Международный журнал информационных технологий и энергоэффективности

Том 7 Номер 4 (26)

2022

Международный журнал информационных технологий и энергоэффективности
Т.7 №4(26) часть 1 2022 г.

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

СОДЕРЖАНИЕ / CONTENT

Самодолов И.А., Селезнев Д.Н., Колмаков В.О. Суперконденсаторы, как перспективное направление для развития энергосбережения на железнодорожном транспорте// Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 5–7

Международный журнал информационных технологий и энергоэффективности

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

УДК 621.319.4

СУПЕРКОНДЕНСАТОРЫ, КАК ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ ДЛЯ РАЗВИТИЯ ЭНЕРГОСБЕРЕЖЕНИЯ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

[1] Самодолов И.А., [2] Селезнев Д. Н, [3]Колмаков В.О.
Красноярский институт железнодорожного транспорта ИрГУПС, Красноярск, Россия (660028, г. Красноярск, ул. Ладо Кецховели, д.89), e-mail: [1]vech1964@mail.ru, [2]seleznyov.mitry@yandex.ru, [3]kolmakov_vo@krsk.irgups.ru.

В статье рассматривается вопрос применения суперконденсаторов для железнодорожного транспорта. Данным вопросом занимается компания ТЭЭМП, которая занималась разработкой нового типа ячейки блоков суперконденсатора. В результате анализа аналогичных устройств, была создана новая конструкция, которая уменьшила массу блока и ячейки и позволило увеличить диапазон рабочих температур. Также ТЭЭМП занималась вопросом улучшения системы автоматического запуска и остановки двигателя тепловозов и минимизации неэффективного потребления дизеля. Ведутся работы над комбинированными системами питания электропоездов на базе батарей Li-ION и суперконденсаторами в связке с дизель-генераторной установкой, что позволяет применять данную систему для участков не оборудованных сетью питания.

Ключевые слова: суперконденсатор, энергосбережение, аккумулятор, ячейка, блок, топливо, тепловоз.

SUPERCAPACITORS AS A PROMISING DIRECTION FOR THE DEVELOPMENT OF ENERGY SAVING IN RAILWAY TRANSPORT

[1]Samodolov I. A., [2]Seleznev D. N., [3]Kolmakov V.O..
Krasnoyarsk Institute of Railway Transport IrGUPS, Krasnoyarsk, Russia (660028, Krasnoyarsk, st. Lado Ketskhoveli, 89), e-mail: [1]vech1964@mail.ru, [2]seleznyov.mitry@yandex.ru, [3]kolmakov_vo@krsk.irgups.ru.

The article discusses the use of supercapacitors for railway transport. This issue is being handled by the TEEMP company, which was engaged in the development of a new type of cell of supercapacitor blocks. As a result of the analysis of similar devices, a new design was created that reduced the mass of the unit and cell and allowed to increase the operating temperature range. TEEMP also dealt with the issue of improving the system of automatic start and stop of the diesel locomotive engine and minimizing inefficient diesel consumption. Work is underway on combined electric train power systems based on Li-ION batteries and supercapacitors in conjunction with a diesel generator set, which allows this system to be used for sites not equipped with a power supply network.

Keywords: supercapacitor, energy saving, battery, cell, unit, fuel, diesel locomotive.

В наше время электротранспорт получил быстрое развитие, а вопрос энергосбережения продолжает пользоваться большим спросом, тем временем технология, которая была проверена исследованиями и разработками, практическим применением, получила второе дыхание. Это суперконденсаторы (СК), которые способны обеспечивать устройства током

высокой мощности. Работы в этой области ведет ООО «Товарищество энергетических и электромобильных проектов» (ТЭЭМП). Данная компания сконструировала новый тип ячейки, которая может быть использован на железнодорожном транспорте [1]. Создание гибридных локомотивов с использованием суперконденсаторов получило перспективное направление для ОАО «РЖД».

Суперконденсаторы не выделяются большой плотностью энергии, но они могут обеспечивать ток высокой мощности и имеют больший ресурс. Эти особенности обусловлены совокупностью качеств, таких система стартерного пуска, в работе кратковременных источников бесперебойного питания (ИБП) высокой мощности и являются хорошей базой для железнодорожных объектов, а также в системах восстановления электроэнергии [2].

Глобальный рынок суперконденсаторов оценивался в 549,1 млн долларов США в 2021 году. Однако в России СК не имеют большой спрос из-за незаинтересованности в них, сомнениях в экономических затратах и внедрении на железнодорожный транспорт и предприятия. ТЭЭМП решает заняться вопросом повышения спроса на данную технологию.

В 2014 году ТЭЭМП, совместно с национальным исследовательским технологическим университетом МИСиС, начинается разработку новой конструкции и электролита для ячейки суперконденсатора в котором по требованию заказчика собираются модули с заданными характеристиками напряжения и емкости [3]. В 2017 году продукт поступил в серийное производство. Благодаря особому дизайну основные ячейки блоков СК имеют ряд достоинств: уменьшение массы ячейки и блока на 30% по сравнению с аналогами, минимизация количества элементов ячейки, поддержание функциональности после проведения испытаний на ток короткого замыкания, повышение эффективности полей тока и тепла, уменьшение внутреннего сопротивления. Для увеличения диапазона рабочих температур СК и систем пуска до -60°С стали использоваться композитные органические электролиты.

В маневренных и магистральных дизельных двигателях в зимний период жидкость, используемая для охлаждения, нагревается при простаивании дизель-генератора, что приводит к низкоэффективному потреблению топлива. Чтобы уменьшить этот эффект, рекомендуется использовать автоматические системы обогрева с автоматическим включением и отключением силовой установки тепловоза. В связи с этим были улучшены и гармонизированы технические условия системы автоматического запуска-остановки двигателя (САЗДТ) для маневровых и магистральных тепловозов. Это приводит к снижению расхода топлива, увеличению срока эксплуатации тягового оборудования, уменьшения негативного воздействия на окружающую среду. Примерно 80% экономических затрат приходиться на дизельное топливо. Согласно статистике, при работе тепловоза более 15 минут на холостом ходу, расход топлива увеличится на 40%. В течение этого периода САЗДТ должен обеспечить автоматическое отключение тепловоза и автоматический запуск двигателя с накопителем энергии при падении температуры ниже допустимого значения, а также производить контрольные замеры температуры охлаждающей жидкости. Это позволяет уменьшить скорость нагрева тепловоза на половину. Кроме того, при применении энергетических аккумуляторов значительно снижается нагрузка на аккумулятор тепловоза при запуске двигателя, что увеличивает срок эксплуатации аккумуляторов в 1,5 раз [4].

Создание гибридных тепловозов, которые будут оснащены как дизель-генераторной установкой (ДГУ), так и суперконденсаторами, позволит данному тепловозу проходить

дистанцию 320 км со скоростью 120 км/ч. Необходимая мощность разделяется между ДГУ, СК и литий-ионными аккумуляторами. Система восстанавливает энергию торможения и возвращает ее к источнику питания электродвигателя. Достоинства такой установки могут быть полностью раскрыты в неэлектрофицированных районах, а также экономия на и эксплуатационных расходах тепловоза. Планируемая стоимость такой системы составляет 115,2 млн. рублей.

Применение новой сконструированной ячейки суперконденсатора может обеспечить большое количество вариантов для использования в железнодорожной автоматизации. ТЭЭМП разработала систему бесперебойного питания, которая повышает надежность электроснабжения в случае потери питания от основного источника. Они могут обеспечить мощность 20 кВт за 6 минут, при отсутствии основного источника питания. В 2018 году ТЭЭМП совместно с итальянской компанией DUCATI Energia SpA, завершили установку ИБП на базе суперконденсаторов для железной дороги Италии. В настоящее время производится тестовое применение системы для использования на объектах первой категории.

Список литературы

1. Годовой отчет ОАО «РЖД» за 2019 год. – 121 с. – [Электронный ресурс] URL: https://bit.ly/31ULAJ7. (Дата обращения: 01.10.2022).
2. Постановление Правительства РФ от 12.06.2003 № 344 (ред. от 24.12.2014) «О нормативах платы за выбросы в атмосферный воздух загрязняющих веществ стационарными и передвижными источниками, сбросы загрязняющих веществ в поверхностные и подземные водные объекты, в том числе через централизованные системы водоотведения, размещение отходов производства и потребления».
3. Суперконденсаторы и аккумуляторы ТЭЭМП, – [Электронный ресурс] URL: https://teemp.ru. (Дата обращения: 02.10.2022).
4. Mordor Intelligence, – [Электронный ресурс] URL: https://www.mordorintelligence.com/ru/industry-reports/supercapacitors-market. (Дата обращения: 29.11.2022).

References

1. Annual report of Russian Railways for 2019. - 121 p. – [Electronic resource] URL: https://bit.ly/31ULAJ7. (Accessed: 01.10.2022).
2. Decree of the Government of the Russian Federation of June 12, 2003 No. 344 (as amended on December 24, 2014) “On the standards of payment for emissions of pollutants into the atmospheric air by stationary and mobile sources, discharges of pollutants into surface and underground water bodies, including through centralized sewerage systems, disposal of production and consumption waste”.
3. TEEMP supercapacitors and batteries, - [Electronic resource] URL: https://teemp.ru/. (Accessed: 02.10.2022).
4. Mordor Intelligence, - [Electronic resource] URL: https://www.mordorintelligence.com/ru/industry-reports/supercapacitors-market. (Accessed: 11/29/2022).

Шацких Ю.В., Шарапов А.И., Арзамасцев А.Г. Расчет регенеративных теплообменных аппаратов// Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 8-14

Международный журнал информационных технологий и энергоэффективности

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

УДК 66.045.13

РАСЧЕТ РЕГЕНЕРАТИВНЫХ ТЕПЛООБМЕННЫХ АППАРАТОВ

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

В статье рассмотрена программа расчета регенеративных теплообменных аппаратов. Программа позволяет рассчитывать теплообменники как с подвижной, так и с неподвижной насадкой. В основу программы положены аналитические зависимости, полученные из решения дифференциального уравнения теплового баланса с принятым линейным распределением температуры по расчетному слою. Отличительной особенностью программы является учет влияния температур газов и насадки на их теплофизические характеристики и коэффициенты теплоотдачи для каждого расчетного слоя, что позволяет добиться высокой точности расчетов при выборе достаточно большого количества расчетных слоев.

Ключевые слова: регенерация теплоты, энергоэффективность, конструктивные характеристики насадки, режимные параметры.

CALCULATION OF REGENERATIVE HEAT EXCHANGERS

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

The article considers a program for calculating regenerative heat exchangers. The program allows you to calculate heat exchangers with both a movable and a fixed nozzle. The program is based on analytical dependencies obtained from the solution of the differential heat balance equation with the assumed linear temperature distribution over the calculated layer. A distinctive feature of the program is taking into account the effect of gas and packing temperatures on their thermophysical characteristics and heat transfer coefficients for each calculation layer, which makes it possible to achieve high accuracy of calculations when choosing a sufficiently large number of calculation layers.

Keywords: heat recovery, energy efficiency, design characteristics of the packing, operating parameters.

Введение

Проектирование регенеративных теплообменников предоставляет собой ложную задачу. Во-первых, расчет нестационарного теплообмена сам по себе сложен и подразумевает использование программного обеспечения. Во-вторых, эффективность работы регенеративного теплообменника определяется сочетанием конструктивных характеристик

насадки и режима работы аппарата. Поэтому при проектировании регенеративного теплообменника нужно «нащупать» это сочетание, что подразумевает большое количество много вариативных трудоемких расчетов.

Различные авторы разрабатывали программное обеспечение для расчета конкретных конструкций регенеративных теплообменников [1]. Причем использованы разные методики расчета, не подходящие для аппаратов другой конструкции. Нужно отметить, что отличия в подходах объясняются скорее историей развития прикладной науки в той или иной отрасли, чем сутью физических явлений, проходящих в регенераторах [2-4]. Таким образом, если в одних и тех же условиях предстоит сравнить регенераторы с подвижной и неподвижной насадкой и выбрать лучший, то на данный момент нет единой методики расчета различных типов теплообменников и методики их сравнительного анализа.

Из вышесказанного следует, что при проектировании регенеративного теплообменного аппарата необходимо предварительно выбрать оптимальное сочетание режимных и конструктивных характеристик аппарата, а затем провести его тепловой расчет. Методика расчета должна подходить как для аппаратов с подвижной насадкой, так и для аппаратов с неподвижной насадкой.

Предварительный анализ регенеративного теплообменника

Анализ различных работ в этой области [4-6] и собственные исследования авторов [7] показывают, что регенеративные теплообменники обеспечивают наибольшую эффективность, в случае если распределение температуры насадки и теплоносителей по высоте близко к линейному, поскольку при линейном распределении обеспечивается постоянный по всей высоте насадки локальный температурный напор, т.е. $\upsilon = const$.

Как было показано в работе [7] при линейном распределении температуры по высоте насадки систему дифференциальных уравнений нестационарного теплообмена можно привести к критериальному виду. Также в [8] рассмотрены критерии подобия, включающие в себя как конструктивные, так и режимные характеристики регенеративного теплообменника. На основе критериев подобия модно сделать предварительный анализ конструкции регенеративного теплообменника. Например, при заданных характеристиках насадки подобрать оптимальные расходы теплоносителей и продолжительность периодов нагрева и охлаждения. Либо, при заданной температуре одного из теплоносителей на выходе из теплообменника подобрать конструктивные характеристики насадки и режимные параметры аппарата. Разумеется, полученные результаты будут приближенными, но это существенно сокращает область поиска оптимального сочетания режимных и конструктивных характеристик аппарата. Точное значение параметров теплообменника можно получить при использовании разработанной авторами программы расчета.

Расчет регенеративного теплообменного аппарата

В основу расчета положена модель Меншикова – Соломенцева [8], в которой вычисления ведутся по аналитическим зависимостям, полученным из решения дифференциального уравнения теплового баланса с принятым линейным распределением температуры по расчетному слою. Достоинством данной модели является учет влияния температур газов и насадки на их теплофизические характеристики и коэффициенты теплоотдачи для каждого

расчетного слоя, что позволяет добиться высокой точности расчетов при выборе достаточно большого количества расчетных слоев.

На основании данной модели разработана «Программа для расчета регенеративных теплообменных аппаратов» [9]. Отличительной особенностью программы является определение числа циклов, при которых для заданного распределения температур насадки и параметров теплоносителей наступает квазистационарный режим, характеризующийся равенством температурных полей насадки в конце предыдущего и начале следующего цикла.

Программа позволяет рассчитать конечные температуры теплоносителей на выходе из регенератора в заданные моменты времени, что имеет большое значение при проверке соблюдения ограничений по величине выходной температуры греющего теплоносителя. Расчет теплообмена по известным методикам дает только средние температуры на выходе из регенератора, в то время как для проверки соблюдения этих ограничений часто необходимо знать значения выходной температуры греющего теплоносителя в течение всего периода нагрева.

