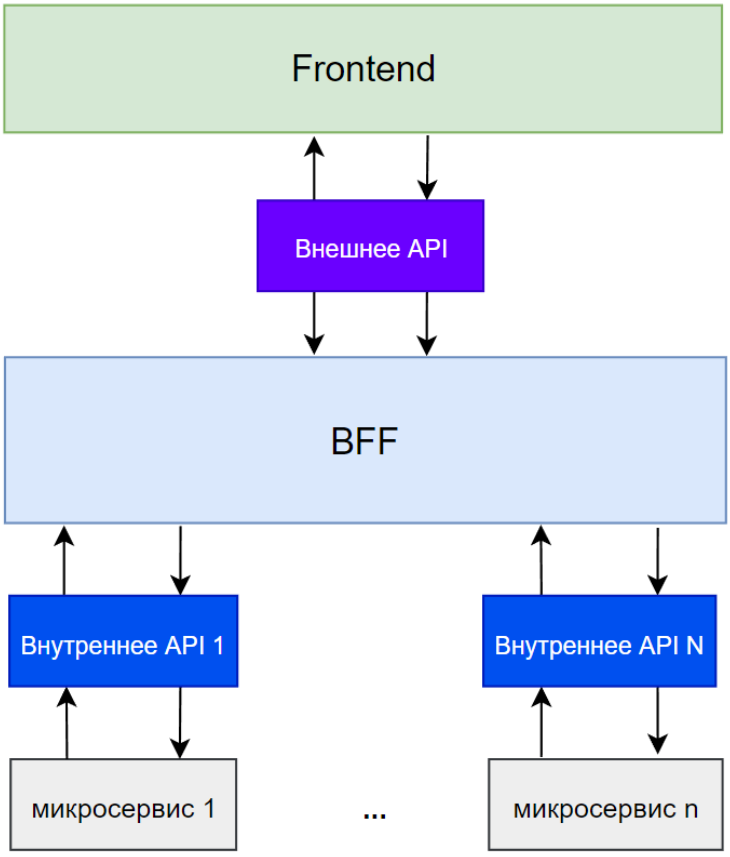


Рисунок 1 – Pattern Backend for Frontend

На рисунке 1 схематически изображен паттерн Backend for Frontend, который является промежуточным слоем между фронтендом и бэкендом, реализованным с помощью микросервисов.

Единое окно должно обеспечивать покрытие следующих требований [6]:

- высокую скорость ответа под нагрузкой;
- единый язык программирования, используемый на фронтенде и сервере BFF;
- единые шаблоны на «клиенте» и сервере.

Стоит отметить, что BFF должен быть реализован как простой интерфейс между фронтендом и бэкендом. Главным приоритетом является обмен данных.

Преимущества паттерна [5]:

- проще поддерживать и модифицировать API;
- бизнес-логика выносится на отдельный уровень;
- параллельно несколько «клиентов» могут обращаться к серверной части, что позволяет обслуживать сразу веб-сервисы и мобильные устройства, удерживая высокий уровень ответа;
- улучшенный пользовательский опыт – BFF обрабатывает ошибки сервера так, чтобы они были понятны пользователю;
- бэкенд разрабатывается на основе продукта;
- ускорение разработки.

Для того, чтобы паттерн приносил пользу, а не был во вред, необходимо понимать, в каких случаях приемлемо применять данную технологию. Ниже представлены основные критерии:

- на стороне бэкенда используется микросервисная архитектура;
- есть необходимость обслуживать несколько типов «клиентов» (мобильные, веб-приложения и т.д.);
- «клиенту» необходимо использовать данные, агрегирующиеся на стороне сервера.

Паттерн проектирование Backend for Frontend своеобразный переводчик между фронтендом и бэкендом, позволяющий облегчить и ускорить разработку, а также улучшить пользовательский опыт. Однако, не во всех случаях необходимо использовать данный стиль, так что перед решением внедрить, следует определить цели и понять, какие проблемы можно решить, применяя данный шаблон.

Список литературы

1. Что такое API? // AWS Amazon [Эл. ресурс]. URL: https://aws.amazon.com/ru/what-is/api/ (дата обращения: 25.11.2022).
2. Что такое API? // Habr URL: https://habr.com/ru/post/464261/ (дата обращения: 25.11.2022).
3. Паттерны Gateway и BFF // Дока URL: https://doka.guide/tools/gateway-bff/ (дата обращения: 26.11.2022).
4. Backend for Frontend BFF // Medium URL: https://medium.com/mobilepeople/backend-for-frontend-pattern-why-you-need-to-know-it-46f94ce420b0 (дата обращения: 26.11.2022).
5. The BFF Pattern (Backend for Frontend BFF) // Bits URL: https://blog.bitsrc.io/bff-pattern-backend-for-frontend-an-introduction-e4fa965128bf (дата обращения: 26.11.2022).
6. Backend for Frontend BFF: когда простого API не хватает // Habr URL: https://habr.com/ru/post/557406/ (дата обращения: 26.11.2022).

References

1. What is an API? // AWS Amazon [Email] resource]. URL: https://aws.amazon.com/en/what-is/api/ (Accessed 11/25/2022).
2. What is an API? // Habr URL: https://habr.com/ru/post/464261/ (date of access: 11/25/2022).
3. Gateway and BFF Patterns // Doka URL: https://doka.guide/tools/gateway-bff/ (accessed 11/26/2022).
4. Backend for Frontend BFF // Medium URL: https://medium.com/mobilepeople/backend-for-frontend-pattern-why-you-need-to-know-it-46f94ce420b0 (accessed 11/26/2022) .
5. The BFF Pattern (Backend for Frontend BFF) // Bits URL: https://blog.bitsrc.io/bff-pattern-backend-for-frontend-an-introduction-e4fa965128bf (accessed 11/26/2022).
6. Backend for Frontend BFF: when a simple API is not enough // Habr URL: https://habr.com/ru/post/557406/

Латыпов И.Р., Владимиров А.Е. Параллельная передача звука и изображения с использованием ЧМ модуляции // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 90–94

Международный журнал информационных технологий и энергоэффективности

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

УДК 621.376.3

ПАРАЛЛЕЛЬНАЯ ПЕРЕДАЧА ЗВУКА И ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЧМ МОДУЛЯЦИИ

[1] Латыпов И. Р., [2] Владимиров А.Е.
МИРЭА – Российский технологический университет, Москва, Россия (119454 г. Москва, проспект Вернадского, д. 78), e-mail: [1] latipov.ildar2015@yandex.ru, [2] leha.vladimirov.99@mail.ru

Данная статья иллюстрирует процесс разработки ЧМ передатчика изображения и звука в программном инструментарии Matlab. Важная цель работы – разработать устройство параллельного приёма и передачи в среде Simulink программы Matlab.

Ключевые слова: Matlab; Simulink; программно определяемое радио.

PARALLEL SOUND AND IMAGE TRANSMISSION USING FM MODULATION

[1] Latypov I.R., [2] Vladimirov A.E.
MIREA - Russian Technological University, Moscow, Russia 119454 Moscow, Vernadsky Avenue, 78, e-mail: [1] latipov.ildar2015@yandex.ru, [2] leha.vladimirov.99@mail.ru

This article illustrates the process of developing an FM image and sound transmitter in the Matlab software toolkit. An important goal of the work is to develop a device for parallel reception and transmission in the Simulink environment of the Matlab program.

Keywords: Matlab; Simulink; software-defined radio.

Введение

В настоящее время существует необходимость в создании современной системы информационного обслуживания, основанной на современной технологической основе и современных информационно-коммуникационных технологиях. Какую бы сферу жизнедеятельности человека мы не взяли: биологию, медицину, архитектуру, машиностроение, образование – без применения компьютерных технологий нигде в современном мире не обходится. Для каждой из этих областей разрабатываются соответствующие программы. И радиотехника не является исключением, на сегодняшний день вопрос об интеграции программирования и радиоэлектронной аппаратуры стал очень актуальным.

Рассматриваемым объектом исследования данной статьи является применение использование программно определяемого радио в решении радиотехнических задач, а именно разработка программно-конфигурируемого QPSK-приемника телеизображений.

Используемое оборудование

В ходе составления статьи в качестве передатчика автор выбрал программно определяемое радиоустройство USRP-2901 – настраиваемый ВЧ приемопередатчик с полным дуплексом и многоканальным вводом выводом (MIMO). Он обеспечивает связь и питание по шине USB 3.0 или USB 2.0. В качестве приёмника использовалось программно определяемое радиоустройство RTL-SDR 2832 U – радиосканер на базе однокристального тюнера RTL2832 [1]. В качестве приёмной и передающей антенн были использованы две всенаправленные антенны на магнитной основе.

Используемое программное обеспечение

Для построения функциональной схемы устройства использовалась среда визуально ориентированного программирования Simulink. которая является средой графического программирования на основе MATLAB для моделирования и анализа динамических систем. Его основной интерфейс представляет собой среду визуально-ориентированного программирования для построения блок-схем и настраиваемая библиотека блоков и инструментов для разработки. Он предлагает тесную интеграцию со средой программирования MATLAB и может либо управлять ею, либо работать с заранее прописанным в нем сценарии. Simulink широко используется в автоматическом управлении и цифровой обработке сигналов для моделирования и проектирования различных моделей. В сочетании с другими своими продуктами Simulink может автоматически генерировать исходный код на языке C для реализации систем в режиме реального времени[4].

Функциональные схемы в Simulink

В процессе разработки были разработаны функциональные схемы приёмника и формирования общего сигнала для передачи звука и изображения в среде SIMULINK. Разберем принцип работы схемы преобразования, выполненного в среде визуально-ориентированного программирования, приведённого на рисунке 1.

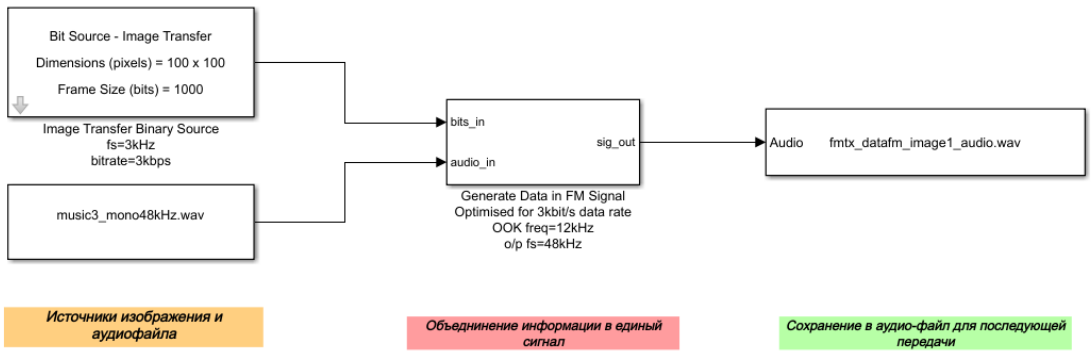


Рисунок 1 – Схема преобразования изображения и аудиофайла в единый сигнал.

В начале через блоки источника бинарного кода и источника аудиофайла задаются изображение и звук которые в дальнейшем будут объединены в единый сигнал. Далее идёт блок генерации единого битового потока, внутри которого изображение, преобразованное в бинарный код, примешивается к звуку, также преобразованному в бинарный код. В результате данных операций мы получаем аудиофайл, внутри которого помимо звука также хранится информация о изображении. Далее по средствам стандартной схемы передатчика сигнал передается на частоте 100 МГц [2].

После передачи сигнал принимается с помощью схемы приемника, также реализованной в среде визуально ориентированного программирования Simulink программы Matlab. Давайте поподробнее разберем принцип работы данной схемы, представленной на рисунке 2.

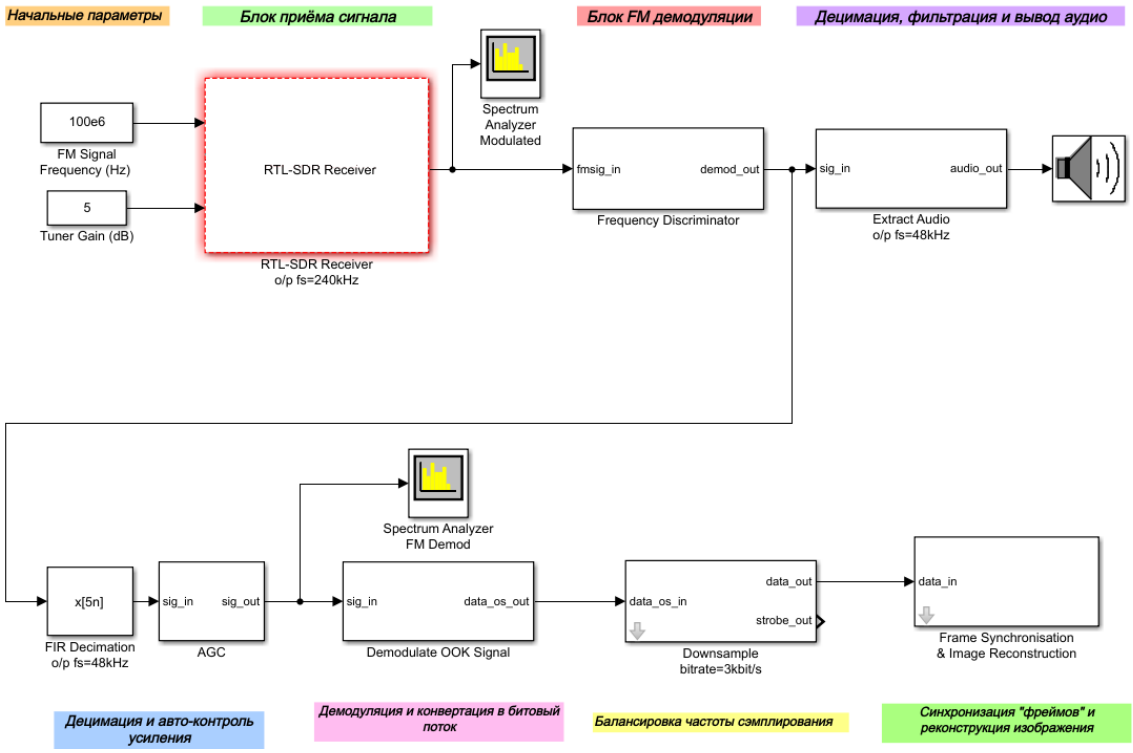


Рисунок 2 – Схема приёма и обработки сигнала.

В начале идут блоки задания начальных параметров сигнала, частоты на которой будет осуществляться приём и усиления в децибелах. Далее идёт блок программно определяемого приёмника с заданной частотой семплирования 240 килогерц, после этого сигнал разветвляется на блок анализатор спектра и на блок FM демодуляции [3]. После этого сигнал разветвляется на блок децимации, фильтрации и дальнейшего вывода аудио с частотой семплирования 48 килогерц, а также на цепочку блоков децимации и автоматического контроля усиления [4]. Далее сигнал попадает на блок анализатора спектра и на блок демодуляции и конвертации сигнала в битовый поток для дальнейшей обработки. После этого сигнал попадает на блок балансировки частоты семплирования, далее обработанный сигнал попадает на блок синхронизации «фреймов» и реконструирования изображения. В ходе проведения модуляции была проверена стабильность работы разработанной схемы, и получены определенные результаты.

Полученные результаты.

В ходе проведения модуляции была получена спектрограмма сигнала до FM демодуляции представленная на рисунке 3.

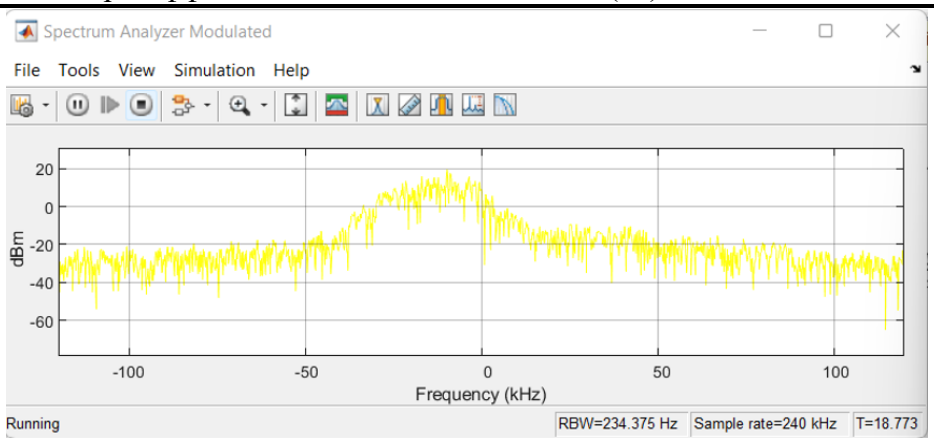


Рисунок 3 – Спектрограмма сигнала до FM демодуляции.

А также спектрограмма сигнала после FM демодуляции представленная на рисунке 4.

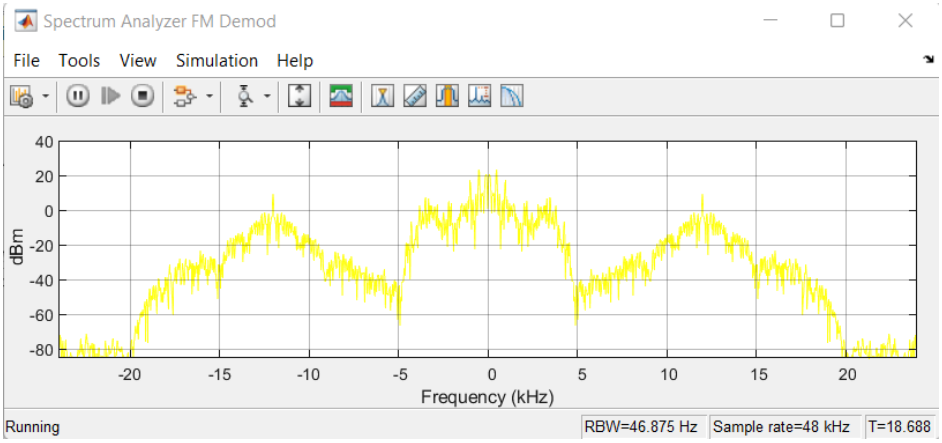


Рисунок 4 – Спектрограмма сигнала после FM демодуляции.

Было получено реконструированное изображение, представленное на рисунке 5.

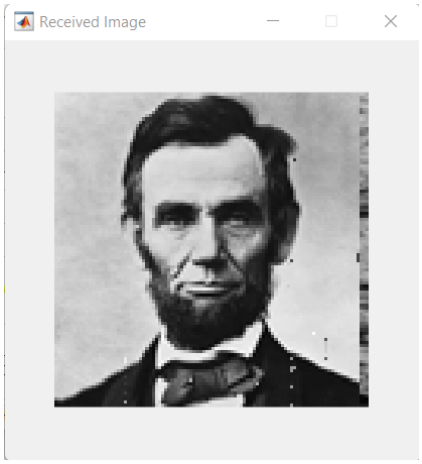


Рисунок 5 – Принятое и реконструированное изображение.

Список литературы

1. Костин М.С., Ярлыков А.Д. Архитектурно-конфигурируемые SDR-технологии радиомониторинга и телеметрии: учебное пособие. – Москва; Вологда: Инфра-Инженерия, 2021. – 148 с.
2. Хемминг Р.В. «Цифровые фильтры» Пер. с англ./Под ред. А.М.Трахтмана. -М.: Сов.радио,1980. – 224 с.
3. Бессалов Анатолий, Основы теории информации и кодирования / Анатолий Бессалов. - М.: Palmarium Academic Publishing, 2014. -280 с.
4. Скляр, Бернард. Цифровая связь. Теоретические основы и практическое применение: пер. с англ. / Бернард Скляр. - Изд. 2-2, испр. - М.: Издательский дом "Вильямс", 2003. – 1104 с.

References

1. Kostin M.S., Yarlykov A.D. Architecturally configurable SDR technologies for radio monitoring and telemetry: a tutorial. - Moscow; Vologda: Infra-Engineering, 2021. - 148 p.
2. Hemming R.V. "Digital filters" Per. from English / Ed. A.M. Trakhtman. -M.: Sov.radio, 1980. – 224 p.
3. Bessalov Anatoly, Fundamentals of information theory and coding / Anatoly Bessalov. - M.: Palmarium Academic Publishing, 2014. -280 p.
4. Sklyar, Bernard. Digital communication. Theoretical foundations and practical application: Per. from English. / Bernard Sklyar. - Ed. 2-2, rev. - M.: Williams Publishing House, 2003. - 1104 p..

Латыпов И.Р., Владимиров А.Е. Автоматизированная система эхолота. Разработка и анализ // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 95–99

Международный журнал информационных технологий и энергоэффективности

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

УДК 62

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ЭХОЛОТА. РАЗРАБОТКА И АНАЛИЗ.

[1] Латыпов И. Р., [2] Владимиров А.Е.
МИРЭА – Российский технологический университет, Москва, Россия (119454 г. Москва, проспект Вернадского, д. 78), e-mail: [1] latipov.ildar2015@yandex.ru, [2] leha.vladimirov.99@mail.ru

Данная статья отражает процесс разработки и анализа автоматизированной системы эхолота. Основная цель задачи разработчика - разработка прибора, превосходящего аналогичные устройства по характеристикам массы, габаритов и стоимости, дополнительным требованием для разрабатываемого устройства является новизна и актуальность элементной базы

Ключевые слова: Эхолот, автоматизированная система, гидроаккустика.

AUTOMATED SONAR SYSTEM. DEVELOPMENT AND ANALYSIS

[1] Latypov I.R., [2] Vladimirov A.E.
MIREA - Russian Technological University, Moscow, Russia (119454 Moscow, Vernadsky Avenue, 78), e-mail: [1] latipov.ildar2015@yandex.ru, [2] leha.vladimirov.99@mail.ru

This article reflects the process of development and analysis of an automated echo sounder system. The main goal of the developer's task is to develop a device that exceeds similar devices in weight, size and cost, an additional requirement for the device being developed will be the novelty and relevance of the element base.

Keywords: Automated syste, echo sounder, hydroacoustics.

Эхолоты - это устройства, которые имеют огромное множество применений. Например, обрисовка топографических карт дна моря, вычисление высоты столба воды под судном. Также эхолоты применяются в профессиональной и любительской рыбалке для определения местоположения и глубины скопления косяков рыбы в водоеме .