Расчет регенеративного теплообменника с использованием программы основан на следующих принципах:

- Начальное распределение температур насадки принято линейным. Насадка рассматривается как термически тонкое тело с поправкой на коэффициент массивности. Отсчет координаты ведется от входа греющего теплоносителя.
- Задаются начальная температура и расход греющего теплоносителя на входе в теплообменник.
- Принято линейное распределение температуры насадки по высоте Δz расчетного слоя насадки за расчетный отрезок времени $\Delta\tau$ (1):

$$t_{z\tau} = t_{0\tau} - bz \quad (1)$$

- где $t_{0\tau}$– средняя по массе температура насадки на входе в расчетный слой насадки в момент времени τ расчетного отрезка времени $\Delta\tau$, °С; b – константа, характеризующая изменение температуры насадки по высоте z данного слоя насадки в данный отрезок времени $\Delta\tau$, К/м.
- Коэффициент теплоотдачи определяется по критериальным уравнениям для соответствующего типа поверхности насадки. Коэффициент теплоотдачи рассчитывается для каждого слоя и каждого шага по времени с учетом изменения температуры среды. Это позволяет повысить точность расчета. Для расчета принимаются средние значения температур теплоносителей в слое в предыдущий момент времени.

Расчет регенеративного теплообменного аппарата с помощью программы строится по следующему алгоритму:

1. Задаются состав теплоносителей, высота и материал слоев насадки, геометрические характеристики насадки.
2. Задается температура греющего и нагреваемого теплоносителей на входе в насадку, продолжительность периодов нагрева/охлаждения, расход нагреваемого и греющего теплоносителя.
3. При заданной неизменной входной температуре греющего теплоносителя для первого отрезка времени для каждого расчетного слоя в конце данного временного интервала определяются температуры насадки на входе в слой и температура газов

на выходе из слоя. Температура греющего теплоносителя на выходе из данного слоя принимается как входная температура для следующего слоя, температура насадки на выходе из слоя рассчитывается как входная температура для следующего слоя. Для второго и последующего расчетного отрезка времени начальным распределением температур насадки является уже распределение температур для предыдущего временного интервала. При расчетах для каждого слоя и шага по времени теплофизические параметры теплоносителей и насадки вычисляются с учетом их температур.

Аналогично рассчитывается период охлаждения насадки.

В программе заданы функции зависимости теплофизических параметров теплоносителей и насадки от температуры, поэтому на каждом шаге по высоте и по времени расчет теплообмена происходит с учетом изменения температур, что позволяет повысить точность расчетов. Также при расчете теплофизических параметров теплоносителей учитываются потери давления теплоносителей при течении вдоль насадки.

Программа позволяет выполнить два вида расчета.

- Определение температуры теплоносителей на выходе из регенеративного теплообменника при заданных расходах греющей и нагреваемой сред. Расчет выполняется в несколько итераций (их количество можно задать в программе), пока температура насадки в конце цикла для каждой рассмотренной точки не будет отличаться от температуры насадки в начале цикла для соответствующей точки не более чем на заданную величину температурного расхождения (в программе принято 1 °С), т.е. пока режим не станет квазистационарным. Результат расчета цикла, при котором это условие соблюдается, программа выдает на экран.
- Определение расхода греющего теплоносителя, при котором будет получена требуемая температура нагрева холодного теплоносителя или требуемая температура охлаждения греющего теплоносителя. В этом случае расход греющего теплоносителя задается предварительно. Программа рассчитывает теплообмен в насадке по вышеописанному алгоритму. Если заданные температуры не достигаются (разница 1 °С), то программа корректирует значение расхода греющего теплоносителя и повторяет расчет.

Таким образом, программа позволяет рассчитывать температурные поля теплоносителей и насадки в расчетные моменты времени. В конце расчета выдаются минимальные, максимальные и средние значения температур теплоносителей на выходе из регенератора. Также по запросу для каждого шага по времени выдается распределение по высоте насадки теплофизических параметров насадки и теплоносителей и значения локальных коэффициентов теплоотдачи.

Проведённые расчеты позволяют получить распределение температуры насадки и теплоносителей по высоте, что дает возможность судить о том, насколько выбранный режим работы аппарата обеспечивает линейное распределение температуры по высоте насади. Кроме того, программа рассчитывает значения средних коэффициентов теплоотдачи теплоносителей и теплопроводности насадки, что позволяет оценить интенсивность теплообмена.

Пример вывода результаты расчета приведены на рисунке 1. Результаты расчета выводятся в графическом виде и в виде текстового файла в формате txt, распределение температуры теплоносителей и насадки по высоте выводится в файле формата xlsx.

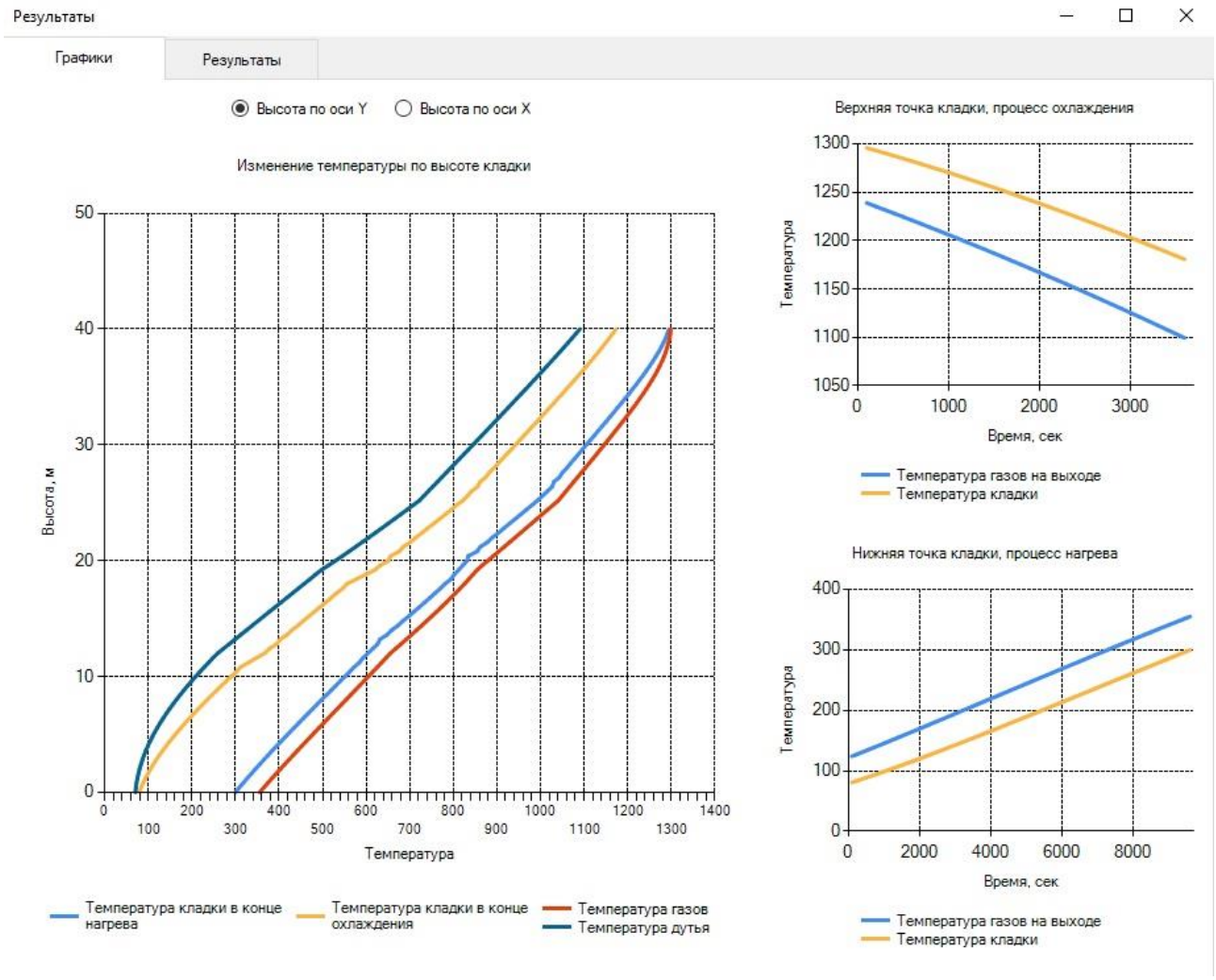

Рисунок 1 – Интерфейс вывода результатов расчета в графическом виде

Заключение

Авторы предложили метод инженерного расчета регенеративных теплообменников с разным типом насадки. На основе критериального анализа нестационарного теплообмена в насадке выбирается оптимальное сочетание конструктивных характеристик насадки и режимных параметров работы аппарата. То есть для заданного типа насадки можно подобрать оптимальный режим нагрева/охлаждения. Затем, с помощью разработанной авторами программы проводится расчет регенеративного теплообменника. В результате расчета можно получить распределение температуры по высоте насадки в конце периодов нагрева/охлаждения, изменение температуры теплоносителей на выходе из насадки в течение периодов нагрева/охлаждения, средний за период нагрева/охлаждения коэффициент теплоотдачи. Также с помощью программы можно определить расход греющего теплоносителя при заданном расходе нагреваемого теплоносителя. Предложенный подход позволяет значительно сократить количество расчетов при проектировании регенеративных теплообменников.

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

Список литературы

1. Губарев А.Ю., Кудинов А.А. Программы теплового расчета стандартных регенеративных воздухоподогревателей и регенеративных воздухоподогревателей в форме усеченного конуса // Тезисы докладов межд. науч. конф., «XIX Туполевские чтения». – Казань: КНИТУ-КАИ, 2011, т.1, с. 190-192.
2. Кирсанов Ю.А. Циклические тепловые процессы и теория теплопроводности в регенеративных воздухоподогревателях. М.: ФИЗМАТЛИТ –2007, 240 с.
3. Самарин О.Д. Температурная эффективность пластинчатых и роторных теплоутилизаторов при различных расходах воздуха // Сантехника, Отопление, Кондиционирование, 2014, № 1 (145). – С. 118-119.
4. 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.
5. Соломенцев С.Л. Рациональные типы насадок и доменных воздухонагревателей. Липецк: ЛГТУ., 2001. 432 с.
6. 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. DOI:10.1088/1742-6596/2119/1/012156
7. Yu. V. Shatskikh, Yu. A. Geller. Development of optimization criterions of regenerative heat exchangers and operating regime of regenerative heat exchangers / Published under licence by IOP Publishing Ltd Journal of Physics: Conference Series, Volume 1683, Actual issues of thermal power engineering and thermal engineering, 2020 J. Phys.: Conf. Ser. 1683 042028. DOI:10.1088/1742-6596/1683/4/042028.
8. Меншиков Р.И., Соломенцев С.Л. Приближенный метод расчета температур по высоте воздухонагревателей. Известия вузов. Черная Металлургия. 1983. № 111.С.140-143.
9. Программа для расчета регенеративных теплообменных аппаратов. Свидетельство о государственной регистрации программы на ЭВМ 2022683184, 01.12.22. Заявка № 2022682401 от 22.11.2022.

References

1. Gubarev A.Yu., Kudinov A.A. Programs for thermal calculation of standard regenerative air heaters and regenerative air heaters in the form of a truncated cone // Abstracts of reports int. scientific Conf., "XIX Tupolev Readings". - Kazan: KNRTU-KAI, 2011, v.1, p. 190-192.
2. Kirsanov Yu.A. Cyclic thermal processes and the theory of heat conduction in regenerative air heaters. M.: FIZMATLIT -2007, 240 p.
3. 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.
4. 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 With.

5. Solomentsev S.L. Rational types of nozzles and blast furnaces. Lipetsk: LGTU., 2001. 432 p.
6. 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 Thermophysical Seminar (STS37), 2021 J. Phys.: Conf. Ser. 2119 012156. DOI:10.1088/1742-6596/2119/1/012156
7. Yu. V. Shatskikh, Yu. A. Geller. Development of optimization criteria of regenerative heat exchangers and operating regime of regenerative heat exchangers / Published under license by IOP Publishing Ltd Journal of Physics: Conference Series, Volume 1683, Actual issues of thermal power engineering and thermal engineering, 2020 J. Phys.: Conf . Ser. 1683 042028. DOI:10.1088/1742-6596/1683/4/042028.
8. Menshikov R.I., Solomentsev S.L. An approximate method for calculating temperatures from the height of air heaters. Izvestiya vuzov. Ferrous metallurgy. 1983. No. 111.S.140-143.
9. Program for calculation of regenerative heat exchangers. Certificate of state registration of the computer program 2022683184, 01.12.22. Application No. 2022682401 dated 11/22/2022.

Балашов В.С. Современное состояние вопроса по использованию высокопроводящих вставок в теплообменных аппаратах // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 15–19

Международный журнал информационных технологий и энергоэффективности

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

УДК 66.045

СОВРЕМЕННОЕ СОСТОЯНИЕ ВОПРОСА ПО ИСПОЛЬЗОВАНИЮ ВЫСОКОПРОВОДЯЩИХ ВСТАВОК В ТЕПЛООБМЕННЫХ АППАРАТАХ

Балашов В.С.
Самарский Государственный Технический Университет, Самара, Россия (443100, г. Самара, ул. Молодогвардейская, д.244), e-mail: slavkab163@gmail.com

Рассмотрены актуальные мировые вопросы повышения энергоэффективности теплообменных аппаратов в сфере теплоэнергетики и теплотехники. В связи с развитием теплоэнергетической отрасли в 21 веке и стремлением к повышению энергоэффективности теплообменников, обеспечивающейся путем внедрения высокопроводящих вставок в оребрение теплообменных аппаратов, выявлены оптимальные материалы, геометрические формы вставок, а также их объем относительно основных ребер.

Ключевые слова: оребрение, высокопроводящие вставки, теплообменные аппараты, энергоэффективность.

THE CURRENT STATE OF THE ISSUE ON THE USE OF HIGHLY CONDUCTIVE INSERTS IN HEAT EXCHANGERS

Balashov V.S.
Samara State Technical University, Samara, Russia (443100, Samara, st. Molodogvardeyskaya, 244), e-mail: slavkab163@gmail.com

The current world issues of increasing the energy efficiency of heat exchangers in the field of heat power engineering and heat engineering are considered. In connection with the development of the heat and power industry in the 21st century and the desire to increase the energy efficiency of heat exchangers, provided by the introduction of highly conductive inserts into the fins of heat exchangers, optimal materials, geometric shapes of inserts, as well as their volume relative to the main ribs, have been identified.

Keywords: finning, highly conductive inserts, heat exchangers, energy efficiency.

Существует множество способов повышения энергоэффективности теплообмена. Одним из самых популярных является оребрение труб теплообменных аппаратов. Этот метод получил широкое распространение за возможность значительно увеличить тепловую эффективность теплообменника при его малых размерах.

Ребра могут иметь как прямоугольную, так и конусовидную форму, а также изготавливаются из разнообразных материалов.

Теплообменные аппараты с оребренными трубами могут производиться двумя способами:

- Цельные ТА – оребрение происходит в момент производства ТА.
- Составные ТА – оребрение производится уже на изготовленном ТА различными способами.

Для того, чтобы получить понимание насколько эффективно то или иное ребро теплообменного аппарата, необходимо определить значение коэффициента теплопередачи. Эффективность ребра напрямую зависит от его формы и, конечно же, материала. Ребра могут изготавливаться как из стали, так и из меди и алюминия. Однако производство ребер из меди довольно затратно, поэтому в последнее время получило широкое распространение использование высокопроводящих вставок для повышения энергоэффективности оребренных теплообменных аппаратов. Использование таких вставок позволяет значительно снизить тепловое сопротивление ребра и добиться его максимальной производительности, не увеличивая его размеры.