Во всех без исключения эхолотах используется метод гидроакустического анализа. Иными словами, эхолот формирует и излучает звуковые волны в жидкость для сканирования объектов и определения их характеристик. Звуковые волны используются неспроста. Их применение обусловлено тем, что в настоящее время данный тип волн являются единственным, который может излучаться и передаваться без критического ослабления сигнала как в пресной, так и в морской воде. Именно свойство звуковых волн распространяться как в пресной, так и в солёной воде без существенного ослабления оказывается принципиальным преимуществом перед использованием радиоволн или света.

Разрабатываемое устройство будет функционирует по принципу двухлучевого сканирования. Данный метод представляет собой датчик гидролокатора (гидрофона) который

излучает два конусных луча, расположенных внутри друг друга. Первый имеет большую частоту и меньший угол обзора, а второй обладает меньшей частотой и большим углом обзора. Для максимального захвата объекта используется широкий луч. Первоначальное сканирование водоема осуществляется широким лучом, а после обнаружения интересующего объекта эхолот переключается на более узкий луч, обеспечивающий лучшую детализацию.

Принцип эксплуатации и назначение прибора

Данный прибор является многофункциональном блоком эхолота и предназначен для первичной обработки сигналов (усиления, фильтрации, а также оцифровки), полученных от гидрофона и дальнейшей передачи на ЭВМ [4, с.24].

Оборудование относится к классу морской аппаратуры и эксплуатируется в погодных зонах с умеренным климатом для эксплуатации на открытом воздухе (под влиянием всех атмосферных факторов). Рабочее значение температуры воздуха при эксплуатации составляет от -50 до +45 °С. Относительная влажность воздуха до 100% при температуре +25 °С.

Аналоги устройства и их анализ

На сегодняшний день существует огромное множество как любительских, так и профессиональных приборов. Выполним разбор имеющихся на сегодняшний день аналогичных эхолотов. Функционал большинства устройств можно поделить на две группы: первые работают только с одним спектром частот, а вторые - с несколькими спектрами частот. Ближайшим аналогом устройства является Garplin GLS-11 [4].

Фундаментальной задачей при разработке приемного устройства эхолота является изменение и доработка конструкторских и технологических параметров устройства.

Основой для разработки конструкции приемного устройства эхолота является электрическая принципиальные схема МРАГ.466333.001 Э3 (рисунок 1) и перечень элементов МРАГ.466333.001 ПЭ3.

Главной целью анализа схемы электрической принципиальной устройства является проверка всех входящих в схему элементов, на соответствие требованиям исходного задания.

Полный список элементов представлен в перечне МРАГ.466333.001 ПЭ3. Все конструктивные элементы, вошедшие в данный перечень, соответствуют исходным требованиям данных.

Приемное часть прибора собрана по известной схеме прямого усиления. Биполярные транзисторы VT1, VT2 усиливают эхосигнал, полученный датчиком- излучателем BQ1, биполярный транзистор VT3 используется как амплитудный обнаружитель, а биполярный транзистор VT4 усиливает обнаруженный сигнал. На транзисторах VT5, VT6 собран одновибратор, позволяющий поддерживать постоянство выходных параметров импульсов и порога чувствительности приемной части прибора. Для защиты приемника от импульса передатчика применяют диодный ограничитель (VD1, VD2) и токоограничивающий резистор R1.

В приемном части транзистор VT7 выполняет вынужденное выключение одновибратора. Зарядка конденсатора C8 происходит благодаря короткому положительному тактовому импульсу с транзистора через диод VD3. Транзистор VT7, постепенно открываясь, подключает базу транзистора VT5 с плюсовым проводом питания, исключая тем самым возможность его срабатывания от ложных импульсов [3, с.240]. По окончании тактирующего импульса конденсатор C8 разряжается через резистор R18, а транзистор VT7 постепенно начинает призакрываться, и одновибратор приемной части получает приемлемую

чувствительность. На микроконтроллерах DD1-DD4 выполнена цифровая часть прибора. Ключевой элемент DD1.1, управляется с помощью триггеров на элементах DD1.3, DD1.4. Начальный импульс счета попадает в триггер от модулятора передающей части через биполярный транзистор VT16, импульс окончания счета попадает с выхода приемного устройства проходя через биполярный транзистор VT15 [1, с.325].

Частотный генератор импульсов с частотой повторения (7500 Гц) выполнен на элементе DD1.2. Из катушки индуктивности L1 и резистора R33 составлена схема с ООС (отрицательной обратной связью), позволяющий выйти элементу на линейную характеристику, что порождает процесс самовозбуждения на частотах, определяемой параметрами контура L1C18 цепочки. На точно заданную частоту генератор подстраивают подстрочником катушки LC цепи.

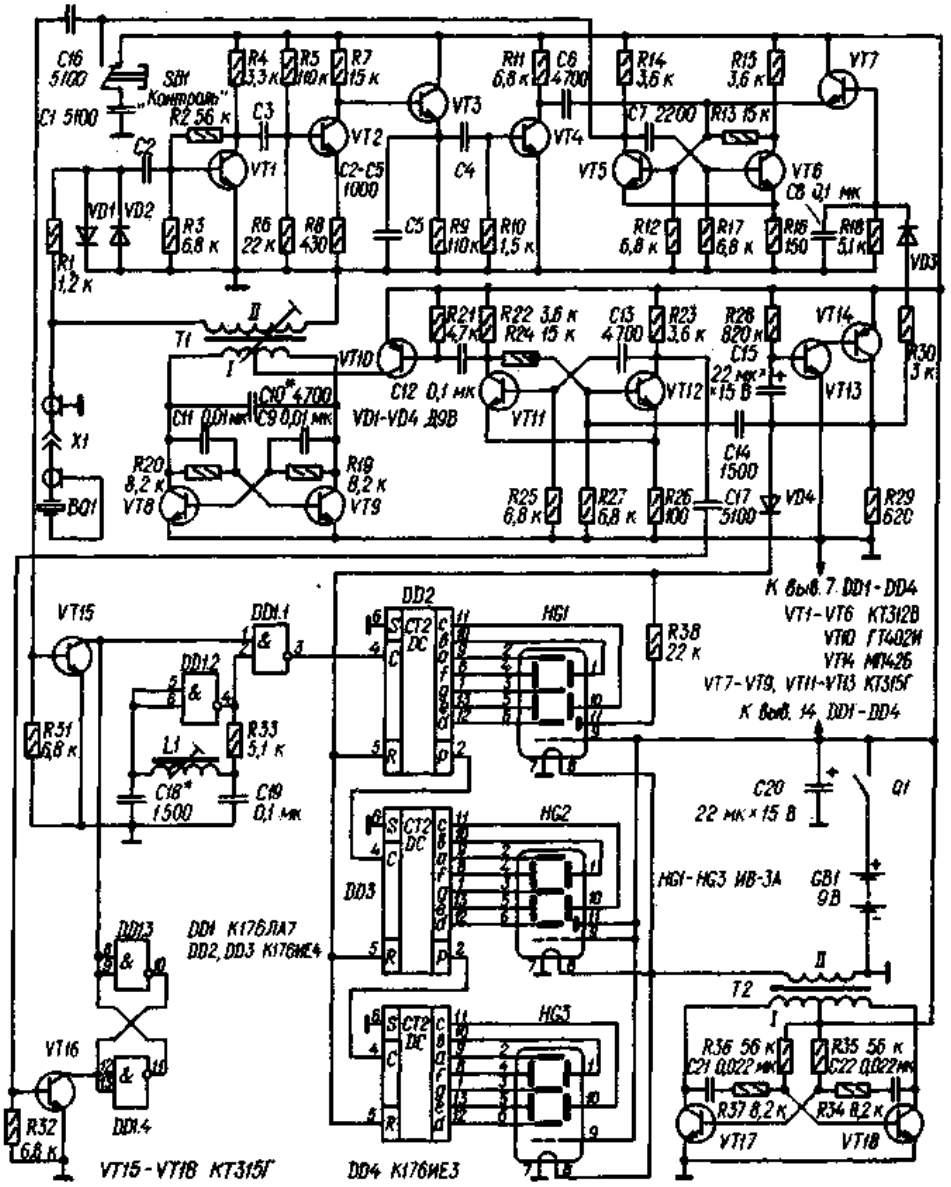


Рисунок 1 – Функциональная схема устройства

Принцип работы прибора и его описание

Приемная часть прибора эхолота состоит из пяти функциональных частей, связанных между собой: блока питания, усилителя, двух активных полосовых фильтров, которые выполняют фильтрацию входящих сигналов в двух различных диапазонах частот, а также аналогово-цифрового преобразователя (АЦП).

На приемную часть устройства эхолота от гидрофона поступает сигнал, который впоследствии усиливается при помощи блока усиления. После этого усиленный сигнал попадает на блок фильтрации, выполненный из двух активных полосовых фильтров. Затем отфильтрованный сигнал поступает на АЦП, который преобразует аналоговый сигнал в цифровой и передает его на ЭВМ.

Прибор для своей работы требует двухполярное питание +15 В и -15 В, а максимально потребляемый ток составляет 0,1 А. В приборе имеется преобразователи и стабилизаторы напряжение необходимых значений.

Схема функциональная прибора

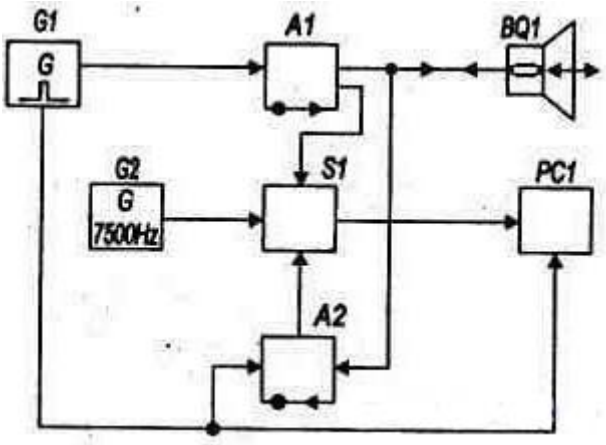


Рисунок 2 – Схема функциональная прибора

Генератор тактов отвечает за правильную автоматическую работу прибора. С его выхода поступают импульсы (0.1 с.) с периодом в 15 секунд, которые имеют прямоугольную форму и с помощью фронта, переключают PC1 (цифровой счетчик) в логический ноль. Как следствие, A2 (приемник) перекрывается и больше не реагирует на внешние сигналы. После этого, включается A1 (передатчик) и BQ1 (излучатель) излучает ультразвуковой импульс. Вместе с выходным излучением в открытое состояние переходит S1 (ключ), и колебания от G2 (генератор) подаются на PC1. Как только A1 завершает свою работу, A2 обретает чувствительность. Отражающийся сигнал, в виде эха, вернется к BQ1 и закроет S1[2, с.76]. После этого процесс измерения можно назвать законченным. Индикатор PC1 показывает клиенту глубину толщи воды. Если сигнал отразится, например, от рыбы, то индикатор покажет меньшую глубину. Именно таким образом и проверяется дно на наличие рыбы [3, с 15].

Заключение

В данной статье приводится теоретическое исследование изделия предназначенного для сканирования дна на наличие рыбы в водоеме или для построения подводной картографии с помощью сигналов от датчиков, которые обрабатываются аналогово-цифровым преобразователем для передачи информации на дисплей пользователя. Также рассмотрена схема электрическая принципиальная и изучен принцип работы прибора.

Список литературы

1. Конструирование узлов и устройств электронных средств: учебное пособие / Д.Ю. Муромцев, И.В. Тюрин, О.А. Белоусов. –Ростов н/Д.: Феникс, 2013. – 540 с.
2. Датчики: Справочное пособие / В.М. Шарапов, Е.С. Полищук, Н.Д. Кошевой, Г.Г. Ишанин, И.Г. Минаев, А.С. Совлуков. - Москва: Техносфера, 2012. – 617 с.
3. Волков Ю.В. Датчики для измерений при производстве электрической и тепловой энергии: учебное пособие / ВШТЭ СПбГУПТД. СПб., 2019 – 89 с.: ил. 64 – ISBN 978-5-91646-188-6.
4. Завьялов, В. В. Судовые навигационные эхолоты. В 2 ч. Ч. I. Теория. [Текст] : учеб. пособие / В. В. Завьялов, В. Ф. Полковников, А. И. Саранчин. – Владивосток : Мор. гос. ун-т, 2012 – 93 с.

References

1. Designing components and devices of electronic means: study guide / D.Yu. Muromtsev, I.V. Tyurin, O.A. Belousov. - Rostov n / D .: Phoenix, 2013. - 540 pp.
2. Sensors: Reference manual / V.M. Sharapov, E.S. Polishchuk, N.D. Koshevoy, G.G. Ishanin, I.G. Minaev, A.S. Sovlukov. - Moscow: Technosphere, 2012 – 617 pp.
3. Volkov Yu.V. Sensors for measurements in the production of electrical and thermal energy: textbook / VSTE SPbGUPTD. St. Petersburg, 2019 - 89 p.: ill. 64 - ISBN 978-5-91646-188-6.
4. Zavyalov, VV Ship navigation echo sounders. At 2 pm Part I. Theory. [Text]: textbook. allowance / V. V. Zavyalov, V. F. Polkovnikov, A. I. Saranchin. - Vladivostok: Mor. state un-t, 2012 - 93 pp.

Руденко Н.В. Характеристики дорожного движения по автомобильным дорогам и методы оценки безопасности дорожного движения // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 100–106

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.94

ХАРАКТЕРИСТИКИ ДОРОЖНОГО ДВИЖЕНИЯ ПО АВТОМОБИЛЬНЫМ ДОРОГАМ И МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ ДОРОЖНОГО ДВИЖЕНИЯ

Руденко Н.В.
Военная академия материально- технического обеспечения им. генерала армии А.В. Хрулёва, Санкт-Петербург, Россия (199034, Санкт-Петербург, наб. Макарова, 8), e-mail: ask.dying@mail.ru

В статье проведен анализ характеристик дорожного движения по автомобильным дорогам и рассмотрены методы оценки безопасности дорожного движения. Актуальность работы заключается в том, что в наше время растет количество участников дорожного движения, а следовательно возрастает и актуальность таких вопросов, как повышение безопасности движения на автомобильных дорогах.

Ключевые слова: Анализ, безопасность дорожного движения, автомобильные дороги, организация движения, аварийность.

ROAD TRAFFIC CHARACTERISTICS AND METHODS FOR ASSESSING ROAD SAFETY

Rudenko N.V.
Military Academy of Logistics named after. Army General A.V. Khruleva, St. Petersburg, Russia (199034, St. Petersburg, emb. Makarova, 8), e-mail: ask.dying@mail.ru

The paper analyzes the characteristics of road traffic on highways and considers methods for assessing road safety. The relevance of the work lies in the fact that nowadays the number of road users is growing, and therefore the relevance of issues such as improving traffic safety on highways is also increasing.

Keywords: Analysis of characteristics, road safety, highways, traffic management, accident rate.

Исходным пунктом поиска мер по обеспечению безопасности движения следует считать появление первого газового уличного светофора в Лондоне 10 декабря 1868 г.

С тех пор было разработано много теоретических и практических методов повышения безопасности дорожного движения [1-7], которые основываются на анализе безопасности системы «водитель- автомобиль – дорога» и предназначены для повышения безопасности движения одиночных транспортных средств по автомобильным дорогам в условиях мирного времени (рисунок 1).

Среди методов оценки безопасности дорожного движения следует выделить [7-10]: метод коэффициентов аварийности; метод коэффициентов безопасности; метод шума ускорений; метод частных коэффициентов относительной безопасности; метод конфликтных ситуаций; методы оценки геометрических и технических характеристик дороги; методы оценки профессиональных и психофизиологических качеств водителей; документальное изучение

статистики ДТП и материалов обследования дорог; исследование транспортных и пешеходных потоков, метод оценки дорожных и природно-климатических факторов и др.

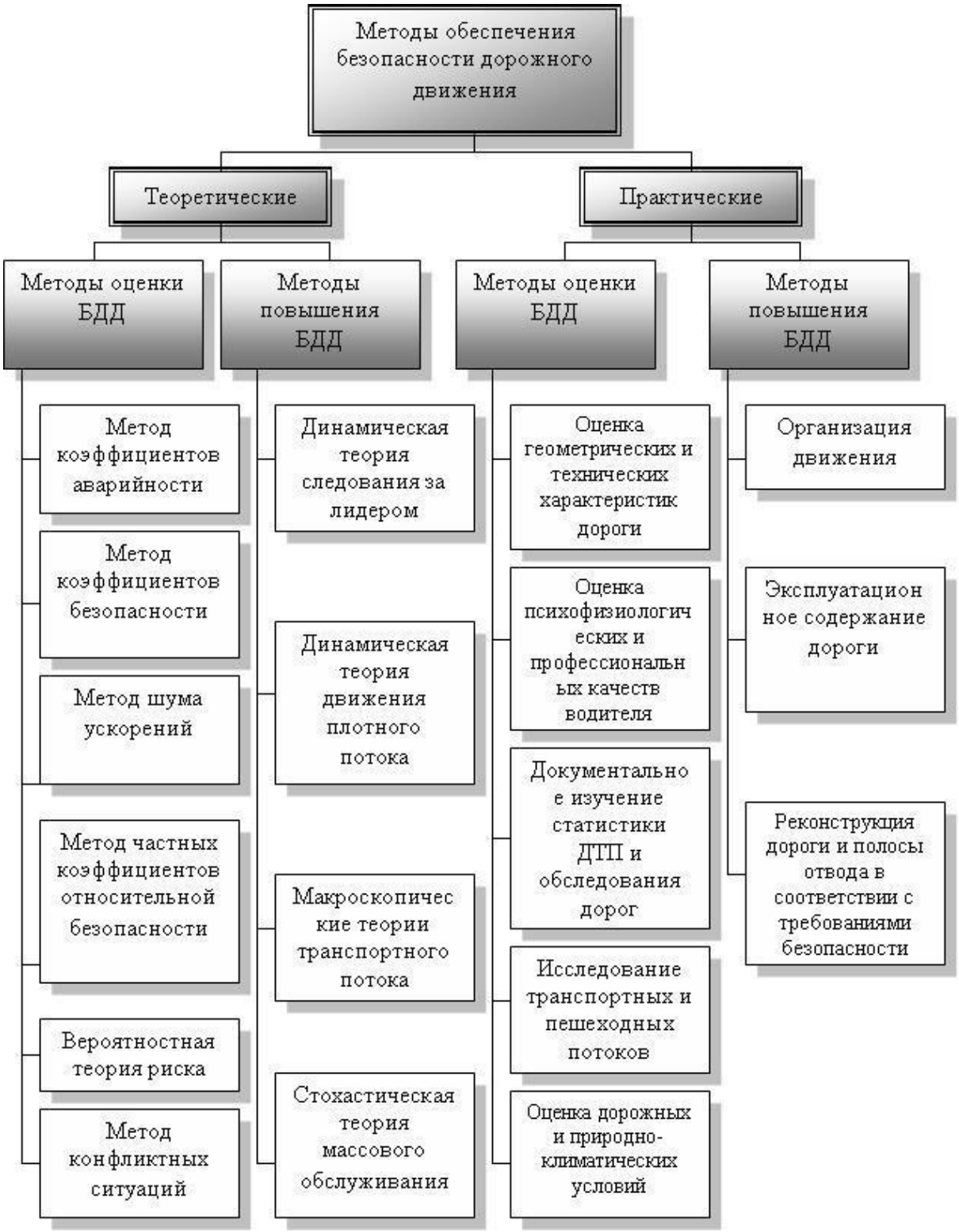


Рисунок 1 – Классификация методов обеспечения безопасности дорожного движения мирного времени

Метод коэффициентов аварийности

Сущность метода заключается в нахождении итогового коэффициента аварийности для определенного участка дороги потенциированием частных коэффициентов аварийности. Частные коэффициенты определяются эмпирическим путем, причем каждый из них – для конкретных условий.

Метод позволяет просто и достаточно быстро оценить безопасность участка дороги (или дороги в целом), при известных дорожных условиях и условиях окружающей обстановки, пошагово используя имеющиеся таблицы нахождения частных коэффициентов . Метод был разработан в 60-е годы прошлого века, претерпевал изменения в 70-е и 80-е годы. С того времени существенно изменились технические и эксплутационные характеристики транспортных средств и транспортного потока, требования к безопасности дорожного движения.

Метод коэффициентов безопасности

Основан на сравнении максимальных скоростей движения на расчетном и предыдущем участке дороги. Сравнение ведется по рассчитанному коэффициенту безопасности. Считается, что если коэффициент больше или равен 1 (максимальная скорость на данном участке выше, чем на предыдущем), то данный участок безопаснее предыдущего. Однако практика показывает, что улучшение дорожных условий влечет за собой увеличение средней скорости движения потока, что не увеличивает безопасность, а снижает ее.

Метод шума ускорений

Этот метод основан на оценке степени неоднородности движения и интенсивности изменения скоростей на разных участках пути средней квадратичной величиной реализуемых водителями ускорений (сначала замедления при въезде на участок, затем разгона при выезде с него). Данный показатель называется «шумом ускорения». В связи с тем, что интенсивность торможения обычно связана со степенью опасности происшествий, предложили оценивать безопасность движения шумом ускорений.

Метод частных коэффициентов относительной безопасности

Аналогичен методу коэффициентов аварийности. Частные коэффициенты относительной безопасности учитывают влияние интенсивности, скорости движения, числа полос движения, ширину укрепляемой полосы обочин, продольного уклона, видимости встречного автомобиля, радиусов кривых в плане. Численные значения данных коэффициентов приблизительно равны обратной величине частных коэффициентов аварийности. Широкого распространения этот метод не получил, поскольку во время его разработки уже широко использовался метод коэффициентов аварийности. Частные коэффициенты относительной безопасности, полученные эмпирическим путем в 70-е годы прошлого века, не отражают существующих условий движения на автомобильных дорогах в мирное время [1].

Теория надежности (теория риска)

Применение теории риска позволяет оценить следующие параметры: вероятность (риск) наезда на впереди идущий автомобиль; интервалы между автомобилями в зависимости от риска, допускаемого водителями; вероятность (риск) столкновения при обгоне и параметры обгона; вероятность (риск) опрокидывания на кривой в плане; вероятность (риск) столкновения при въезде на автомагистраль; вероятность (риск) столкновения при пересечении главной дороги и другие характеристики опасности столкновения, наезда и опрокидывания .