Оребрение является одним из самых эффективных способов для передачи тепла. В связи с этим создание ребра с меньшим размером и такой же эффективностью имеет важное значение. Для этого необходимо усилить коэффициент теплопроводности ребра. Такого результата можно достичь путем вставки высокопроводящих материалов в ребро (см. рисунок 1). Однако, как говорилось ранее, использование таких материалов довольно затратно, поэтому следует создать такую геометрическую форму ребра, чтобы это было не дорого, а самое главное – эффективно.

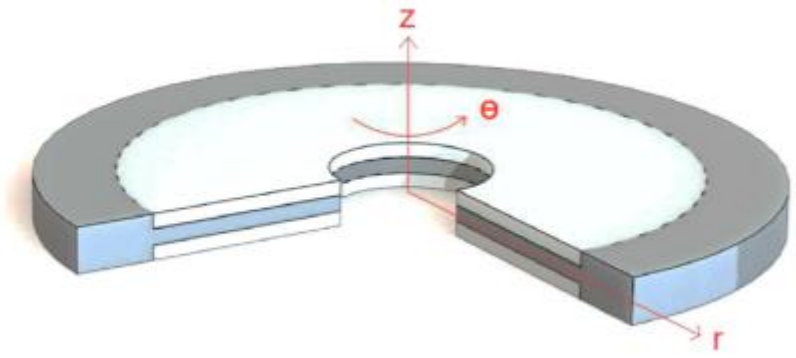

Рисунок 1 – 3D-модель ребра с высокопроводящей вставкой

Идея использования высокопроводящих материалов (‘вставок’) внутри систем теплопередачи и создания проводящих маршрутов, впервые была предложена Бежаном [1,2]. Он рассматривал объем конечного размера, в котором тепло генерируется равномерно и отводится в раковину на краю. Основной целью было направление тепла, выделяемого в объеме, в точку с использованием высокопроводящих материалов. Основываясь на теории построения [3-5], он исследовал несколько форм, предполагая, что количество высокопроводящего материала в среде фиксированное.

Лучшим результатом его исследования стал маршрут в форме дерева. С момента появления структурной теории было проведено множество исследований по этой теории [6-8]. Работа Бежана стала важной вехой в области систем охлаждения и побудила ученых предложить и оптимизировать возможные формы высокопроводящих вставок, полостей и ребер в тепловыделяющих корпусах. Бисерни и др. были первыми, кто исследовал полости [9]. Они ввели ‘I-образные", "T-образные’ полости. Результаты их работ показали, что лучшая T-образная конфигурация работает на 29% лучше, чем I-образная конфигурация.

Работу Бежана продолжили и другие ученые, предложив свои варианты использования высокопроводящих вставок.

Фенг и др. представили новый конструктивный дизайн пути с высокой проводимостью по квадратному телу [10]. Они предложили высокую проводимость в форме буквы ‘+’ и смогли снизить безразмерную пиковую температуру на 75,79% по сравнению с X-образной. В этой статье впервые предлагается использовать высокопроводящие материалы, встроенные в прямое ребро.

В то время как количество таких материалов с высокой теплопроводностью (‘вставок’) рассматривается как ограничение, геометрическая форма и конфигурация вставок оптимизированы для достижения максимальной теплопередачи.

Цеткин рассматривал охлаждение тепловыделяющей области путем введения высокопроводящих материалов [11]. Он внедрил материалы с высокой проводимостью с фиксированным объемом в каналы охлаждения и снизил максимальную температуру в домене. Он обнаружил наименьшие пиковые температуры в определенных местах и формах этих материалов.

Хаймохаммади и др. предложили новую конструкцию встраивания высокопроводящей вставки в тепловыделяющее тело [12]. Их целью было минимизировать пиковую температуру тепловыделяющего элемента.

Конан и Цеткин улучшили теплопередачу за счет использования высокопроводящих вставок в форме снежинок [13]. Они вставили высокопроводящий канал в форме снежинки в тепловыделяющее тело и уменьшили тепловое сопротивление.

Таким образом, вопрос внедрения в теплообменные аппараты высокопроводящих вставок и повышения их энергоэффективности широко распространен и имеет важнейшее значение в дальнейшем развитии теплоэнергетики, ведь множество ученых изучают данный вопрос. Бисерни, Фенг, Хаймохаммади изучали и описывали оптимальную форму вставок, а Конан и Бежан выясняли наиболее подходящий объем и материал.

Список литературы

1. D.D.L. Chung Materials for thermal conduction Appl. Therm. Eng., 21 (2001), pp. 1593-1605
2. Bejan, Constructal-theory network of conducting paths for cooling a heat generating volume Int. J. Heat Mass Transf., 40 (1997), pp. 799-816
3. Bejan, Shape and Structure, From Engineering to Nature Cambridge University Press (2000)
4. Bejan, S. Lorente Design with constructal theory Des. Constr Theory (2008), pp. 1-529
5. Bejan, S. Lorente The constructal law and the evolution of design in nature Phys. Life Rev., 8 (2011), pp. 209-240
6. U. Lucia, G. Grisolia Constructal law and ion transfer in normal and cancer cells Proc. Rom. Acad. Ser. A-Math. Phys. Tech. Sci. Inf. Sci., 19 (2018), pp. 213-218
7. U. Lucia, G. Grisolia, M.R. Astori Constructal law analysis of Cl- transport in eyes aqueous humor Sci. Rep., 7 (2017), p. 6856
8. U. Lucia, G. Grisolia, D. Dolcino, M.R. Astori, E. Massa, A. Ponzetto Constructal approach to bio-engineering: the ocular anterior chamber temperature Sci. Rep., 6 (2016), p. 31099
9. Biserni, L.A.O. Rocha, A. Bejan Inverted fins: geometric optimization of the intrusion into a conducting wall Int. J. Heat Mass Transf., 47 (2004), pp. 2577-2586

10. M.R. Hajmohammadi, V.A. Abianeh, M. Moezzinajafabadi, M. Daneshi Fork-shaped highly conductive pathways for maximum cooling in a heat generating piece Appl. Therm. Eng., 61 (2013), pp. 228-235
11. M.R. Hajmohammadi, O.J. Shariatzadeh, M. Moulod, S.S. Nourazar Phi and Psi shaped conductive routes for improved cooling in a heat generating piece Int. J. Therm. Sci., 77 (2014), pp. 66-74
12. H. Feng, L. Chen, Z. Xie, F. Sun Constructal design for "+" shaped high conductivity pathways over a square body Int. J. Heat Mass Transf., 91 (2015), pp. 162-169
13. H.C. Konan, E. Cetkin Snowflake shaped high-conductivity inserts for heat transfer enhancement Int. J. Heat Mass Transf., 127 (2018), pp. 473-482
14. M.R. Hajmohammadi, E. Rasouli, M. Ahmadian Elmi, Geometric optimization of a highly conductive insert intruding an annular fin, International Journal of Heat and Mass Transfer, Volume 146, 2020
15. Tao Dong, In Micro and Nano Technologies, Thermohydrodynamic Programming and Constructal Design in Microsystems, Academic Press, 2019, Pages 11-76

References

1. D.D.L. Chung Materials for thermal conduction Appl. Therm. Eng., 21 (2001), pp. 1593-1605
2. Bejan, Constructal-theory network of conducting paths for cooling a heat generating volume Int. J. Heat Mass Transf., 40 (1997), pp. 799-816
3. Bejan, Shape and Structure, From Engineering to Nature Cambridge University Press (2000)
4. Bejan, S. Lorente Design with constructal theory Des. Constr Theory (2008), pp. 1-529
5. Bejan, S. Lorente The constructal law and the evolution of design in nature Phys. Life Rev., 8 (2011), pp. 209-240
6. U. Lucia, G. Grisolia Constructal law and ion transfer in normal and cancer cells Proc. Rom. Acad. Ser. A-Math. Phys. Tech. Sci. Inf. Sci., 19 (2018), pp. 213-218
7. U. Lucia, G. Grisolia, M.R. Astori Constructal law analysis of Cl- transport in eyes aqueous humor Sci. Rep., 7 (2017), p. 6856
8. U. Lucia, G. Grisolia, D. Dolcino, M.R. Astori, E. Massa, A. Ponzetto Constructal approach to bio-engineering: the ocular anterior chamber temperature Sci. Rep., 6 (2016), p. 31099
9. Biserni, L.A.O. Rocha, A. Bejan Inverted fins: geometric optimization of the intrusion into a conducting wall Int. J. Heat Mass Transf., 47 (2004), pp. 2577-2586
10. M.R. Hajmohammadi, V.A. Abianeh, M. Moezzinajafabadi, M. Daneshi Fork-shaped highly conductive pathways for maximum cooling in a heat generating piece Appl. Therm. Eng., 61 (2013), pp. 228-235
11. M.R. Hajmohammadi, O.J. Shariatzadeh, M. Moulod, S.S. Nourazar Phi and Psi shaped conductive routes for improved cooling in a heat generating piece Int. J. Therm. Sci., 77 (2014), pp. 66-74
12. H. Feng, L. Chen, Z. Xie, F. Sun Constructal design for "+" shaped high conductivity pathways over a square body Int. J. Heat Mass Transf., 91 (2015), pp. 162-169
13. H.C. Konan, E. Cetkin Snowflake shaped high-conductivity inserts for heat transfer enhancement Int. J. Heat Mass Transf., 127 (2018), pp. 473-482

14. M.R. Hajmohammadi, E. Rasouli, M. Ahmadian Elmi, Geometric optimization of a highly conductive insert intruding an annular fin, International Journal of Heat and Mass Transfer, Volume 146, 2020
15. Tao Dong, In Micro and Nano Technologies, Thermohydrodynamic Programming and Constructal Design in Microsystems, Academic Press, 2019, Pages 11-76

Агеев В.А., Костригин А.А., Каргин Д.Н. Анализ и актуальность внедрения нетрадиционной электроэнергетики в Российской Федерации в 2021 году // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 20–26

Международный журнал информационных технологий и энергоэффективности

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

УДК 621.31

АНАЛИЗ И АКТУАЛЬНОСТЬ ВНЕДРЕНИЯ НЕТРАДИЦИОННОЙ ЭЛЕКТРОЭНЕРГЕТИКИ В РОССИЙСКОЙ ФЕДЕРАЦИИ В 2021 ГОДУ

[1]Агеев В.А., [2]Костригин А.А., [3]Каргин Д.Н.
Институт механики и энергетики, ФГБОУ ВО "МГУ им. Н.П. Огарёва", Саранск, Россия (430904, Республика Мордовия, г. Саранск, р. п. Ялга, ул. Российская, 5), e-mail: [1]ageyevva@mrsu.ru, [2]kostrigin42@mail.ru, [3]danik.kargin@yandex.ru

В работе выполнен анализ состояния нетрадиционной электроэнергетики Российской Федерации в 2021 году. По данным Сетевого оператора Единой энергетической системы РФ были построены диаграммы структуры производства электроэнергии СЭС и ВЭС в ОЭС РФ. Также была проанализирована актуальность внедрения нетрадиционной электроэнергетики.

Ключевые слова: нетрадиционная электроэнергетика, возобновляемые источники энергии, Единая энергетическая система Российской Федерации, Объединенная энергетическая система Российской Федерации, Сетевой оператор Единая энергетическая система Российской Федерации, солнечная электростанция, ветряная электростанция, приливная электростанция, геотермальная электростанция.

ANALYSIS AND RELEVANCE OF INTRODUCTION OF NON-TRADITIONAL ELECTRIC POWER INDUSTRY IN THE RUSSIAN FEDERATION IN 2021

[1]AgeevV.A., [2]Kostrigin A.A., [3]Kargin D.N.

Institute of mechanics and power engineering, National Research Mordovia State University, Saransk, Russia (430904, Republic of Mordovia, Saransk, Yalga, st. Rossiyskaya, 5), e-mail: [1]ageyevva@mrsu.ru, [2]kostrigin42@mail.ru, [3]danik.kargin@yandex.ru

The work analyzed the state of the non-traditional electric power industry of the Russian Federation in 2021. According to the Network Operator of the Unified Energy System of the Russian Federation, diagrams of the structure of electricity production of the SES and wind power plants in the OES of the Russian Federation were built. The relevance of the introduction of non-traditional electric power industry was also analyzed.

Keywords: non-traditional electric power industry, renewable energy sources, Unified Energy System of the Russian Federation, Unified Energy System of the Russian Federation, Grid operator Unified Energy System of the Russian Federation, solar power plant, wind power plant, tidal power plant, geothermal power plant

В современном мире невозможно представить жизнь без электроэнергетики, по праву именно она является фундаментом цивилизации. Формирование гарантированного и бесперебойного электроснабжения с учетом требуемого качества для обеспечения производственного процесса, нормального функционирования оборудования и

жизнедеятельности людей является приоритетным направлением эффективной работы всех экономических сфер любого государства.

Социальный процесс развития общества, совершенствование индустрии и увеличения численности населения запрашивают повышения производства электрической энергии. Постоянно повышается стоимость добычи и транспортировки материалов, в большинстве своем новые месторождения располагаются в отдаленных уголках страны, в которых не развита логистика транспортных поставок. Реальная острая нехватка органических энергетических ресурсов (уголь, природный газ, нефть, уран), от которых зависит выработка около 80% энергии, вполне возможна к середине двадцать первого века [3, с. 51].

Все более приходится считать воздействия электроэнергетики на окружающую среду и экологию. Электростанции, генерирующие электрическую энергию на основе традиционных видов топлива, выделяют до 30% объема вредных выбросов в атмосферу, загрязняя природу своими продуктами сгорания и сточными водами [4, с. 6]

Поэтому можно смело утверждать, что одним из приоритетных направлений развития электроэнергетики в XXI веке является широкое применение нетрадиционных источников электроэнергии, которые в свою очередь опираются на имеющие естественные возобновляемые ресурсы, позволяя тем самым снизить негативное воздействие на экологию и обеспечить энергетическую безопасность.

Актуальность данной работы заключается в анализе состояния и перспектив развития нетрадиционной и возобновляемой электроэнергетики в составе Единой энергетической системы Российской Федерации (ЕЭС) в 2021 году.

По данным Системного оператора Единой энергетической системы (СО ЕЭС) в электроэнергетический комплекс РФ включает в себя 911 электростанций, мощностью выше 5 МВт каждая [5]. Выработка электроэнергии электростанциями ЕЭС России в 2021 году составила 1 114 548,0 млн кВт·ч., а потребление электроэнергии в 2021 году составило 1 090 437,0 млн кВт·ч., что на 56 717,0 млн кВт·ч (+5,5%) больше в сравнении с 2020 годом. Основными источниками генерации электроэнергии в стране остаются представители традиционной электроэнергетики (выработка за 2021 год составляет: на ТЭС 676,908,00 млн кВт·ч; на ГЭС 209,519,80 млн кВт·ч; на АЭС 222,244,80 млн кВт·ч). Представителями нетрадиционной электроэнергетики в 2021 году вырабатывалось на СЭС и ВЭС 2 253,8 млн кВт·ч и 3 621,7 млн кВт. На рисунке 1 представлена структура выработки электроэнергии в ЕЭС РФ в 2021 году. Не популярность возобновляемых источников электроэнергии в сравнении с традиционными энергетическими ресурсами объясняется рядом факторов, представленных в таблице 1.