Метод конфликтных ситуаций

Применим для оценки безопасности в местах и на участках, сложных для движения. Оценка уровня опасности участка осуществляется по количеству конфликтных ситуаций на 1 млн. автомобиле-километров. Метод позволяет оперативно определить уровень опасности участка дороги, если имеется накопленная статистика по конфликтным ситуациям (но не по аварийности). Однако возможность в реальных, а не смоделированных, условиях, отследить возникновение конфликтной ситуации весьма затруднительна.

Методы оценки геометрических и технических характеристик дороги

Суть этих методов заключается в измерении геометрических параметров дороги. Затем по известным формулам находятся значения допустимых скоростей и максимальных интенсивностей движения. Метод позволяет оценить безопасность движения одиночных ТС с точки зрения расположения и размеров элементов дороги и дорожного обустройства. [11]

Документальное изучение статистики ДТП и материалов обследования дорог

Проводится на основе документов ГИБДД, регистрирующих ДТП и документов организаций дорожного хозяйства. В результате их изучения находятся конфликтные точки на дорожной сети, которые затем устраняются в ходе проведения текущих и капитальных ремонтов дороги. Метод действенный, но он оценивает безопасность движения уже после совершенных ДТП.

Исследование пешеходных и транспортных потоков

При помощи подготовленных специалистов или электронных приборов проводится измерение интенсивности движения пешеходов и транспортных средств. На основе полученных данных делается вывод о необходимости управления данными потоками с помощью технических средств.

Оценка дорожных и природно-климатических условий

На основе накопленных статистических данных выводятся зависимости безопасности условий для движения транспортных средств при действии различных природных явлений: дождя, снега, тумана, ветра, гололеда, ночных условий и т.п. Полученные зависимости применяют для оценки природно-климатических и дорожных условий в реальной дорожной обстановке.

К указанной группе методов (рисунок 1) относятся: методы теории следования за лидером; методы теории массового обслуживания; методы организации дорожного движения; обустройство дороги и полосы отвода в соответствии с требованиями безопасности движения; имитационное моделирование движения для оптимизации параметров потока; устранение конфликтных точек на дороге и др.

Рассмотрим подробнее данную группу методов.

Динамическая теория следования за лидером

Теория «следования за лидером» является развитием теорий упрощенных динамических моделей. Она основана на гипотезе о существовании определенной закономерности взаимодействия автомобилей, движущихся друг за другом на близком расстоянии.

Применение теории следования за лидером позволяет получить следующие параметры: среднюю скорость и среднюю плотность транспортного потока (на каждой полосе движения); пропускную способность полос движения; скорость и плотность движения отдельных пачек (групп) автомобилей; плотность при заторе; максимальное значение плотности и минимальное значение скорости движения (при превышении максимальной плотности поток

останавливается и образуется затор); интервалы во времени между автомобилями, включая интервалы в отдельных пачках (группах) автомобилей и др.[7]

Динамическая теория движения плотного потока автомобилей

Взаимодействие между автомобилями в плотном транспортном потоке, зависящее от действий водителей, в первую очередь, проявляется в изменении дистанции между автомобилями. Поэтому первые упрощенные динамические теории были разработаны с целью возможности расчета средней дистанции между автомобилями при различных скоростях движения.

Все упрощенные динамические модели основаны на предположении о том, что автомобили движутся в потоке с одинаковой скоростью на расстоянии, достаточном для полной остановки без наезда на впереди идущий автомобиль.

Макроскопические теории транспортного потока

Поток рассматривается, как сплошная среда, состоящая из большого числа близко расположенных друг к другу автомобилей.

Для математического описания состояния движущегося потока автомобилей как сплошной среды используются следующие основные законы: уравнение состояния потока автомобилей; уравнение неразрывности; закон сохранения количества движения; закон сохранения энергии.

Теория массового обслуживания

Методы теории массового обслуживания применимы для обеспечения безопасности движения одиночных ТС (однородность заявок на обслуживание и стационарность потока).

Организация движения

Организация движения - действия органов управления движением по выполнению комплекса организационно-технических мероприятий, предусматривающих планирование, построение движения, установление допустимых скоростей и порядка пропуска участников движения, определения порядка движения в сложных местах, организацию использования запасных маршрутов и дублирующих мостовых переходов, а также другие мероприятия, в результате которых устанавливается и в дальнейшем поддерживается единый и обязательный для всех порядок движения по автомобильным дорогам, обеспечивающий максимальное использование их пропускной способности, организованность и своевременность движения.

Эксплуатационное содержание дороги

Эксплуатационное содержание заключается в выполнении необходимых работ по поддержанию эксплуатационных показателей дороги в соответствии с требованиями безопасности дорожного движения, сохранению дорог от преждевременных разрушений, предотвращению и своевременному устранению повреждений и других препятствий, вызванных движением автомобилей и природными явлениями.

Реконструкция дороги и полосы отвода в соответствии с требованиями безопасности

Широко применяется в практике дорожного строительства. Является итогом оценки безопасности методом коэффициентов аварийности, безопасности и конфликтных ситуаций. В результате оценки указанными методами выявляются участки дорог и придорожной территории, которые провоцируют или способствуют возникновению ДТП. Устранение таких участков при реконструкции дороги является одним из практических методов повышения безопасности дорожного движения.

Применение технических устройств для повышения безопасности автомобиля и дороги

В настоящее время разработаны различные технические устройства и системы для повышения активной и пассивной безопасности автомобиля: противотуманные фары и угловые фонари, антиблокировочная и антипробуксовочная системы торможения, интеллектуальная система информирования водителя, система динамической стабилизации и контроля тяги, различные датчики давления и перегрева и т.п. Их влияние на безопасность хорошо исследовано [8].

Работа выполнена под научным руководством к.т.н, проф. Никонорова А.Н.

Список литературы

1. СНиП 2.05.02-85. Автомобильные дороги. – Госстрой СССР, 1986 (1997 г.). – 51 с.
2. ГОСТ Р 50597-93. Автомобильные дороги и улицы. Требования к эксплуатационному состоянию, допустимому по условиям обеспечения безопасности движения.
3. ГОСТ Р 51256-99. Технические средства организации дорожного движения. Разметка дорожная. Типы и основные параметры. Общие технические требования.
4. ОДН 218.012.-99. Общие технические требования к ограждающим устройствам на мостовых сооружениях, расположенных на магистральных автомобильных дорогах.
5. ГОСТ Р 52289-2004. Технические средства организации дорожного движения. Правила применения дорожных знаков, разметки, светофоров, дорожных ограждений и направляющих устройств.
6. ГОСТ Р 52290-2004. Технические средства организации дорожного движения. Знаки дорожные. Общие технические требования.
7. «Технические требования к оборудованию комплексов весогабаритного контроля на автомобильных дорогах общего пользования федерального значения», Росавтодор, Исх. №01-1135 от 08.08.2013.
8. Артынов, А.П. Автоматизация управления транспортными системами / А.П. Артынов [и др.] / отв. ред. А.А. Воронов. – М., 1984. – 272 с.
9. Рэнкин, В. У. Автомобильные перевозки и организация дорожного движения: Справочник. Пер. с англ. / В.У. Рэнкин [и др.]. – М., 1981. – 592 с.
10. Бабков, В.Ф. Дорожные условия и безопасность движения: учеб. для вузов / В.Ф. Бабков. – М.: Трансп., 1993. – 271 с.
11. Беляев, Э.И. Применение современных методов оптимизации транспортной системы // Инновации в науке: Материалы науч.-практ. конф./ Э.И. Беляев, И.В. Макарова, Р.Г. Хабибуллин / под ред. Я.А. Полонского. – Новосибирск: Сибирская ассоциация консультантов, 2012. – 110 с.

References

1. SNiP 2.05.02-85. Car roads. - Gosstroy of the USSR, 1986 (1997). – 51 p.
2. GOST R 50597-93. Highways and streets. Requirements for the operational state, admissible under the terms of ensuring traffic safety.
3. GOST R 51256-99. Technical means of organizing traffic. Road marking. Types and basic parameters. General technical requirements.
4. ODN 218.012.-99. General technical requirements for fencing devices on bridge structures located on main roads.

5. GOST R 52289-2004. Technical means of organizing traffic. Rules for the use of road signs, markings, traffic lights, road barriers and guides.
6. GOST R 52290-2004. Technical means of organizing traffic. Road signs. General technical requirements.
7. "Technical requirements for the equipment of complexes of weight and size control on highways of general use of federal significance", Rosavtodor, Ref. No. 01-1135 dated 08/08/2013.
8. Artynov, A.P. Automation of transport systems management / A.P. Artynov [and others] / otv. ed. A.A. Voronov. - M., 1984. - 272 pp.
9. Rankin, VU Automobile transportation and organization of traffic: a Handbook. Per. from English. / V.U. Rankin [i dr.]. - M., 1981. - 592 pp.
10. Babkov, V.F. Road conditions and traffic safety: textbook. for universities / V.F. Babkov. - M.: Transp., 1993. - 271 pp.
11. Belyaev, E.I. Application of modern methods of optimization of the transport system // Innovations in science: Proceedings of scientific-practical. conf. / E.I. Belyaev, I.V. Makarova, R.G. Khabibullin / ed. Ya.A. Polonsky. - Novosibirsk: Siberian Association of Consultants, 2012. - 110 pp.

Липкович И.Э., Петренко Н.В., Кубак Н.А. Организационные основы безопасности работ при обслуживании подстанций и распределительных устройств // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3 (25) часть 3 с. 107–116

Международный журнал информационных технологий и энергоэффективности

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

УДК 331.45

ОРГАНИЗАЦИОННЫЕ ОСНОВЫ БЕЗОПАСНОСТИ РАБОТ ПРИ ОБСЛУЖИВАНИИ ПОДСТАНЦИЙ И РАСПРЕДЕЛИТЕЛЬНЫХ УСТРОЙСТВ

[1]Липкович И.Э., [2]Петренко Н.В., Кубак Н.А.
Азово-Черноморский инженерный институт ФГБОУ ВО Донской ГАУ в г. Зерограде, Россия (347740, г. Зерноград, Ростовская область, ул. Советская ул., 21,), e-mail: [1]lipkovich012@yandex.ru; [2]petrenko.new@mail.ru

В статье рассмотрены все этапы операций по обслуживанию подстанций и распределительных устройств. Данные операции требуют четкую последовательность выполнения в строгом соблюдении мер безопасности.

Ключевые слова: Безопасность; обслуживание; подстанция; распределительные устройства; оборудование.

ORGANIZATIONAL BASES OF WORK SAFETY WHEN SUBSTATION AND SWITCHGEAR MAINTENANCE

[1]Lipkovich I.E., [2]Petrenko N.V., Kubak N.A.
Azov-Chernomorsk Engineering Institute, Donskoy State Agrarian University in Zernograd, Russia (347740, Zernograd, Rostov region, ul. Sovetskaya St., 21,), e-mail: [1]lipkovich012@yandex.ru, [2]petrenko.new@mail.ru

The article considers all stages of operations for the maintenance of substations and switchgears. These operations require a clear sequence of execution in strict observance of security measures.

Keywords: Safety; service; substation; distribution devices; equipment.

Согласно ГОСТ Р 55608-2018 формы обслуживания подстанций (ПС) и распределительных устройств (РУ) определяются их расположением и значением в энергосистеме, в промышленном предприятии и степенью автоматизации и телемеханизации. В промышленных предприятиях и сетевых районах имеются ПС и РУ с постоянным дежурством персонала и без него. В первом случае дежурный персонал находится постоянно на обслуживаемом объекте, во втором случае персонал не прикрепляют к одному объекту; он производит одновременное обслуживание нескольких ПС и РУ. На автоматизированных и телемеханизированных ПС и РУ обслуживание централизовано; на них отсутствует постоянный дежурный персонал промышленного предприятия или сетевого района, за которым закреплено несколько ПС и РУ [1].

В СП 76.13330.2016 отмечено, что осматривать оборудование на ПС и РУ можно при наличии напряжения и при снятом напряжении одновременно с их ремонтом. При осмотре без снятия напряжения соблюдают необходимые меры предосторожности, например, запрещается

проникать за ограждения или заходить в камеры РУ и ПС. При осмотрах эксплуатируемых ПС и РУ следят за тем, чтобы температура воздуха внутри помещений не превышала +40 °С и не отличалась от температуры наружного воздуха более чем на 15 °С. Необходимость этого контроля обусловливается тем, что для оборудования и аппаратуры ПС и РУ опасен нагрев выше пределов, допускаемых ГОСТом. Важнейшее значение имеет тщательный уход за оборудованием и производственными помещениями; строгое выполнение указаний производственных и заводских инструкций. Необходимо поддерживать чистоту в помещении, так как запыление изоляции приводит к ее ускоренному износу; пыль, попадая во вращающиеся механизмы, ухудшает условия их работы. Очень важно следить за состоянием систем охлаждения трансформаторов, электродвигателей и выключателей. Для понижения температуры либо снижают нагрузку на оборудование и аппаратуру ПС и РУ, либо усиливают вентиляцию, с тем чтобы отвести избыток теплоты наружу. Вентиляция должна обеспечивать заданный температурный режим в помещении при различных колебаниях температуры окружающего воздуха [1, 2].

Превышение допустимых температур нагрева сильно влияет на изоляцию оборудования и аппаратов, вызывая ее ускоренное старение, а при значительном перегреве может произойти разрушение и пробой изоляции. Повышение температуры разъемных контактных соединений ведет к усиленному окислению контактных поверхностей, увеличению их переходного сопротивления и к еще большему нагреву.

Повышенные нагревы могут возникать не только в том случае, если ухудшается охлаждение, но и при перегрузках соответствующих аппаратов и оборудования. Поддержание надежного и экономичного режима работы всего оборудования входит в обязанности оперативного дежурного персонала.

На экономичность работы установки влияет правильное распределение нагрузки между параллельно работающими агрегатами и их число, схема сети и ряд других факторов. Если нагрузка уменьшается, то бывает целесообразно, чтобы работало меньшее количество агрегатов, так как при этом сокращаются потери энергии.

При осмотрах маслонаполненных аппаратов следят за тем, чтобы они содержали необходимое количество масла. Это обстоятельство имеет особенно важное значение в тех случаях, когда масло является дугогасящей средой отключение короткого за мыкания при недостатке масла в аппарате приводит к аварии. Ответственное место в масляных выключателях – контактная система, четкость работы которой может нарушиться при отключениях коротких замыканий. Поэтому после разрыва выключателем тока к. з. большой мощности производят осмотр выключателя и проверяют качество контактной системы как в отношении четкости работы, так и одновременности включения контактов. Качество состояния контактов признается удовлетворительным, если их переходное сопротивление соответствует данным завода-изготовителя [3].

Перед измерением несколько раз включают и отключают аппарат для того, чтобы вызвать самоочистку контактов. У правильно отрегулированных контактов разновременность их включения составляет не более 0,5–3% хода их траверсы. Для нормальной работы воздушных выключателей необходимо, чтобы подаваемый к ним сжатый воздух был свободен от механических примесей и не имел повышенной относительной влажности (более 50%). Воздух сушат редуцированием. Примеси в воздухе понижают четкость работы выключателя,

а наличие повышенной влажности вызывает конденсацию влаги и перекрытие изоляции внутри выключателя. Обслуживающий персонал систематически следит за исправностью фильтров, очищающих воздух, и состоянием водопоглотителей (адсорбентов), своевременно заменяя их заполнителем. Магистральные воздухопроводы РУ и ПС продувают не реже одного раза в год [2, 4].

При осмотре обращают внимание на то, чтобы плиты, закрывающие кабельные каналы, во избежание распространения огня при пожарах в каналах были из несгораемых материалов. При осмотрах проверяют исправность вентиляции общего назначения и аварийной, предназначенной для быстрого вывода при авариях из ПС и РУ продуктов сгорания органической изоляции, а также исправность отопления и сети освещения. Кровля помещений должна быть всегда в исправности, так как попадание внутрь помещений влаги приводит к увлажнению изоляции электрооборудования и аппаратов. Все проемы и отверстия в наружных стенах закрывают сетками. Подъездные дороги для транспорта к ПС и РУ по условиям пожарной безопасности должны всегда находиться в исправном состоянии и ничем не загромождаться.

При осмотрах РУ напряжением до 1000 В разрешается проводить без наряда следующие работы: уборку помещения, смену ламп, ремонт замков и дверей, замену плавких вставок при снятом напряжении, ремонт или замену выключателей освещения. Сроки осмотров РУ без их отключения зависят от вида обслуживания, принятого для них: на объектах с постоянным дежурством – один раз в сутки (для выявления наличия электрических разрядов – не реже одного раза в месяц); на объектах без постоянного дежурного персонала – не реже одного раза в месяц.

График плановых осмотров РУ и ПС устанавливает главный энергетик предприятия. Кроме плановых осмотров все РУ и ПС подлежат внеочередным осмотрам после ликвидации короткого замыкания. Внеочередные осмотры открытых РУ и ПС проводят также при неблагоприятной погоде. Во время осмотров в журналах записывают показания приборов (вольтметров, амперметров и др.) и фиксируют выявленные при осмотрах неисправности, с тем чтобы они могли быть устранены в кратчайший срок. Для контроля обнаруженных неисправностей в журнале имеется специальная графа, в которой отмечается время ликвидации неисправности. При эксплуатации РУ и ПС необходимо осматривать состояние резервного электрооборудования. Оно должно быть готово к включению в любой момент без предварительной подготовки. Такую проверку осуществляют периодически, включая резервное оборудование под напряжение. Сроки проверки резервного электрооборудования устанавливают местными инструкциями [5].

Периодические осмотры шкафов КРУ и вмонтированных в них аппаратов проводят также в зависимости от местных условий. При осмотрах КРУ проверяют состояние электрической изоляции устройства, выключателей, проводов, механизмов доводки и блокировки разъединяющихся контактов первичной и вторичной цепей и наличие смазки на трущихся частях механизмов. Периодически контролируют состояние резервных элементов КРУ (трансформаторов, кабельных муфт, шин), с тем чтобы они всегда находились в состоянии, допускающем их немедленное включение в эксплуатацию.

Большую роль в повышении надежности и экономичности режима работы электроустановок и улучшении качества электроэнергии играют устройства автоматики,

телемеханики и диспетчеризации. Поэтому они всегда должны быть включены в работу. Их роль особенно возрастает при авариях и других внезапных изменениях режима работы электроустановок.

Наиболее сложными и ответственными являются действия дежурного персонала при ликвидации нарушений режима работы установки, вызванных повреждением или аварией оборудования. Такие нарушения режима обычно происходят неожиданно и требуют от дежурного персонала незамедлительных действий.

При обслуживании ПС периодически проверяют состояние заземляющего устройства и, если необходимо, измеряют его сопротивление специальным прибором – измерителем заземления МС-07 или МС-08. Для измерения (рисунок 1) используют вспомогательный *4* и потенциальный *5* заземлители – стальные стержни диаметром не менее 5 мм, забиваемые в грунт на глубину 0,5 м. Потенциальный заземлитель называется зондом. Измеритель заземления *1* располагают в непосредственной близости к испытываемому заземлителю б; вспомогательный заземлитель и зонд – соответственно на расстояниях 30 и 20 м от измеряемого заземления. При измерениях зажимы I_1 и E_1, замкнутые перемычкой, присоединяют к испытываемому заземлителю. К зажиму I_2 присоединяют вспомогательный заземлитель, а к зажиму E_2 – зонд. Перед измерением производят компенсацию сопротивления зонда, для чего переключатель *3* ставят в положение *Регулировка* и, вращая рукоятку генератора с частотой вращения 135 об/мин, поворотом головки переключателя пределов измерения *2* устанавливают стрелку прибора на красную отметку шкалы. Если это не получается, необходимо уменьшить сопротивление зонда. Затем измеряют сопротивление заземляющего устройства, отсчитывая его по шкале (в омах) с учетом выбранного коэффициента измерения [2, 5].

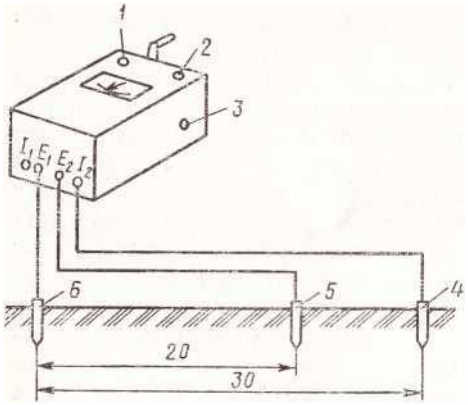


Рисунок 1 – Схема включения измерителя заземления МС-07

Сроки осмотров, ремонта и профилактических испытаний, электрооборудования подстанций и распределительных устройств.

При эксплуатации производят осмотр, чистку, ремонт и профилактические испытания оборудования подстанций и распределительных устройств.

Текущий ремонт включает работы, не требующие вскрытия оборудования: чистку электрооборудования от пыли; проверку действия движущих частей аппаратуры; контроль состояния изоляции; подтяжку крепящих болтов по мере надобности в сроки, установленные главным энергетиком предприятия.

Отключение для ремонта любого РУ и ПС неизбежно вызывает нарушение нормальной схемы электроснабжения потребителей, поэтому ремонт должен начинаться со сборных шин и линейных присоединений, т. е. с транзитной части РУ. 'Такой порядок позволяет при необходимости, не закончив весь объем ремонтных работ, включить сборные шины и создать нормальную схему для других ПС.

При проверке контактов шин затяжку выполняют гаечными ключами. Качество контакта при ремонте проверяют щупом толщиной 0,05 мм и шириной 10 мм, который не должен проходить на глубину более 5 мм, а в процессе эксплуатации с помощью термоиндуктора. В качестве стационарного индикатора применяют специальную пленку, наклеиваемую вблизи контактов. При температуре 60–70 °С термопленка имеет красный цвет, при дальнейшем нагревании – темнеет, что указывает на плохой контакт затяжки шин. Масляные выключатели и их приводы, разъединители с приводами и заземляющие ножи ремонтируют не реже одного раза в три года, а воздушные выключатели с их приводом – не реже одного раза в два-три года; все остальные аппараты РУ – по результатам осмотров и профилактических испытаний. Кроме указанного выключатели ремонтируют после того, как произведено отключение трех-четырех коротких замыканий [3, 6].