Таблица 1 – Факторы, сдерживающие развитие ВИЭ

Экономический:	Нормативно-правовой:	Технический:	Географический:
- инвестиции; -локализации производства оборудования.	- разработка стандартов; - гармонизация национальных стандартов; -земельный вопрос.	- вопросы подключения и эксплуатации объектов на ВИЭ.	- ограничение применения ВИЭ ввиду причин природного характера.

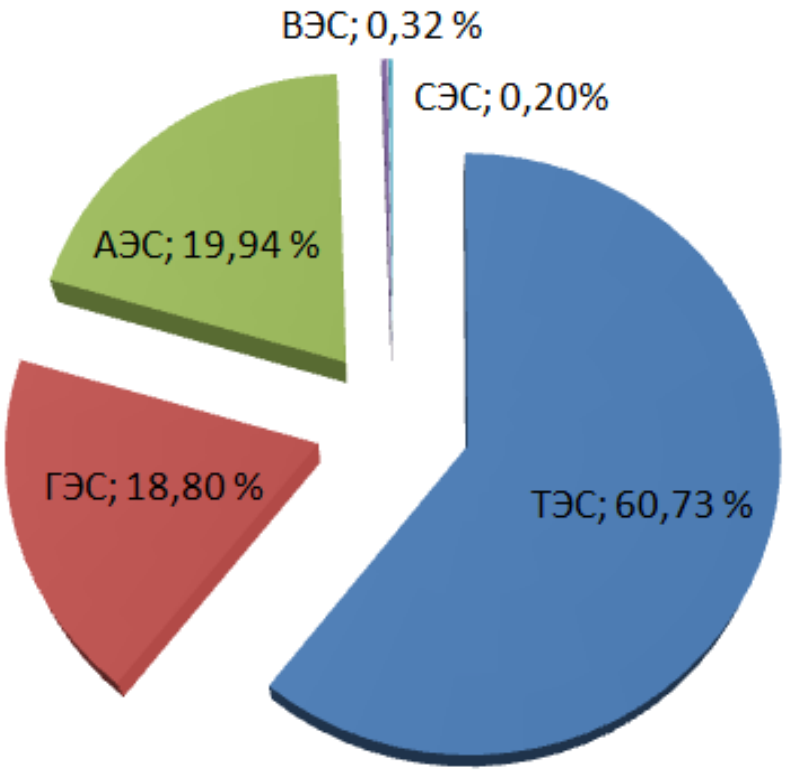

Рисунок 1 – Структура производства электроэнергии в ЕЭС РФ в 2021 году

Нетрадиционная электроэнергетика страны разнообразна, так как в ней имеются существенные ресурсы возобновляемой энергии: солнца, земли, ветра, а гидроэнергетических ресурсов. На территории абсолютно любого региона страны можно смело обнаружить несколько типов ресурсов для ВИЭ, экономическая эксплуатация которых может быть полностью оправдана. При этом есть субъекты, которые обладают всеми типами ресурсов возобновляемой энергии [1, с. 22].

Более подробно рассмотрим функционирующие на сегодняшний день объекты нетрадиционной электроэнергетики РФ. Доля электроэнергии, выработанной за счет представителей нетрадиционной энергетики, производится электрическими станциями следующих типов:

- солнечная электростанция или гелиоэлектростанция (СЭС);
- ветроэлектростанция (ВЭС);
- геотермальная электростанция (ГеоТЭС);
- приливная электростанция (ПЭС) [2, с. 48]

Солнечные электростанции в Российской Федерации выработали по данным СО ЕЭС в 2021 году около 2 253,8 млн·кВт·ч в год. Представители данного типа генерации находятся в объединенных энергетических системах (ОЭС) Юга, Средней Волги, Урала и Сибири. Крупнейшие электростанции СЭС в РФ, мощность которых выше 50 МВт представлены в таблице 2. На рисунке 2 представлена диаграмма структуры производства электроэнергии СЭС в ОЭС РФ по данным СО ЕЭС в 2021 году [5].

Таблица 2 – Крупнейшие электростанции на базе СЭС, мощность которых выше 50 МВт

Название СЭС	Установленная мощность, МВт	Регион
Аршанская	105,56	Республика Калмыкия

Перово	105,56	Республика Крым
Охотниково	82,65	Республика Крым
Самарская	75,00	Самарская область
Николаевка	69,70	Республика Крым

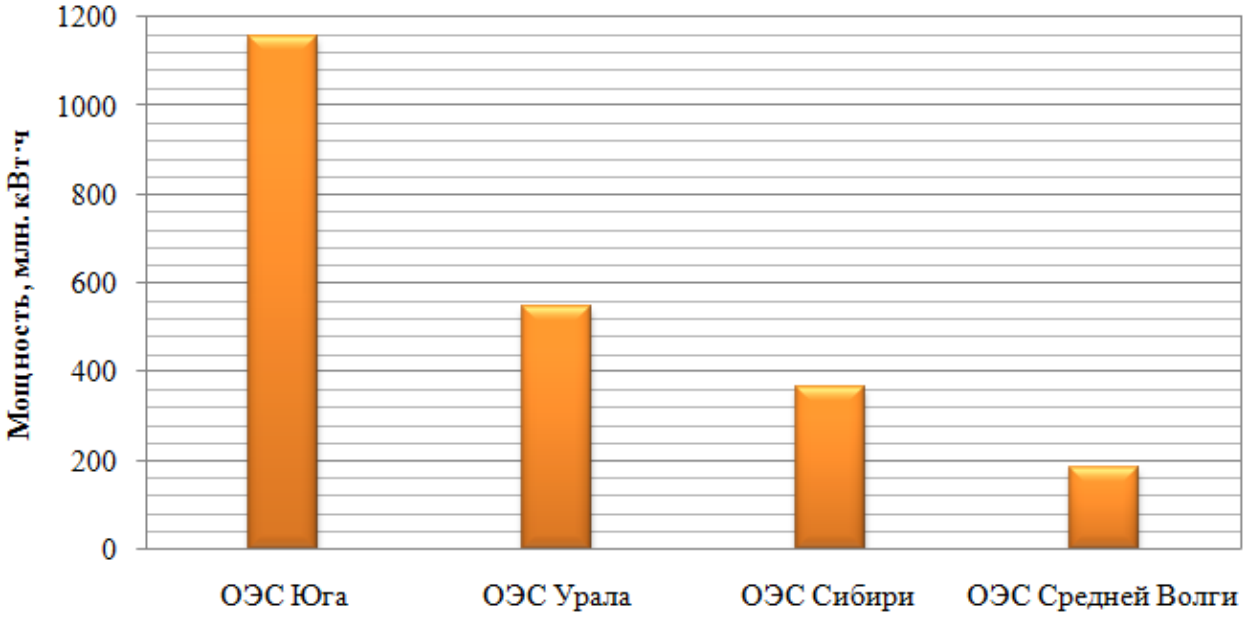

Рисунок 2 – Структуры производства электроэнергии СЭС в ОЭС РФ в 2021 году

Ветряные электростанции в Российской Федерации произвели по данным СО ЕЭС в 2021 году около 3 621,7 млн·кВт·ч в год. Данный тип выработки электроэнергии располагается в объединенных энергетических системах (ОЭС) Юга, Средней Волги, Северо-запада и Урала. Крупнейшие электростанции ВЭС в РФ, мощность которых выше 20 МВт представлены в таблице 3. На рисунке 3 изображена диаграмма структуры производства электроэнергии ВЭС в ОЭС РФ по данным СО ЕЭС в 2021 году [5].

Таблица 3 – Крупнейшие электростанции на базе ВЭС, мощность которых выше 50 МВт

Название ВЭС	Установленная мощность, МВт	Регион
Кочубеевская	210,00	Ставропольский край
Адыгейская	150,00	Республика Адыгея
Азовская	90,00	Ростовская область
Кармалиновская	60	Ставропольский край
Ульяновская-2	50,40	Ульяновская область

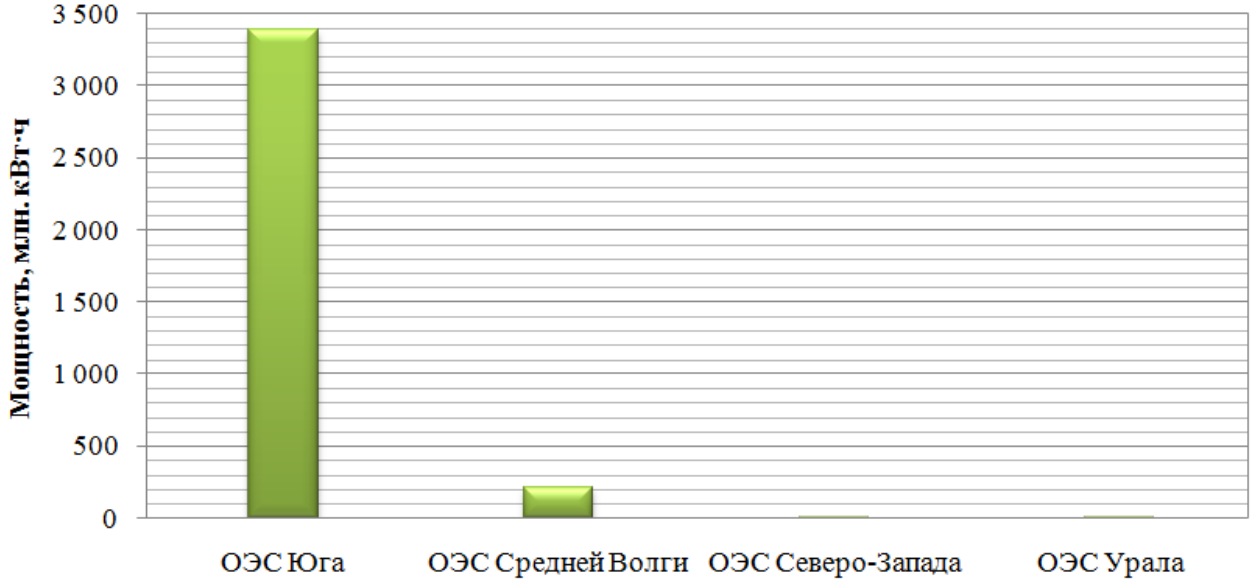

Рисунок 3 – Структуры производства электроэнергии ВЭС в ОЭС РФ в 2021 году

Приливные и геотермальные электростанции (ПЭС и ГеоТЭС) имеют меньшее представительство в РФ в сравнение с ВЭС и СЭС. ПЭС используют энергию напора, который создается между морем и бассейном во время прилива и отлива. На сегодняшний в РФ функционирует только одна опытная Кислогубская ПЭС, мощность которой в 2021 году составила 1200 кВт. Помимо этого разрабатывается ряд проектов ПЭС, которые будут располагаться в районах Белого и Охотского морей. Геотермальные электростанции используют в качестве источника энергии тепло земных недр. В 2021 году на территории РФ функционируют всего четыре ГеоТЭС три из которых в Камчатском крае и одна в Сахалинской области. Общая мощность выработанной электроэнергии составляет 81,4 МВт [2, с. 52].

Актуальность внедрения и использования нетрадиционной электроэнергетики в Российской Федерации формируется не только требованиями сегодняшнего дня, а той ролью, которую будет играть спустя 10-15 лет. Ее использование в первую очередь должно распространяться на районы с низкой плотностью населения, в которых не рентабельно строить крупные электростанции и протяженные линии электропередачи. Также актуально применение ВИЭ в местах временной работы и отдыха, садово-огородных сооружений. В местах с низкой степенью надежности электрических сетей объекты нетрадиционной электроэнергетики будут значительно играть роль резерва.

Перспективы развития и модернизации нетрадиционной электроэнергетики страны на сегодняшний день прописаны в Энергетической стратегии Российской федерации на период до 2035 года, утвержденной Правительством Российской Федерации 9 июня 2020 года [6]. В основе данного курса лежит Энергетическая стратегия Российской федерации на период до 2030 года, утвержденная Правительством Российской Федерации 13 ноября 2009 года и Энергетическая стратегия Российской федерации на период до 2020 года, утвержденная Правительством Российской Федерации 28 августа 2003 года [7][8]. Энергетическая стратегия РФ на период до 2020 года является основополагающим документом, содержащим стратегические цели и необходимость роста использования возобновляемых источников

энергии. Последующие стратегии уже направлены на реализацию и усовершенствование объектов нетрадиционной энергетики.

К ведущим целям энергетической стратегии РФ относятся: сокращение вредных выбросов в окружающую среду от объектов традиционной электроэнергетики; снижение роста потребления топливных ископаемых, в условиях истощения запасов; построение системы электроснабжения удаленных уголков страны за счет реализации возобновляемых источников электроэнергии и т. д.

В период реализации стратегии по итогам 2018 года было завершено строительство генерирующих объектов ВИЭ суммарной мощностью около 370 МВт, что выше показателя 2017 года более чем в 2,5 раза. Среди крупнейших объектов: Сорочинская СЭС (СЭС «Уран») мощностью 60 МВт и Новосергиевская СЭС (СЭС «Нептун») мощностью 45 МВт в Оренбургской области (ПАО «Т Плюс»); Фунтовская СЭС мощностью 60 МВт в Астраханской области (ГК «Хевел)»; 2-ая очередь Ульяновского ветропарка мощностью 50 МВт в Ульяновской области (ПАО «Фортум»). Всего с 2014 по 2018 гг. построено 648,5 МВт объектов ВИЭ, из них более 555 МВт – СЭС, более 90 МВт – ВЭС.

Проведенный анализ состояния нетрадиционной электроэнергетики Российской Федерации за 2021 год показывает, что возобновляемые источники электроэнергии не могут составить конкуренцию традиционным объектам электроэнергетики по причине имеющихся в стране запасов органических ресурсов, объем которых позволяет спокойно генерировать электрическую энергию на протяжении долгих лет. При всем этом нетрадиционная электроэнергетика является неотъемлемой частью энергосистемы, а развитие и рост ее потенциала позволит сэкономить имеющие в стране не возобновляемые ресурсы и снизить нагрузку на окружающую среду.