Капитальный ремонт электрооборудования ПС и РУ производят с вскрытием оборудования. Масляные выключатели и их приводы подвергают капитальному ремонту не реже одного раза в три года, а воздушные выключатели с их приводом – не реже одного раза в два-три года. Кроме указанного масляные и воздушные выключатели подвергают внеочередному капитальному ремонту после того, как произведено отключение трех-четырех коротких замыканий. Разъединители и их приводы дистанционного управления, а также заземляющие ножи подвергают ремонту не реже одного раза в три года, все остальные аппараты ПС и РУ – по результатам осмотров и профилактических испытаний.

Приведенные сроки работы электрооборудования РУ без капитального ремонта являются максимальными и соответствуют нормальным условиям эксплуатации этого электрооборудования. При тяжелых условиях эксплуатации, например повышенной частоте отключений к. з., капитальный ремонт выключателей производят чаще – в сроки, установленные главным энергетиком предприятия применительно к местным условиям.

Профилактические испытания масляных и воздушных выключателей, их приводов, а также приводов дистанционного управления разъединителей производят, как правило, одновременно с капитальным ремонтом. Статические конденсаторы, маслонаполненные измерительные трансформаторы, контакты соединений шин и присоединений к аппаратам (при отсутствии термоиндикаторов) подвергают профилактическим испытаниям не реже одного раза в три года, остальные аппараты РУ – не реже одного раза в шесть лет.

Объем и порядок профилактических испытаний и нормы для них приводятся в ПТЭ и ПТБ. Объем и сроки профилактических испытаний силовых трансформаторов определяются местными инструкциями, в которых учитываются условия работы трансформаторов и их техническое состояние [3, 4].

Оперативные переключения. Оперативные переключения – одна из наиболее ответственных операций, выполняемых дежурным персоналом электроцеха РУ и ПС. Переключения выполняет дежурный персонал, прошедший специальную подготовку. Все

сложные и простые переключения в установках, не имеющих устройств блокировки разъединителя, производят два человека, один из которых непосредственно выполняет переключения, а другой контролирует их правильность. Перечень лиц, которым предоставлено право производить оперативные переключения, ограничивается и утверждается лицом, ответственным за электрохозяйство установки.

Оперативные переключения производят по распоряжению лица, в ведении которого находится РУ и ПС. Дежурный, которому предстоит осуществить переключения, на основе полученного распоряжения продумывает предстоящие операции. После этого он заполняет бланк переключений, в котором дается последовательность предстоящих операций. Производить оперативные переключения без бланков переключений разрешается в особых случаях при пожарах, несчастных случаях с людьми и ликвидациях аварий.

Исполнителю перед выполнением переключения разъясняют порядок и последовательность предстоящих действий. При переключениях необходимо помнить, что высоковольтный выключатель и разъединитель предназначены для разных функций – разъединитель не предназначен для отключения или включения электросети с нагрузкой. Если его использовать для этой цели, это приведет к образованию дуги, которая перебросится на соседние фазы, вызывая короткое замыкание. Замыкание и размыкание нагрузочной цепи является операцией, для которой предназначен силовой выключатель, имеющий специальное дугогасящее устройство. Перед операцией разъединителем предварительно убеждаются, что выключатель действительно находится в отключенном положении. Разъединитель необходимо включать быстро, доводя операцию до конца даже при возникновении дуги при подходе ножа к неподвижному контакту. Отключать разъединитель надо, наоборот, медленно; в случае появления дуги в начале операции разъединитель необходимо быстро и решительно включить обратно. Ниже приведены примеры простейших оперативных переключений в РУ и ПС.

Вывод в ремонт одной из спаренных кабельных линий № 3 напряжением 10 кВ, питающейся от одного выключателя, показан на Рисунке 2. Для этого надо предварительно снять нагрузку с кабеля № 3 у потребителя. Затем выяснить длину кабеля. Если его длина более 10 км, то отключать разъединителями зарядный ток запрещается [1, 4].

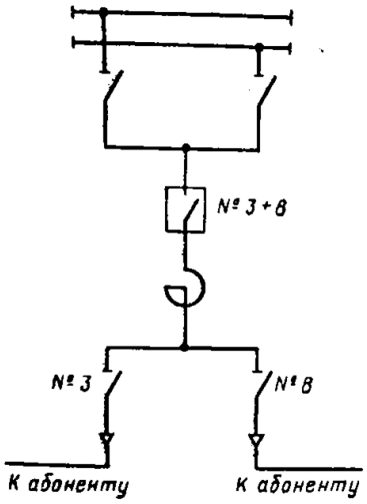


Рисунок 2 – Схема вывода в ремонт одной из спаренных кабельных линий напряжением 10 кВ, питающихся от одного выключателя

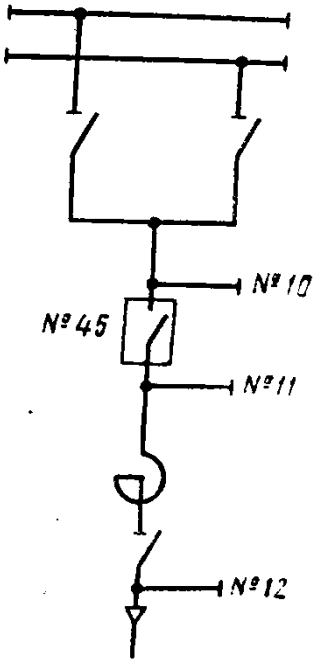


Рисунок 3 – Схема включения в работу линии напряжением 10 кВ после ремонта

При длине кабеля до 10 км по амперметру проверяют отсутствие нагрузки на кабеле и отключают линейные разъединители кабеля № 3; закрывают на замок привод отключенного разъединителя; на приводе линейных разъединителей вывешивают плакат *«Не включать – работают люди»;* сообщают потребителю о снятии напряжения с кабеля № 3, после чего потребитель, соблюдая все правила безопасности, устанавливает у себя защитное заземление, вывешивает необходимые плакаты. Только после этого можно производить ремонтные работы.

В работу линию напряжением 10 кВ включают после ремонта (Рисунок 3). Например, получено распоряжение включить в работу после ремонта линию № 45. Действие персонала: снять заземление № 10 и 11 с выключателя и заземление № 12 с линейных разъединителей линии № 45, а также все плакаты и ограждения; по механическому указателю или по положению контактов проверить отключение выключателя линии № 45; снять замки с приводов разъединителей линии № 45; включить шинные разъединители линии на заданную систему шин; включить линейные разъединители линии; подать оперативный ток на привод выключателя линии № 45; включить выключатель; сообщить потребителю о том, что напряжение на линию № 45 подано. По условиям техники безопасности при включении и отключении разъединителей необходимо пользоваться изолирующей штангой и диэлектрическими перчатками [4, 6].

Анализируя все этапы операций по обслуживанию подстанций и распределительных устройств, можно с уверенностью сказать, что данные операции требуют четкую последовательность выполнения в строгом соблюдении мер безопасности.

Общие требования охраны труда.

1.1. К использованию технических средств обучения допускаются лица, прошедшие инструктаж по охране труда, медицинский осмотр и не имеющие противопоказаний

по состоянию здоровья, имеющие 1 квалификационную группу допуска по электробезопасности. К использованию проекционной аппаратуры и других технических средств обучения учащиеся не допускаются.

1.2. Лица, допущенные к использованию технических средств обучения, должны соблюдать правила внутреннего трудового распорядка, расписание учебных занятий, установленные режимы труда и отдыха.

1.3. При использовании технических средств обучения возможно воздействие на работающих следующих опасных и вредных производственных факторов:

- поражение электрическим током при отсутствии заземления корпуса демонстрационного электрического прибора или неисправном электрическом шнуре и электрической вилки;
- ослепление глаз сильным световым потоком при снятии защитного кожуха демонстрационного электрического прибора во время его работы;
- ожоги рук при касании защитного кожуха демонстрационного электрического прибора во время его работы;
- возникновение пожара при воспламенении кинопленки, диафильма, диапозитивов, слайдов и пр.

1.4. При использовании технических средств обучения необходимо соблюдать правила пожарной безопасности, знать места расположения первичных средств пожаротушения.

1.5. При несчастном случае пострадавший или очевидец несчастного случая обязан немедленно сообщить администрации колледжа. При неисправности технических средств обучения прекратить работу и сообщить администрации колледжа.

1.6. Соблюдать порядок использования технических средств обучения, правила личной гигиены, содержать в чистоте рабочее место.

1.7. Лица, допустившие невыполнение или нарушение инструкции, законодательных и нормативно-правовых требований по охране труда, привлекаются к ответственности в соответствии с законодательством РФ.

2. Требования охраны труда перед началом работы

2.1. Установить проекционную электрическую аппаратуру с противоположной стороны от выхода из помещения.

2.2. Заземлить корпус электрического прибора, имеющего клемму «Земля».

2.3. Убедиться в целостности электрического шнура и вилки прибора, а также исправности линз объектива и наличии защитного кожуха.

3. Требования охраны труда во время работы

3.1. Не подключать демонстрационный электрический прибор к электрической сети влажными руками.

3.2. Включить демонстрационный электрический прибор и убедиться в его нормальной работе, а также работе охлаждающего вентилятора.

3.3. Во избежание ослепления глаз мощным световым потоком, не снимать защитный кожух во время работы демонстрационного электрического прибора.

3.4. Во избежание ожогов рук не касаться защитного кожуха демонстрационного электрического прибора во время его работы.

3.5. Не оставлять работающие технические средства обучения без присмотра. пожарной безопасности.

4. Требования охраны труда в аварийных ситуациях

4.1. При возникновении неисправности в работе демонстрационного; электрического прибора или нарушении заземления его корпуса выключить прибор и отключить его от электрической сети. Работу продолжать только после устранения неисправности.

4.2. При воспламенении немедленно выключить демонстрационный электрический прибор, эвакуировать учащихся из помещения, сообщить о пожаре администрации колледжа и в пожарную часть по тел. 01, приступить к тушению очага возгорания с помощью первичных средств пожаротушения.

4.3. При получении травмы оказать первую помощь пострадавшему, при необходимости отправить его в ближайшее лечебное учреждение и сообщить об этом администрации колледжа.

5. Требования охраны труда по окончании работы

5.1. Выключить демонстрационный электрический прибор и после его остывания охлаждающим вентилятором отключить от электрической сети.

5.2. Убрать демонстрационный прибор в отведенное для хранения место.

5.3. Проветрить помещение и тщательно вымыть руки с мылом.

Список литературы

1. Организационные основы безопасности при ремонте электрических двигателей в условиях предприятия АПК / Липкович И.Э., Украинцев М.М., Егорова И.В., Петренко Н.В // АгроЭкоИнфо. 2022. № 3 (51).
2. Электробезопасность в сельскохозяйственном производстве: монография / И.Э. Липкович, М.М. Украинцев, И.В. Егорова, С.М. Пятикопов, М.В. Жолобова, Н.В. Петренко, С.В. Панченко, А.Н. Токарева, Ж.В. Матвейкина, А.С. Гайда. – Зерноград: Азово-Черноморский инженерный институт ФГБОУ ВО Донской ГАУ, 2022. – 244 с.
3. Пястолов А.А. Ерошенко Г.П. Эксплуатация электрооборудования - М.: Агропромэнерго, 1990 - 287 с.
4. Правила устройства электроустановок - М.: Энергоатомиздат, 1986 г. - 424 с
5. Е.А.Конюхова Электроснабжение объектов.- М, 2001-320 с.
6. П.Н.Листова Применение электрической энергии в сельскохозяйственном производстве, 1984 г.

References

1. Organizational bases of safety in the repair of electric motors in the conditions of the agricultural enterprise / Lipkovich I.E., Ukraintsev M.M., Egorova I.V., Petrenko N.V. // AgroEcoInfo. 2022. No. 3 (51).
2. Electrical safety in agricultural production: monograph / I.E. Lipkovich, M.M. Ukraintsev, I.V. Egorova, S.M. Pyatikopov, M.V. Zholobova, N.V. Petrenko, S.V. Panchenko, A.N. Tokareva, Zh.V. Matveikina, A.S. Guide. - Zernograd: Azov-Chernomorsk Engineering Institute of FGBOU VO Donskoy GAU, 2022. – p.244.

3. Pyastolov A.A. Eroshenko G.P. Operation of electrical equipment - M .: Agro-promenergo, 1990 – p. 287.
4. Rules for the installation of electrical installations - M .: Energoatomizdat, 1986 – p. 424.
5. E.A. Konyukhova Power supply of objects. - M, 2001- p.320
6. P.N. Listova Application of electric energy in agricultural production, 1984

Проблематика обеспечения пожарной безопасности в зданиях с массовым пребыванием людей / Снежко А.А. [и др.] // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 117–120

Международный журнал информационных технологий и энергоэффективности

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

УДК 614.84

ПРОБЛЕМАТИКА ОБЕСПЕЧЕНИЯ ПОЖАРНОЙ БЕЗОПАСНОСТИ В ЗДАНИЯХ С МАССОВЫМ ПРЕБЫВАНИЕМ ЛЮДЕЙ

[1] Зайнидинов А. С., [2] Крохта К. С, [3] Жданкин С. С., [4,5] Снежко А. А.
[1,2,3,4] Сибирская пожарно-спасательная академия ГПС МЧС России, Железногорск, Россия (662972, Красноярский край, г. Железногорск, ул. Северная, 1,), e-mail: [1]ZainidinovAS@mail.ru, [2] 125556@bk.ru, [3] 555668@mail.ru, [4] SnezhkoA006@yandex.ru
[5] Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева, Красноярск, Россия (660000, Красноярский край, г. Красноярск, просп. имени газеты Красноярский Рабочий, 31), e-mail: [5]SnezhkoA006@yandex.ru

Проблемы в области обеспечения пожарной безопасности показывают несовершенство данной системы. На примере зданий с массовым пребыванием людей выявлен ряд вопросов о реализации пожарной безопасности, предложены пути их решения.

Ключевые слова: Пожарная безопасность, здания с массовым пребыванием людей, пожарный риск, государственный пожарный надзор, законодательство в области пожарной безопасности.

THE PROBLEM OF ENSURING FIRE SAFETY IN BUILDINGS WITH A MASS STAY OF PEOPLE

[1] Zainidinov A.S., [2] Krokhta K.S., [3] Zhdankin S. S., [4,5] Snezhko A. A.
[1,2,3,4] Siberian Fire and Rescue Academy of the State Fire Service of the Ministry of Emergency Situations of Russia, Zheleznogorsk, Russia (662972, Krasnoyarsk Territory, Zheleznogorsk, st. Severnaya, 1), e-mail: [1]ZainidinovAS@mail.ru, [2] 125556@bk.ru, [3] 555668@mail.ru, [4] SnezhkoA006@yandex.ru
[5] Siberian State University of Science and Technology named after academician M. F. Reshetnev, Krasnoyarsk, Russia (660000, Krasnoyarsk Territory, Krasnoyarsk, Ave. named after the newspaper Krasnoyarsky Rabochiy, 31), e-mail: SnezhkoA006@yandex.ru

Problems in the field of fire safety show the imperfection of this system. On the example of buildings with a massive stay of people, a number of issues about the implementation of fire safety have been identified, and ways to solve them have been proposed.

Keywords: Fire safety, buildings with mass stay of people, fire risk, state fire supervision, fire safety legislation.

Пожар, случившийся в «Полигоне», заставил довольно многих вспомнить о трагической ночи в клубе «Хромая лошадь», расположенном в Перми. В 2009 году в том клубе заживо сгорели 156 человек. Это почти каждый второй, кто находился в тот момент в заведении. Виновными лицами были признаны местные пиротехники, бывшие сотрудники Государственного пожарного надзора, а также администрация клуба. Иными словами, лица,

которые были ответственны за пожарную безопасность. На территории клуба в ночь пожара был организован фейерверк из «холодного огня». Согласно основной версии следствия, возгоранию способствовала относительно небольшая высота потолка помещения и имевшийся на нем декор, выполненный их ивовых прутьев и холста. Искры, достигнутые потолка, привели к его возгоранию. Молниеносному распространению огня способствовали использованный пенопласт, пластиковая отделка стен, а также скопившаяся на потолке пыль [1].

Отмечается неутешительная «пожарная» статистика в подобных развлекательно-досуговых организациях. Так, на протяжении нескольких последних лет «отметились» пожарами театров и других культурных заведений следующие города: Москва, Санкт-Петербург, Новосибирск, Саратов, Пенза, Пермь, Иркутск, Красноярск, Находка, Якутск и другие. При этом только в Москве фиксировалась масса возгораний: Государственный академический Большой театр, Российский академический Молодежный театр (РАМТ), Театр Русской драмы, Театр «Школа современной пьесы», Театр кукол имени С.В. Образцова, Театр имени М.Н. Ермоловой, Театр «Эрмитаж», Центральный Академический Театр Российской Армии, Театр имени А.С. Пушкина (филиал), Московский драматический театр имени К.С. Станиславского, Театр имени Е. Вахтангова, Театр зверей Дурова, Дом Культуры «Октябрь» и др. Воспламенялись пристройки, подвальные помещения, кровли театров, а также занавес и декорации на сцене. Площадь пострадавших и полностью сгоревших помещений достигала 600 м^2 и более с эвакуацией до 500 человек [2].

Наблюдения, экспертные опросы и анализ показывают, что в театрах не всегда установлены и оборудованы места, предназначенные для курения, не везде регламентирован порядок проведения временных огневых и иных пожароопасных работ, не везде регламентирован порядок осмотра и закрытия помещений после того, как работа завершена, а также не регламентированы действия сотрудников театра в случае обнаружения ими возгорания. Стоит отметить, что также недостаточно четко обеспечивается и контролируется порядок и сроки проведения эвакуационных тренировок, прохождения противопожарного инструктажа и занятий по пожарно-техническому минимуму. Помимо этого не на постоянной основе проводится обучение действующих сотрудников театра действиям в случае обнаружения ими возгорания, а также обращению с пожарной сигнализацией и системой оповещения в целом. В театрах также далеко не всегда осуществляется реализация мероприятий, направленных на проведение инструктажа по охране труда и пожарной безопасности. Не решены проблемы эвакуации с чердачных и подвальных помещений. В числе не разрешённых проблем также – противоречия между требованиями пожарной безопасности, обеспечение беспрепятственного доступа к эвакуационным выходам [2].

Особой проблемой является и тот факт, что на сегодняшний день нормативно-правовая база, регламентирующая требования пожарной безопасности, имеет довольно внушительный объём. Следствием данного факта является вероятная возможность запутаться в огромном многообразии нормативно-правовых актов. Также стоит отметить, что большое количество актов имеет ряд дополнений и изменений, что тоже показывает несовершенства существующей законодательной системы в области пожарной безопасности.

Тот же комплекс проблем часто присутствует и на других объектах значительного риска, к которым кроме театров, клубов и цирков относятся сооружения, на территории которых одновременно пребывает более 200 человек. К подобным зданиям относятся

следующие: гостиницы, санатории, музеи, кинотеатры, библиотеки, высшие и средние профессиональные учебные учреждения, рестораны, офисные сооружения, высота которых составляет более 28 метров, а также промышленные предприятия I, II, II класса опасности и другие [2].

Объекты, которые предполагают массовое пребывание людей, в обязательном порядке должны обладать рядом специализированных средств и приспособлений, направленных на обеспечение соответствующей пожарной безопасности. Наличие исправной телефонной или радиосвязи предоставляет возможность молниеносно сообщить о возникшем пожаре в службу пожарной охраны. Территории организаций должны обладать достаточным наружным освещением в темное время суток для того, чтобы оперативно находить пожарные гидранты, наружные пожарные лестницы и специально оборудованные места с пожарным инвентарем, а кроме того подъезды к пирсам пожарных водоемов и входам в сооружения. Места расположения первичных средств пожаротушения, а также пожарные щиты и специализированные места для курения должны быть обозначены соответствующими знаками пожарной безопасности. Стоит отметить, что территория и помещения в обязательном порядке должны содержаться в чистоте и порядке.

По итогу установления расчетных величин индивидуального пожарного риска сооружений с массовым пребыванием людей, как показывает практика, определяется, что указанный риск отвечает требуемому и никак не превышает значение одной миллионной в год при размещении отдельно взятого человека в более удаленной точке от выхода из сооружения [3]. Однако часто возникает вопрос несоответствия заявленной расчетной вероятности наступления пожарных рисков реальным событиям.

Таким образом, проблемы, поднятые в статье – достаточно распространённые и требуют скорейшего решения. Задачи пожарной безопасности на территории зданий, где предполагается массовое пребывание людей, может разрешить исключительно полная реализация предписаний, установленных государственным пожарным надзором, а также эффективный контроль со стороны пожарных инспекторов по вопросу соблюдения упомянутых предписания и совершенствование действующего законодательства в области пожарной безопасности.

Список литературы

1. Пожар в пермском ночном клубе "Хромая лошадь". Что случилось 10 лет назад [Электронный ресурс]. URL: https://tass.ru/info/7265987. (Дата обращения: 06.11.2022).
2. Демешко, Е. В. Ответственность за нарушение правил пожарной безопасности в местах с массовым пребыванием людей / Е. В. Демешко // Вестник науки. – 2022. – Т. 5. – № 10(55). – С. 109-113.
3. Приложение к Приказу МЧС России № 382 от 30.06.2009г. «Методика определения расчетных величин пожарного риска в зданиях, сооружениях и пожарных отсеках различных классов функциональной пожарной опасности» (с изменениями от 12.12.2011 г. в ред. Приказа МЧС России № 749 и с изменениями от 02.12.2015 г. в ред. Приказа МЧС России № 632).

References

1. Fire in the Permian nightclub Lame Horse. What happened 10 years ago [Electronic resource]. URL: https://tass.ru/info/7265987. (Accessed: 06.11.2022).
2. Demeshko, E. V. Responsibility for violation of fire safety rules in places with mass stay of people / E. V. Demeshko // Bulletin of Science. - 2022. - V. 5. - No. 10 (55). - S. 109-113.
3. Appendix to the Order of the Ministry of Emergency Situations of Russia No. 382 dated 30.06.2009. "Methodology for determining the calculated values of fire risk in buildings, structures and fire compartments of various classes of functional fire hazard" (as amended on December 12, 2011, as amended by Order No. EMERCOM of Russia No. 632).