Список литературы

1. Юдаев, И. В. Возобновляемые источники энергии : учебник для вузов / И. В. Юдаев, Ю. В. Даус, В. В. Гамага. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 328 с. — ISBN 978-5-8114-9502-3.
2. Основы электротехники и электроснабжения предприятий лесного комплекса. Основы электроснабжения: учебник для вузов / Г. И. Кольниченко, Я. В. Тарлаков, А. В. Сиротов, М. С. Усачев ; под редакцией Г. И. Кольниченко. — Санкт-Петербург : Лань, 2022. — 252 с. — ISBN 978-5-8114-8466-9.
3. Общая энергетика: учебное пособие / составители М. Б. Балданов, Л. П. Шкедова. — Улан-Удэ: Бурятская ГСХА им. В.Р. Филиппова, 2021. — 75 с.
4. Нетрадиционные и возобновляемые источники энергии : учеб. пособие [Электронный ресурс] / В. А. Агеев, А. А. Костригин. – Саранск :Изд-во Мордов. ун-та, 2018 – 202 с. – .ISBN 978-5-7103-3574-1.
5. Отчет о функционировании ЕЭС России в 2021 году // ОАО «СО ЕЭС» [Электронный ресурс]: Режим доступа: https://www.so-ups.ru/fileadmin/files/company/reports/disclosure/2022/ups_rep2021.pdf
6. Энергетическая стратегия Российской Федерации на период до 2035 года [Электронный ресурс] : распоряжение Правительства Российской Федерации от 09.06.2020 №1523-р. –

М., 2020. – Режим доступа: http://static.government.ru/media/files/w4sigFOiDjGVDYT4IgsApssm6mZRb7wx.pdf
7. Энергетическая стратегия Российской Федерации на период до 2030 года [Электронный ресурс] : распоряжение Правительства Российской Федерации от 13.11.2009 №1715-р. – М., 2009. – Режим доступа: https://www.infobio.ru/sites/default/files/Energostrategiya-2030.pdf
8. Энергетическая стратегия Российской Федерации на период до 2020 года [Электронный ресурс] : распоряжение Правительства Российской Федерации от 28.08.2003 №1234-р. – М., 2009. – Режим доступа: http://www.energystrategy.ru/projects/ES-28_08_2003.pdf

References

1. Yudaev, I.V. Renewable energy sources: a textbook for universities/I.V. Yudaev, Yu. V. Daus, V.V. Gamaga. - 3rd ed., erased. - St. Petersburg: Doe, 2022. - 328 s. - ISBN 978-5-8114-9502-3.
2. Fundamentals of Electrical Engineering and Power Supply of Forestry Enterprises. Basics of power supply: a textbook for universities/G. I. Kolnichenko, Ya. V. Tarlakov, A. V. Sirotov, M. S. Usachev; edited by G. I. Kolnichenko. - St. Petersburg: Doe, 2022. - 252 s. - ISBN 978-5-8114-8466-9.
3. General Energy: textbook/compilers M. B. Baldanov, L. P. Shkedova. - Ulan-Ude: Buryat State Agricultural Academy named after V.R. Filippova, 2021. - 75 s.
4. Non-traditional and renewable energy sources: a textbook [Electronic resource]/V. A. Ageev, A. A. Kostrigin. - Saransk: Publishing House of Mordov. un-ta, 2018 - 202 p. - .ISBN 978-5-7103-3574-1.
5. Report on the operation of the UES of Russia in 2021//JSC SO UES [Electronic resource]: Access mode: https://www.so-ups.ru/fileadmin/files/company/reports/disclosure/2022/up
6. Energy Strategy of the Russian Federation until 2035 [Electronic Resource]: Order of the Government of the Russian Federation of 09.06.2020 No. 1523-r. - M., 2020. - Access mode: http://static.government.ru/media/files/w4sigFOiDjGVDYT4IgsApssm6mZRb7wx.pdf
7. Energy Strategy of the Russian Federation for the Period until 2030 [Electronic Resource]: Order of the Government of the Russian Federation of 13.11.2009 No. 1715-r. - M., 2009. - Access mode: https://www.infobio.ru/sites/default/files/Energostrategiya-2030.pdf
8. Energy Strategy of the Russian Federation for the Period until 2020 [Electronic Resource]: Order of the Government of the Russian Federation dated 28.08.2003 No. 1234-r. - M., 2003. - Access mode: http://www.energystrategy.ru/projects/ES-28_08_2003.pdf

Махонина Е. А., Верас Н. А., Коньков В. В. Исследование уязвимости браузера Microsoft Edge операционных систем Windows BDU:2022-06064 // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 27–30

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.7

ИССЛЕДОВАНИЕ УЯЗВИМОСТИ БРАУЗЕРА MICROSOFT EDGE ОПЕРАЦИОННЫХ СИСТЕМ WINDOWS BDU:2022-06064

[1]Махонина Е. А., [2]Верас Н. А., [3]Коньков В. В.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г.Санкт-Петербург, Российская Федерация (193232, г. Санкт-Петербург, пр. Большевиков, 22, к. 1), e-mail: [1]Makhonina800@mail.ru, [2]Veras.good@bk.ru, [3]1568487@yandex.ru

В статье рассмотрена уязвимость браузера Microsoft Edge операционных систем Windows BDU:2022-06064, приведено описание актуальных угроз, основанных на использовании уязвимости. Приводятся описания способов предотвращения нарушений информационной безопасности, а также зафиксированных случаев сетевых атак, проведенных при эксплуатации злоумышленником уязвимости.

Ключевые слова: информационная безопасность, веб-браузер, Windows, утечки информации.

VULNERABILITY STUDY OF THE MICROSOFT EDGE BROWSER FOR WINDOWS OPERATING SYSTEMS BDU:2022-06064

[1]Makhonina E.A., [2]Veras N.A., [3]Konkov V.V.
St. Petersburg State University of Telecommunications named after M.V. prof. M.A. Bonch-Bruevich, St. Petersburg, Russia (193232, St. Petersburg, pr. Bolsheviks, 22, building 1), e-mail: [1]Makhonina800@mail.ru, [2]Veras.good@bk.ru, [3]1568487@yandex.ru

The article discusses the vulnerability of the Microsoft Edge browser of Windows operating systems BDU:2022-06064, provides a description of current threats based on the exploitation of the vulnerability. Descriptions are given of ways to prevent information security violations, as well as recorded cases of network attacks carried out when an attacker exploited a vulnerability.

Keywords: information security, web browser, Windows, information loss.

Введение

В настоящее время существует всеобъемлющая потребность пользователей в безопасном использовании веб-ресурсов, а поиск и устранение уязвимостей веб-браузеров являются важными задачами в сфере информационной безопасности. Поэтому исследование уязвимости BDU:2022-06064 является актуальным.

Целью исследования является изучение и описание уязвимости, выявление эффективных решений для борьбы с атаками и утечкой защищаемой информации, возникающими при эксплуатации уязвимости, а также исследование зафиксированных случаев нарушения информационной безопасности с использованием таких атак.

Объектом исследования является уязвимость браузера Microsoft Edge с точки зрения возможности проведения спуфинг-атак, при ее выявлении.

Статья нацелена на студентов технических учебных заведений, специалистов, работающих с сетевыми технологиями, а также читателей, которым интересна данная тематика.

Новизна исследования состоит в обобщении изученной литературы, а также данных, публикуемых компаниями по разработке веб-браузеров на тему уязвимостей в сети Интернет, а также изучение отечественных решений по борьбе со спуфинг-атаками.

Описание уязвимости

Уязвимость браузера Microsoft Edge операционных систем Windows Уязвимость браузера Microsoft Edge возникает из-за ошибок синхронизации при использовании общего ресурса («ситуация гонки»). Использование данной уязвимости позволяет нарушителям проводить спуфинг-атаки. Уязвимость имеет высокий уровень опасности (базовая оценка CVSS 3.0 составляет 8,1). Уязвимость подтверждена производителем и описывается как, переполнение буфера кучи в графическом процессоре в Google Chrome до 107.0.5304.121, что позволяет удаленному злоумышленнику, скомпрометировавшему процесс рендеринга, потенциально выполнить выход из песочницы через созданную HTML-страницу и имеет идентификатор CVE-2022-4135. По шкале серьезности опасности Chromium уязвимость также оценивается как высокая.

Меры защиты

1. *Установка обновлений из доверенных источников.*

3 октября 2022 г. компания Microsoft выпустила последнюю версию Microsoft Edge Stable Channel (version 106.0.1370.34), которая включает в себя обновление безопасности проекта Chromium. В Руководстве по обновлению безопасности задокументировано объявление о том, что последняя версия Microsoft Edge (на основе Chromium) не является уязвимой при одновременном выполнении с использованием общего ресурса. Однако, компания Google в своих источниках сообщает, что эксплойт для CVE-2022-4135 уже существует. Стоит заметить, что установление любых обновлений программного обеспечения возможно только после оценки всех сопутствующих рисков.

2. *Использование средств антивирусной защиты с функцией контроля доступа к веб-ресурсам.*

Антивирусы с функциями контроля использования программ, устройств и веб-ресурсов являются эффективным средством защиты от спуфинг-атак, поэтому целесообразно использование программного обеспечения такого типа для борьбы с угрозами, возникающими на базе уязвимости BDU:2022-06064. В настоящий момент существуют решения отечественных производителей, позволяющие устанавливать Веб-контроль.

3. *Применение систем обнаружения и предотвращения вторжений.*

Такие средства защиты используют метод отслеживания несанкционированных попыток получения доступа к защищаемым ресурсам, называемый мониторингом управления доступом. Задача решений систем обнаружения и предотвращения вторжений состоит в выявлении, а также регистрации уязвимостей в безопасности внутренней инфраструктуры.

Можем выделить и другие эффективные меры защиты, такие как введение регламента по использованию ресурсов сети «Интернет»; отказ от использования запуска браузеров от имени администратора в пользу запуска от имени пользователя минимальными возможными

привилегиями в операционной системе и использование альтернативных веб-браузеров, в которых отсутствует рассматриваемая уязвимость.

Далее будет представлена информация об атаках, которая получена с помощью мониторинга открытых источников в сети Интернет и может не соответствовать действительности [1-3].

Атаки

1. В Telegram-канале (https://t.me/itarmyofukraine2022) с 5 октября 2022 года осуществляется координация DDoS-атаки на сайты российских магазинов торгово-бытового обеспечения военнослужащих «Военторг». Сообщается, что список атакуемых сайтов включает 72 адреса.

2. В Telegram-канале (https://t.me/CyberSquattingChannel) опубликованы

URL-адреса, используемые в атаках с применением социальной инженерии, схожие с адресами интернет-ресурсов крупных российских компаний (такие, как: new-sber.run.app; sberbank.com.cn; sberget.com; sbertibud.cf; sberukmud.ga; investments-gazprom.online; bonus-vtb24-pozdravlenie.site; sushi-for-you-vtb.ru; sushi-tebe-vtb.ru; sushi-vam-vtb.ru; sushi-vsem-vtb.ru; vtb-bonus.site; gosuslugi-r.ru; gosuslugi.vercel.app; gosuslugl.vercel.app; ozon-hd.hu; wb-ozon-obuchenie.ru; yandex-dellivery.net.ru; yandex-leonteva.ru; yandex-oplata37124.online; yandex-oplata37317.online; yandex-yana.ru; cdek-oplata24127.online; cdek-oplatazakaza.online avito.id13860.ru; avito.id7355.ru; avito.id9217.ru; booking.id1704.ru; cdek.id1789523.ru; cdek.id7355.ru; cdek.id7360.ru; cdek.ord-0125.ru; mvd-oplata.top; mvideo.id1704.ru; ozon.id7354.ru; ozon.id7358.ru; wildberries.id47218.ru; wildberries.ord1838.ru; yandex-id8512.ru; youla-paymo.ru; youla.id11327.ru; youla.id13860.ru; youla.id13875.ru; youla.id5755.ru; youla.id7355.ru; youla.id7358.ru; youla.id9215.ru; youla.id9217.ru; youla.id9218.ru) [4].

Заключение

В ходе исследования была изучена научная литература, посвященная уязвимостям в веб-браузерах, а также возможным решениям для предотвращения сетевых атак. Полученные результаты были обобщены, а также была выделена уязвимость BDU:2022-06064, приведены ее основные характеристики. Поставленные цели и задачи были достигнуты в полном объеме. Можно сделать вывод о том, что исследование угроз в сети интернет, в том числе атак, проводимых при использовании веб-браузеров остается важной задачей, стоящей перед специалистами информационной безопасности [5].

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
2. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.
3. Пестов И. Е. и др. Программа обеспечения системы компьютерного зрения на основе библиотеки OpenCV // Свидетельство о регистрации программы для ЭВМ. – 2020. – № 2020664289

4. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры // Свидетельство о регистрации программы для ЭВМ. – 2020. – № 2020617705
5. Методический документ ФСТЭК России Профиль защиты систем обнаружения вторжений уровня узла пятого класса защиты ИТ.СОВ.У5.ПЗ

References

1. Volkogonov V. N., Gelfand A. M., Derevyanko V. S. Relevance of automated control systems // Actual problems of infotelecommunications in science and education (APINO 2019). - 2019. - S. 262-266.
2. Kazantsev A. A. et al. Creation and management of the Security Operations Center for effective use in real conditions // Actual problems of infotelecommunications in science and education (APINO 2019). - 2019. - S. 590-595.
3. Pestov I. E. et al. Program for providing a computer vision system based on the OpenCV library // Certificate of registration of a computer program. - 2020. - № 2020664289
4. Krasov A. V. et al. Software implementation of intrusion and anomality prevention in the network infrastructure // Certificate of registration of a computer program. - 2020. - № 2020617705.
5. Methodological document of the FSTEC of Russia profile of protection of intrusion detection systems of the node level of the fifth protection class IT.SOV.U5.PZ

Рыжов К.Ю., Ненашев С.А. Подавление боковых лепестков сжатого сигнала // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 31–34

Международный журнал информационных технологий и энергоэффективности

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

УДК 621.376

ПОДАВЛЕНИЕ БОКОВЫХ ЛЕПЕСТКОВ СЖАТОГО СИГНАЛА

[1]Рыжов К.Ю., [2]Ненашев С.А.
ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Санкт-Петербург, Россия (190000, Санкт-Петербург, ул. Большая Морская, д. 67, лит. А), e-mail: [1]konstantin.r02.27@gmail.com, [2]nenashev_sergey178@mail.ru

Кодирование радиолокационных сигналов может выполняться с использованием последовательностей для фазового кодирования, таких как коды Баркера и соответствующие вложенные коды. Целью работы являлось получение результатов в области обработки широкополосных сигналов в части подавление боковых лепестков. При получении результатов использовались аппараты имитационного моделирования, а также экспериментального исследования кодов и вложенных кодовых последовательностей Баркера. Результатами являются автокорреляционные функции кодовых конструкций Баркера с подавленными боковыми лепестками. Эти результаты является основой для обеспечения большей помехоустойчивости таких широкополосных сигналов и доказывает целесообразность их применения для различных систем обнаружения гражданского применения.

Ключевые слова. коды Баркера, подавление боковых лепестков, автокорреляционная функция.

COMPRESSED SIDELOBE SUPPRESSION

[1]Ryzhov K. Yu., [2]Nenashev S.A.
Saint-Petersburg State University of Aerospace Instrumentation, Saint-Petersburg, Russia (SUAI, 67, Bolshaya Morskaia str., Saint-Petersburg, 190000, Russia), e-mail: [1]konstantin.r02.27@gmail.com, [2]nenashev_sergey178@mail.ru

Radar signal coding may be performed using phase coding sequences such as Barker codes and corresponding nested codes. The aim of the work was to obtain results in the field of broadband signal processing in terms of sidelobe suppression. When obtaining the results, simulation tools were used, as well as an experimental study of Barker codes and nested code sequences. The results are the autocorrelation functions of Barker code structures with suppressed side lobes. These results are the basis for providing greater noise immunity of such wideband signals and prove the feasibility of their application for various civil detection systems.

Keywords: Barker codes, sidelobe suppression, autocorrelation function.

Сжатие импульсов – это способ обработки широкополосных сигналов, который позволяет получить высокое разрешение по координате «дальность» с использованием кодированных сигналов [1-7]. При этом у такого сжатого сигнала возникают боковые лепестки, для которых требуется реализовать процесс подавления.

Боковые лепестки автокорреляционной функции (АКФ) для кода Баркера равны единице. Некоторые боковые лепестки АКФ кода Баркера возможно привести к нулю, если за соответствующим согласованным фильтром следует линейный фильтр подавления боковых лепестков с импульсной характеристикой, заданной формулой:

$$h(t) = \sum_{k=-N}^{N} \beta_k \delta(t - 2k\tau_0), \quad (1)$$

где N – порядок фильтра, коэффициенты $\beta_k\,(\beta_k = \beta_{-k})$ должны быть определены δ() – дельта-функцией и τ_0- шириной импульса подкода Баркера. Фильтр $h(t)$ порядка N производит (рисунок 1) N ноль боковых лепестков по бокам от главного лепестка АКФ. Амплитуда и ширина главного лепестка не изменяются.

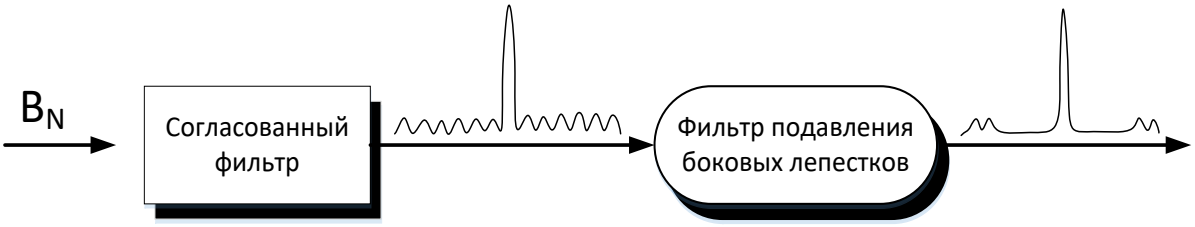

Рисунок 1 – Линейный фильтр подавления боковых лепестков порядка N может быть использован для получения N нулевых боковых лепестков в автокорреляционной функции (N=4)

Чтобы проиллюстрировать этот подход, следует рассмотреть случай, где входные данные к соответствующему фильтру B_{11} и предположим N=4. Значения АКФ для B_{11}.

$$R_{11} = \begin{Bmatrix} -1{,}0, -1{,}0, -1{,}0, -1{,}0, -1{,}0, -11{,}0, -1{,}0, -1{,}0, \\ -1{,}0, -1{,}0, -1 \end{Bmatrix} \quad (2)$$

Выход трансверсального фильтра представляет собой дискретную свертку между его импульсной характеристикой и последовательностью R_{11} . На этом этапе нам нужно вычислить коэффициенты β_k, которые обеспечат желаемый выходной сигнал с фильтра (т. е. неизменный главный лепесток и четыре нулевых уровня боковых лепестков).

Выполнение дискретной свертки, как определено в формуле (2) и сбор равных членов $(\beta_k = \beta_{-k})$ дает следующий набор из пяти линейно независимых уравнений:

$$\begin{bmatrix} 11 & -2 & -2 & -2 & -2 \\ -1 & 10 & -2 & -2 & -2 \\ -1 & -2 & 10 & -2 & -1 \\ -1 & -2 & -1 & 11 & -1 \\ -1 & -1 & -1 & -1 & 11 \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \end{bmatrix} = \begin{bmatrix} 11 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (3)$$

Решение системы линейных уравнений (3) дает

$$\begin{bmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \end{bmatrix} = \begin{bmatrix} 1.1342 \\ 0.2046 \\ 0.2046 \\ 0.1731 \\ 0.1560 \end{bmatrix} \quad (4)$$

Обратите внимание, что значение первого уравнения, равного 11, а всех других уравнений, равно 0, а затем решение для β_k является результатом того, что основной пик останется неизменным, и что следующие четыре боковых лепестка будут равны 0. До сих пор предполагалось, что закодированные импульсы имеют прямоугольную форму. Используя импульсы других форм, например, гауссовский, можно произвести уменьшение боковых лепестков и увеличить коэффициента сжатия кодо-модулированного сигнала.

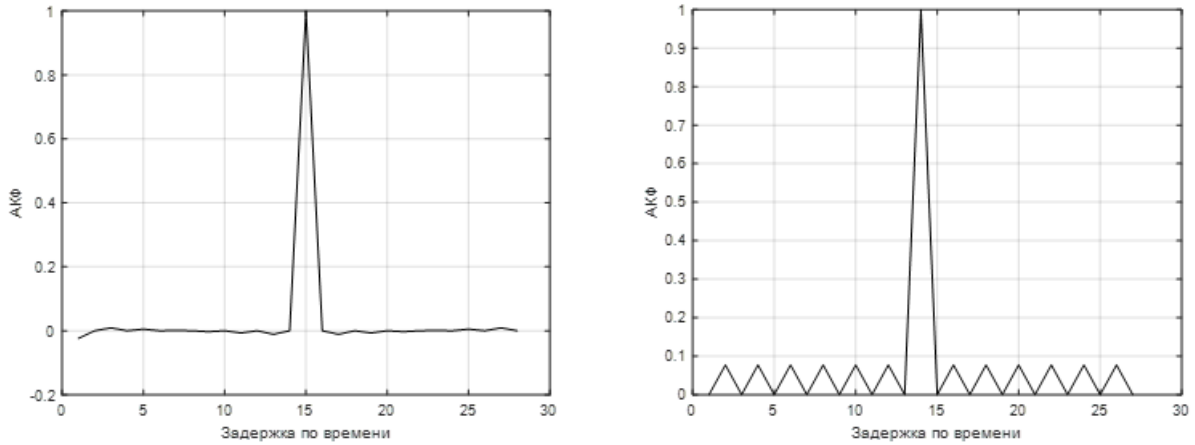

Рисунок 2 – АКФ кода Баркера при N= 13
до (а) и после (б) подавления боковых лепестков

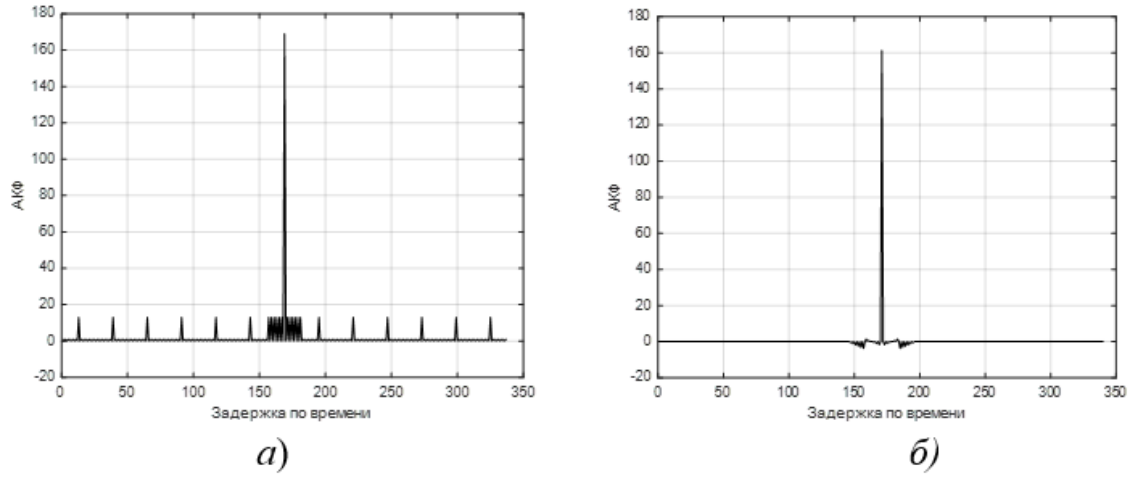

Рисунок 3 – АКФ вложенной конструкции Баркера при N= 13x13
до (а) и после (б) подавления боковых лепестков

Результат сжатия с одновременным подавлением боковых лепестков показаны на рисунках 2 и 3.

В данной работе была рассмотрена возможность подавление боковых лепестков сжатого сигнала, модулированного кодом Баркера, а также рассмотрен аналогичный процесс для вложенных кодовых конструкций. Значимость результатов обеспечивается перспективностью исследования, влияющего на становление и развитие методов выделения, обнаружения и обработки полезной информации. Результаты работы имеют длительное последействие,

поскольку с появлением оригинальных новых кодов и кодовых конструкций возникает потребность их исследования, модификации, обобщения и расширения области применения.

Финансовая поддержка

Исследование выполнено за счет гранта Российского научного фонда (проект № 22-79-00303).

Список литературы

1. Варакин Л. Е. Системы связи с шумоподобными сигналами.: Радио и связь, 1985, 384 с.
2. Букалев П. А. Радиолокационные системы: учеб. Для вузов. М.: Радиотехника, 2004. 320 с.
3. Трухачев А. Радиолокационные сигналы и их применения. Воениздат. 205 г., стр. 320.
4. А.С. Верба, Б.Г. Татарский. Радиолокационные системы авиационно-космического мониторинга земной поверхности и воздушного пространства. Монография. б.м. : Радиотехника, 2014 г. стр. 576.
5. В. А. Ненашев, В. А. Синицын, С. А. Страхов Исследование влияния индустриальных помех на характеристики сжатие фазоманипулированных сигналов в первичных РЛС // Инновационные технологии и технические средства специального назначения: Труды IX общероссийской научно-практической конференции. В 2 томах, Санкт-Петербург, 16–18 ноября 2016 года / Министерство образования и науки Российской Федерации; Балтийский государственный технический университет "Военмех" им. Д. Ф. Устинова. – Санкт-Петербург: Балтийский государственный технический университет "Военмех", 2017. – С. 351-355.
6. R., Mahafza B. Radar Systems Analysis and Design using MATLAB. Chapman&Hall. 2000 г., стр. 532.
7. Шепета А. П., Ненашев В. А. Система сжатия ФМ импульса в задачах высокоточного картографирования. Хроники объединенного фонда электронных ресурсов. Наука и образование. 2014 г., стр. 14)

References

1. Varakin L. E. Communication systems with noise-like signals.: Radio and communication, 1985, 384 p.
2. Bukalev P. A. Radar systems: textbook. For universities. M.: Radiotehnika, 2004. 320 p.
3. Trukhachev A. Radar signals and their applications. Military publishing house. 205, p. 320.
4. A.S. Verba, B.G. Tatar. Radar systems for aerospace monitoring of the earth's surface and airspace. Monograph. b.m. : Radio engineering, 2014, p. 576.
5. V. A. Nenashev, V. A. Sinitsyn, S. A. Strakhov Investigation of the influence of industrial interference on the compression characteristics of phase-shift keyed signals in primary radars // Innovative technologies and special-purpose technical means: Proceedings of the IX All-Russian Scientific and Practical Conference. In 2 volumes, St. Petersburg, November 16–18, 2016 / Ministry of Education and Science of the Russian Federation; Baltic State Technical University "Voenmekh" D. F. Ustinova. - St. Petersburg: Baltic State Technical University "Voenmeh", 2017. - P. 351-355.
6. R., Mahafza B. Radar Systems Analysis and Design using MATLAB. Chapman & Hall. 2000, p. 532.
7. A. P. Shepeta and V. A. Nenashev, FM pulse compression system in high-precision mapping problems. Chronicles of the United Fund of Electronic Resources. Science and education. 2014, p. 14)

Баимов Р.И. Проектирование антенн для устройств IOT // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 35–39

Международный журнал информационных технологий и энергоэффективности

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

УДК 621.396.677; 004.7

ПРОЕКТИРОВАНИЕ АНТЕНН ДЛЯ УСТРОЙСТВ IOT

Баимов Р.И.
Южно-Уральский государственный университет, г. Челябинск, Россия (454080, г. Челябинск, пр. Ленина, 76), e-mail: baimov.roman@internet.ru

В данной статье построена модель, геометрия антенны для устройств интернета вещей. Проведен анализ данной антенны в программе моделирования электромагнитного поля методом конечных элементов- HFSS. Для стабильной работы устройств IoT необходимо применение антенн пятого поколения 5G.

Ключевые слова: технология IoT, 5G, моделирование.

ANTENNA DESIGN FOR INTERNET OF THINGS IOT DEVICES

Baimov R.I.
South Ural State University, Chelyabinsk, Russia (454080, Chelyabinsk, Lenin Ave., 76), e-mail: baimov.roman@internet.ru

In this article, a model is built, the antenna geometry for Internet of Things devices. An analysis of this antenna was carried out in the program for modeling the electromagnetic field by the finite element method - HFSS. In order for the IoT technology to work stably, it is necessary to use fifth-generation 5G antennas.

Keywords: IoT technology, 5G, modeling.

Введение

IoT— это множество умных устройств, подключенных к интернету, которые обмениваются данными. Технология IoT имеет применение в разных отраслях для различных целей: в промышленности, сельском хозяйстве, здравоохранении.

Технология интернет вещей тесно связана с развитием 5G сетей. Данные технологии способны предоставить уникальные возможности взаимодействия умных устройств[3]. Протоколы имеющихся сетей не способны справиться с потоками информации умных устройств. Они урезают скорость обслуживания всей сети. Для расширения технологии устройств IoT, целесообразно наращивать возможности 5G связи путем совершенствования конструкции существующих антенн.

Модель антенны

Модель, геометрия антенны в программе HFSS[1] представлена на рисунке 1.

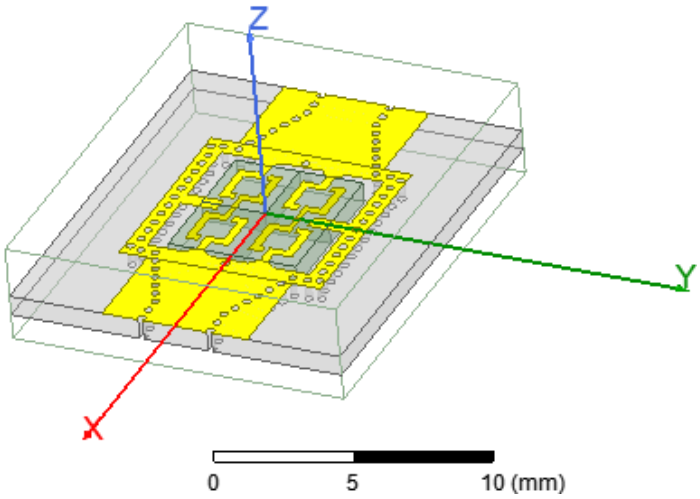

Рисунок 1 – Модель 5G антенны

Анализ S- параметров антенны

Параметры рассеяния или S-параметры описывают поведение линейных электрических сетей при воздействии различных стационарных стимулов электрическими сигналами.

Эти параметры полезны для нескольких отраслей электротехники, включая электронику, проектирование систем связи и особенно для СВЧ-техники.

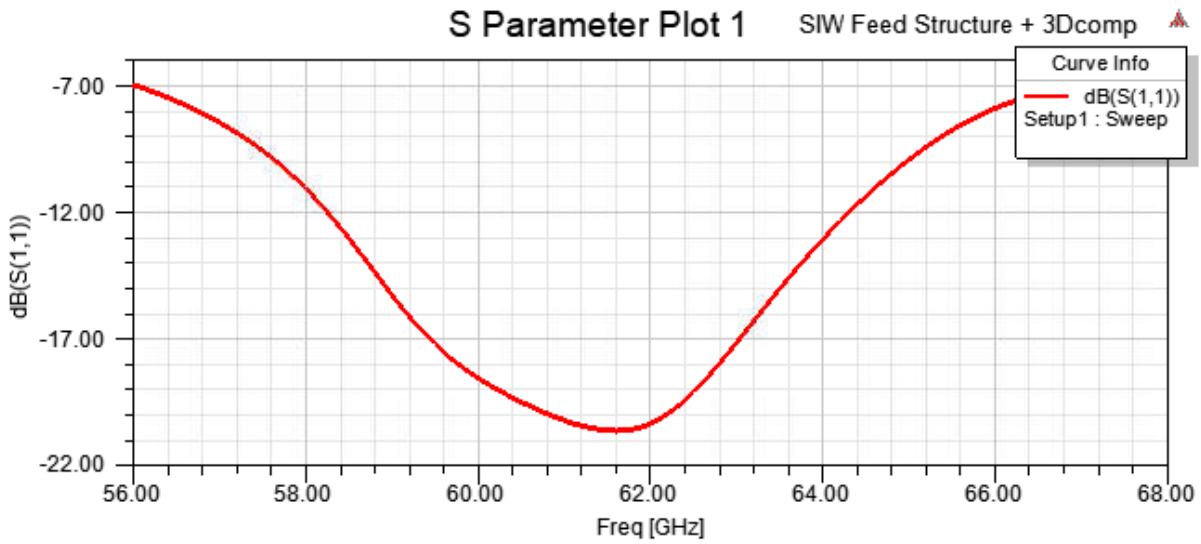

Рисунок 2 – График S- параметров

Антенна имеет пиковое усиление около 20 дБ на частоте 61 ГГц [2], что соответствует технологии сетей 5G (рисунок 2).

Диаграмма направленности антенны

Диаграмма направленности показывает зависимость коэффициента усиления антенны или коэффициента направленного действия от направления антенны в заданной плоскости, представленной в полярной системе координат рисунки 3 и 4 .

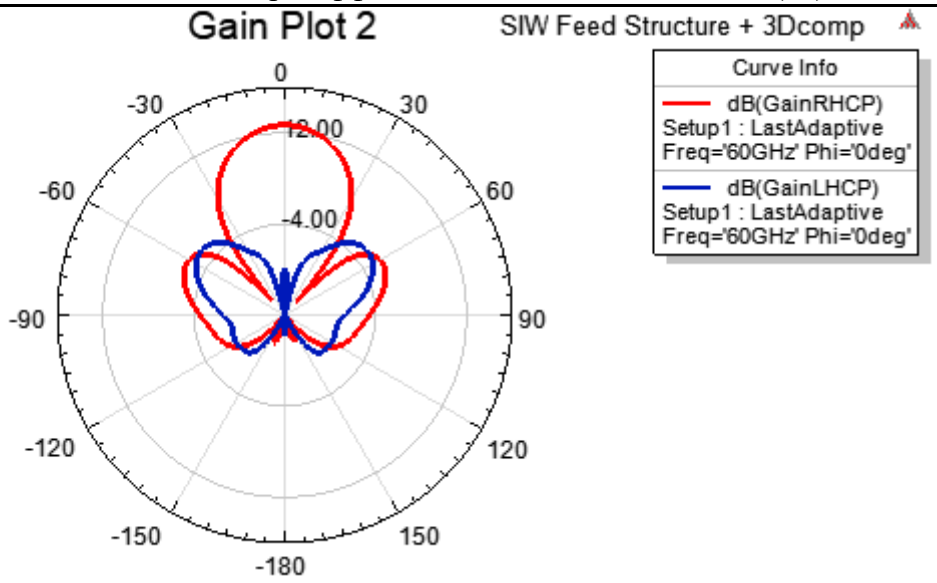

Рисунок 3 – ДН 5G антенны при $\varphi = 0^0$

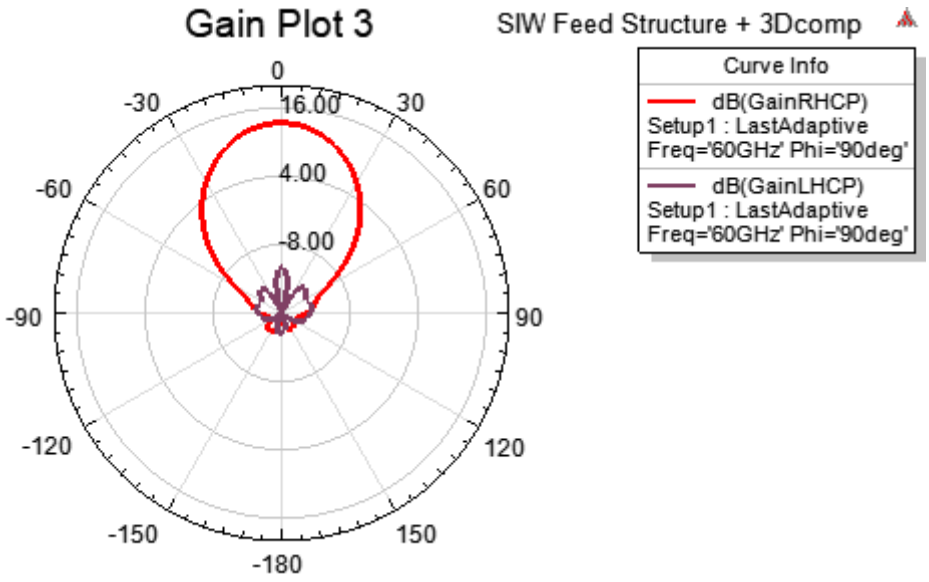

Рисунок 4 – ДН 5G антенны при $\varphi = 90^0$

Платформа Интернета вещей IoT

Спроектирована, собрана платформа интернета вещей, её схема представлена на рисунке 5

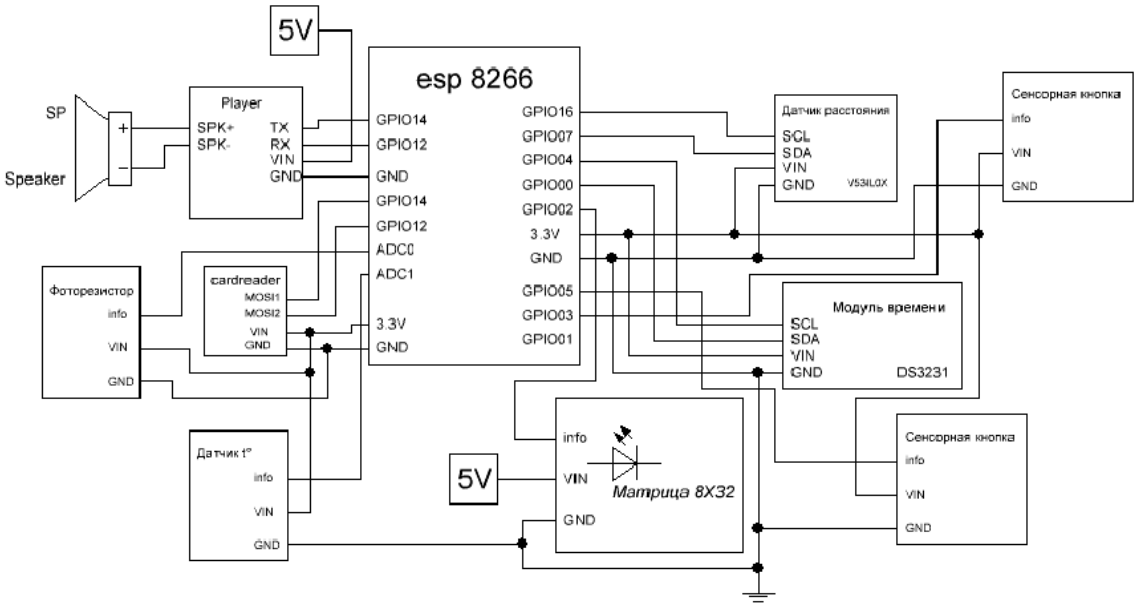

Рисунок 5 – Схема платформы IoT

Связь между другими устройствами осуществляется 5 ГГц сетью.
Собранная платформа (рисунки 6-8).

Рисунок 6 – Платформа отображает время

Рисунок 7 – Платформа отображает погоду

Рисунок 8 – Отображение светомузыки на платформе

Платформа способна отображать время, погоду, воспроизводить музыку. Регулирование яркости и громкости происходит через датчик дальномера. Чем ближе наша рука к станции, тем выше громкость или яркость. Переключать мелодии можно, используя датчик жестов или сенсорные кнопки на корпусе. В станцию включена функция мягкого пробуждения. Ближе к пробуждению светодиодная матрица увеличивает яркость. Матрица имитирует восход солнца – такое пробуждение будет максимально естественным и спокойным.

Платформа представляет собой IoT сеть, к которой можно подключать большое количество умных устройств, взаимодействие между которыми происходит через технологию 5G.

В данной работе построена модель 5G антенны. Используя метод конечных элементов – HFSS, проведен анализ 5G антенны. Построена диаграмма направленности и график параметров рассеяния антенны. IoT даст рывок в развитии беспилотников, автоматизации производства, технологии «умного дома» и «умного города». IoT может существенно улучшить многие сферы нашей жизни и помочь нам в создании более удобного, умного и безопасного мира.

Список литературы

1. Ansys HFSS URL: https://www.ansys.com/products/electronics/ansys-hfss (дата об-ращения 11.21.2022);
2. Dia’aaldin, J. B., Liao, S., & Xue, Q., “High gain and low cost differentially fed circu-larly polarized planar aperture antenna for broadband millimeter-wave applications,” IEEE Trans. Antennas Propag. 64(1), 33-42 (2016);
3. Lu Tan, Neng Wang, “Future internet: The internet of Things”, 2010.

References

1. Ansys HFSS URL: https://www.ansys.com/products/electronics/ansys-hfss (accessed 11.21.2022);
2. Dia’aaldin, J. B., Liao, S., & Xue, Q., “High gain and low cost differentially fed circu-larly polarized planar aperture antenna for broadband millimeter-wave applications,” IEEE Trans. Antennas Propag. 64(1), 33-42 (2016);
3. Lu Tan, Neng Wang, “Future internet: The internet of Things”, 2010)

Кононенко Д. В., Чернова М. А. Визуальные аспекты принципа создания сайта // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 40–43

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

ВИЗУАЛЬНЫЕ АСПЕКТЫ ПРИНЦИПА СОЗДАНИЯ САЙТА

[1]Кононенко Д. В., [2]Чернова М. А.
[1,2] ФГБОУ ВО "Российский государственный гуманитарный университет", Москва, Россия (125993, г. Москва, Миусская пл., д.6), e-mail: [1]kononenko.darya14@gmail.com, [2]marchernov@yandex.ru
[1]ООО «КАР СИСТЕМС», Москва, Россия (115597, г. Москва, Гурьевский проезд, д.35/58)

Целью данной статьи является определение основных принципов создания эффективного сайта с учетом правильно подобранных визуальных аспектов. Главной задачей сайта является привлечение новых клиентов, а именно, получение новых лидов. Поэтому стоит учитывать, что сайт должен быть оформлен так, чтобы клиент задержался на странице, смог получить полную информацию о продукте, товаре или услуге. Именно по этой причине, стоит большое внимание уделять всем основным принципам оформления сайта.

Ключевые слова: сайт; визуальные аспекты; дизайн сайта; привлечение клиентов; тренды дизайна; шрифт; лэндинг; вэб-дизайн; повышение лояльности.

VISUAL ASPECTS OF THE PRINCIPLE OF SITE CREATION

[1]Kononenko D. V., [2]Chernova M. A.
[1,2] Russian State University for the Humanities, Moscow, Russia (125993, Moscow, Miusskaya sq., 6), e-mail: [1]kononenko.darya14@gmail.com, [2]marchernov@yandex.ru
[1]CAR SYSTEMS LLC, Moscow, Russia (115597, Moscow, Guryevskiy proezd, 35/58)

The purpose of this article is to determine the basic principles of creating an effective website, taking into account properly chosen visual aspects. The main task of the site is to attract new customers, namely, to get new leads. Therefore, it is worth bearing in mind that the site should be designed so that the client will linger on the page, be able to get complete information about the product, product or service. For this reason, it is worth paying great attention to all the basic principles of site design.

Keywords: website; visual aspects; website design; attracting customers; design trends; font; lending; web-design; increasing loyalty.

В настоящее время правильный и стильный дизайн сайта является актуальной и главной задачей многих компаний. Если учитывать последствия COVID-19, когда в определенный момент времени, многочисленным компаниям пришлось перейти с оффлайн-площадок, в онлайн, визуально привлекающий и максимально удобный для клиента с точки зрения пользования сайт стал одним из конкурентных преимуществ для огромного ряда компаний. Чем более грамотно составлен сайт, тем проще привлечь внимание клиентов, а самое главное, удержать их внимание. Как показывает практика, человек всегда анализирует и оценивает сайт по первой странице. Это происходит как сознательно, так и бессознательно. В последствии, для клиента будет важен полный функционал сайта и возможность найти нужную

информацию максимально быстро. Чем проще клиенту пользоваться сайтом, находить ответы на все свои вопросы и не прибегать к использованию помощи по сайту или звонков, тем более он лоялен к бренду и продукту. Гораздо больше вероятность, что произойдет покупка товара или продукта, либо человек воспользуется предложенной услугой. И несомненно, хорошо разработанный сайт увеличивает конкурентоспособность компании в целом.

Наиболее важной задачей при разработке сайта можно считать юзабильный веб-дизайн, то есть такой дизайн сайта, который отвечает на все потребности клиента и позволяет ему максимально просто и быстро находить необходимую ему информацию на странице. Для того чтобы сайт соответствовал всем трендам дизайна, а самое главное, юзабилити, необходимо формировать путь пользования сайтом с точки зрения клиента. Это позволяет структурировать все блоки сайта или лендинга, правильно сформулировать миссию, задачи и цели сайта, и каждой страницы, в частности. Многие пропускают данный пункт при разработке сайта, потому что не хотят тратить на это время, но проведя ряд опросов, составив определенные портреты клиентов, можно выявить наиболее подходящую структуру сайта, которая закроет все потребности клиента.

Также необходимо обратить внимание на визуальную составляющую сайта и каждой страницы, а именно правильное и привлекательное использование всех компонентов и блоков, которые могут первыми бросаться в глаза посетителю. Большое внимание уделяется цвету, макету, фотографиям, шрифтам, фону – все это должно гармонично смотреться и соответствовать друг другу, так как именно эти факторы влияют на первое впечатление и последующее пользование сайтом.

Безусловно, существует еще ряд аспектов веб-дизайна, например, интерактивность, которые занимают важную позицию при разработке сайта. Но именно визуальная составляющая, то есть внешняя привлекательность и первое впечатление очень сильно влияют на конверсию посадочной страницы [1-3].

Можно выделить несколько ролей привлекательности в дизайне сайта:

1. Привлечение внимания

Людям нравится смотреть на красивые вещи, и, если есть выбор, они всегда предпочтут красивый, симпатичный объект уродливому или даже нейтральному. Часто можно заметить, что сайт, который разработан, не учитывая цветовую гамму, не соответствует корпоративному цвету и не дает понимания что за продукт, что за компания и визуально не привлекает – никогда не будет эффективным. Но стоит обратить внимание, что представления о красоте весьма субъективны, поэтому вы должны досконально изучить вкусы своей целевой аудитории или протестировать свои лендинги.

2. Первое впечатление

Можно провести аналогию с обычной жизнью. В реальном мире, когда люди первый раз видятся и знакомятся, первое впечатление может сильно повлиять на их дальнейшее взаимодействие и общение, и в целом, влияют на коммуникации в дальнейшей перспективе. То есть за считанные минуты разговора, мы уже имеем представление нравится ли нам человек, интересен ли он, и стоит ли общаться с ним дальше [5]. Все тоже самое, мы можем заметить и в интернет-ресурсах. Если человек заходит на сайт, а первое его впечатление оказалось негативным, то вряд ли, человек вернется на сайт и тем более, захочет приобрести там товар или услугу. И к сожалению, изменить первое впечатление не всегда бывает просто. А самое главное, что дизайн сайта никогда не должен быть максимально загроможден всей

информацией сразу, необходимо всегда придерживаться структуры и лаконичности, так посетителю будет проще ориентироваться на сайте и находить нужную ему информацию. Для этого всегда изначально нужно проводить тексты с фокус группы для разработки пути пользования клиента – данный способ позволяет минимизировать ошибки в сайте, и сделать его максимально удобным для пользования.

3. Построение отношений

Визуальная привлекательность помогает в построении отношений с целевой аудиторией. Если посетители идентифицируют себя, свои вкусы и склонности с вашим ресурсом, если он обращается к посетителю как к единомышленнику, значит, вы сделали большой шаг к построению долгосрочных отношений с таргет-группой и конечно продажам. О важности данной связи даже не стоит говорить. Мы идентифицируем себя через искусство, музыку, увлечения, бренды — а также через веб-сайты, которыми пользуемся. Идеальный вариант для любого бренда — если его рассматривают как символ определенного образа жизни. Если же сайт не отражает наши увлечения и представления о себе, мы склонны продолжать поиски в других местах.

4. Повышение лояльности

Визуальная привлекательность может оправдать другие, менее удачные аспекты целевой страницы. Разумеется, всегда стоит стремиться к идеалу, но достичь его бывает трудно. Поэтому если визуальная часть выполнена первоклассно, посетители будут более снисходительны к прочим составляющим, которые получились менее удачными.

5. Влияние на эмоции

Хорошее изображение стоит тысячи слов — это особенно верно при общении на эмоциональном уровне [4]. Через фото и прочие визуальные элементы можно передать чувства: радость, восторг, печаль, и даже жалость. Кроме того, можно разбудить воспоминания и эмоции, такие как доверие, комфорт, надежду и уверенность в себе — сильные, позитивные чувства, способные привлечь посетителей, и подсадить их на «эмоциональный крючок».

Важно помнить, что в целом визуальный аспекты должны отражать единый стиль компании. То есть при переходе на страницу сайта, например, с контекстной рекламы, сразу был заметен брендированный стиль, определенные цвета, шрифты, фото, подходящие под стиль и сочетающиеся между собой – в таком случае, у клиента всегда будет ассоциация с брендом, запомнится часть визуальных аспектов, поэтому увеличится узнаваемость самого бренда.

Исходя из все этих пунктов, мы можем сделать вывод, что дизайн сайта играет важную и неотъемлемую роль развития бренда. Так как сайт полностью отражает компанию, ее цель и миссию, является проводником в отношениях бренда и клиента. С точки зрения психологии человека, мы всегда обращаем внимание на первое впечатление, поэтому сайт нужно создавать так, чтобы произвести впечатление и он запомнился клиенту. А удобство использования всех блоков и страниц сайта позволит повысить лояльность клиентов.

Список литературы

1. Дакетт, Д. HTML и CSS. Разработка и дизайн веб-сайтов / Джон Дакетт ; пер. с англ. Райтман М. А. – Эксмо, 2020. – 480 с.

2. Диб, А. Одностраничный маркетинговый план. Как найти новых клиентов, заработать больше денег и выделиться из толпы / Аллан Диб ; пер. с англ. Чомахидзе-Доронина Мария. – Библос, 2018. – 228 с.
3. Роэм Д. Визуальное мышление. Как «продавать» свои идеи при помощи визуальных образов / Дэн Роэм; пер. с англ. 0. Медведь — М. : Манн, Иванов, Фербер, Эксмо, 2013. — 300 с.
4. Скотт, Б. Воплощение идей. Как преодолеть разрыв между видением и реальностью / Белски Скотт – М: Манн, Иванов и Фербер, 2013 – 208 с.
5. Уолтер, А. Эмоциональный веб-дизайн / Аарон Уолтер ; пер. с англ. Павла Миронова. — М. : Манн, Иванов и Фербер, 2012. — 144 с.

References

1. Duckett, D. HTML and CSS. Website development and design / John Duckett; per. from English. Reitman M.A. - Eksmo, 2020. - 480 p.
2. Dib, A. One-page marketing plan. How to find new clients, earn more money and stand out from the crowd / Allan Dib; per. from English. Chomakhidze-Doronina Maria. - Byblos, 2018. - 228 p.
3. Rome D. Visual thinking. How to “sell” your ideas with visual images / Dan Romem; per. from English. 0. Bear - M .: Mann, Ivanov, Ferber, Eksmo, 2013. - 300 p.
4. Scott, B. Embodiment of ideas. How to bridge the gap between vision and reality / Belsky Scott - M: Mann, Ivanov and Ferber, 2013 - 208 p.
5. Walter, A. Emotional web design / Aaron Walter; per. from English. Pavel Mironov. — M. : Mann, Ivanov i Ferber, 2012. — 144 p.

Баимов Р.И. Проектирование антенны для дальней космической связи. использование рупорных антенн в CUBESAT // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 44–48

Международный журнал информационных технологий и энергоэффективности

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

УДК 621.396.677; 629.783

ПРОЕКТИРОВАНИЕ АНТЕННЫ ДЛЯ ДАЛЬНЕЙ КОСМИЧЕСКОЙ СВЯЗИ. ИСПОЛЬЗОВАНИЕ РУПОРНЫХ АНТЕНН В CUBESAT

Баимов Р.И.
Южно-Уральский государственный университет, г. Челябинск, Россия (454080, г. Челябинск, пр. Ленина, 76), e-mail: baimov.roman@internet.ru

Сегодня космическая связь — одно из самых сложных и перспективных направлений развития коммуникационных технологий. В данной статье построена модель, геометрия рупорной антенны, которая используется для передачи радиоволн на дальние расстояния, в том числе и в космос. Проведен анализ данной антенны в программе моделирования электромагнитного поля методом конечных элементов- HFSS.

Ключевые слова: рупорная антенна, моделирование, космическая связь, HFSS, CubeSat.

ANTENNA DESIGN FOR EXTREME SPACE COMMUNICATION. USING HORN ANTENNAS IN CUBESAT

Baimov R.I.
South Ural State University, Chelyabinsk, Russia (454080, Chelyabinsk, Lenin Ave., 76), e-mail: baimov.roman@internet.ru

Today, space communications is one of the most complex and promising areas for the development of communication technologies. In this article, a model is built, the geometry of a horn antenna, which is used to transmit radio waves over long distances, including into space. An analysis of this antenna was carried out in the program for modeling the electromagnetic field by the finite element method - HFSS.

Keywords: horn antenna, modeling, space communications, HFSS, CubeSat.

Введение

Для передачи радиоволн из волновода в космос или сбора радиоволн в волновод для приема используется рупорная антенна. Данная антенна состоит из короткой прямоугольной или цилиндрической металлической трубки (волновода), закрытой на одном конце и расширяющейся в открытый пирамидальный рупор (рисунок 1).

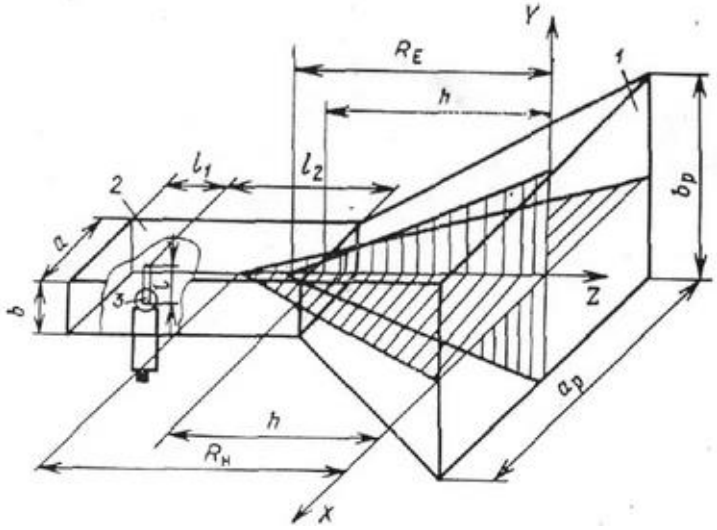

Рисунок 1 – Пирамидальная рупорная антенна

Модель антенны

Модель, геометрия антенны построена в программе HFSS[1] (рисунок 2).

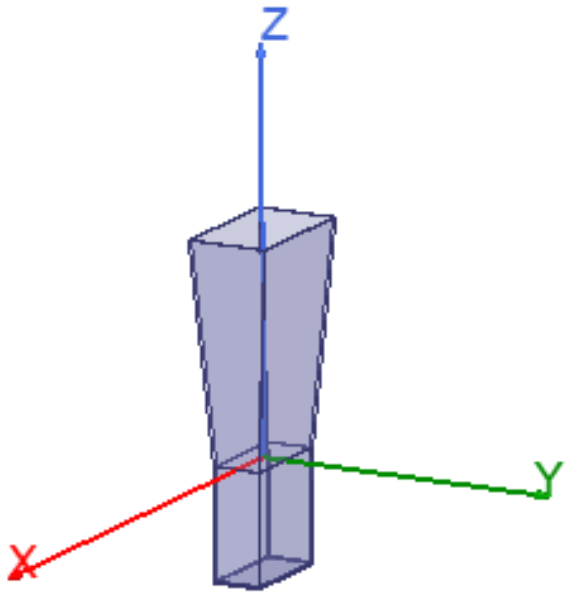

Рисунок 2 – Модель рупорной антенны

Описание: Пирамидальный рупор, предназначенный для работы на частоте 10 ГГц. Источник питания представляет собой волновод х-диапазона.

Излучающая конструкция была охвачена границей, называемой границей излучения, или попросту помещена в вакуумную коробку, на границе которой задано характеристическое сопротивление.

Диаграмма направленности антенны

Диаграмма направленности показывает зависимость коэффициента усиления антенны или коэффициента направленного действия от направления антенны в заданной плоскости, представленной в полярной системе координат (рисунок 3, 4).

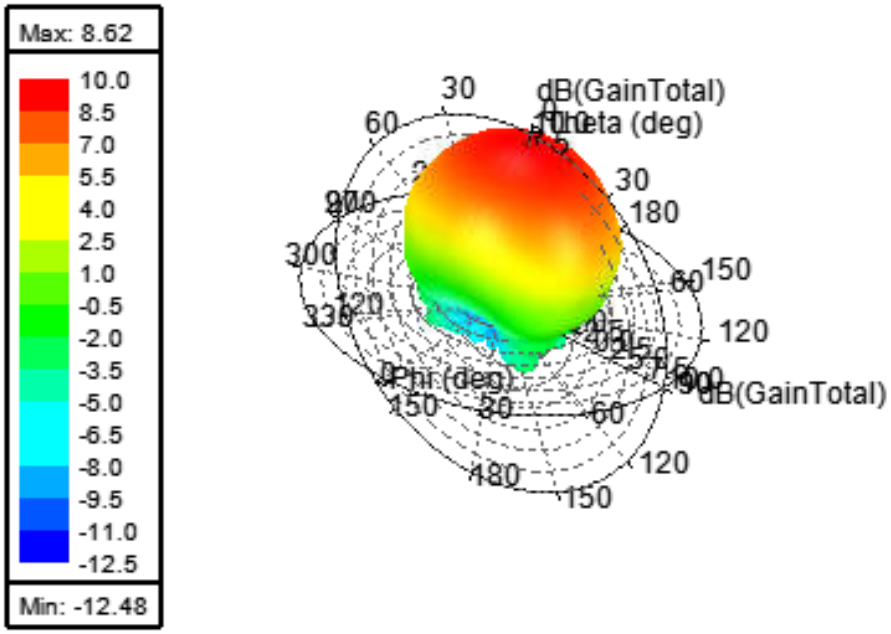

Рисунок – 3. 3D диаграмма антенны в дальней зоне

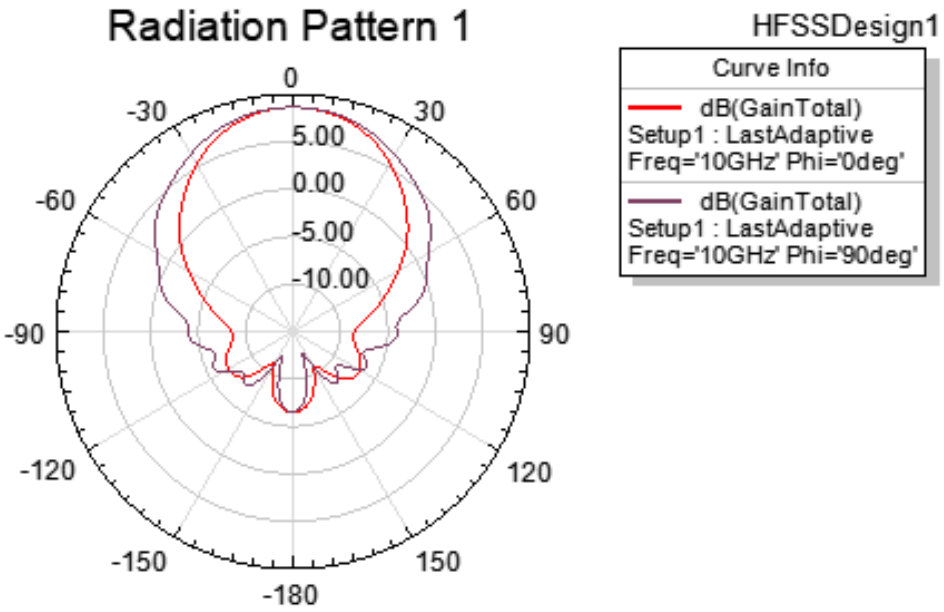

Рисунок 4 – ДН рупорной антенны

Рупор антенны формирует осесимметричную диаграмму направленности с практически неизменной шириной главного лепестка.

Диаграмма направленности рупорной антенны представляет угловое распределение плотности потока мощности или энергии в единицу угла. Прибор широкополосный, имеет питающую линию и небольшой уровень задних лепестков. Антенна имеет широкий коэффициент направленного действия.

Рупорные антенны могут быть использованы в CubeSat[3] (рисунок 5) на высоких частотах. Эти антенны обеспечивают хорошее усиление, а их разработка проста и хорошо изучена. Рупоры также часто используются в качестве облучателей для параболических и

плоских рефлекторных антенн из-за низкой поперечной поляризации и слабовыраженных боковых лепестков [4].

CubeSat

Рисунок 5 – спутник Cubesat[2]

Cubesat— формат сверхмалых искусственных спутников Земли. Они применяются для исследования космоса. Масса спутника составляет не более 1,5 кг.

Основной отличительной особенностью данных миниатюрных спутников является маленькая стоимость их развертывания. Для развертывания этих спутников не требуются большие ресурсы. Это способствует снижению различных рисков, а также существенно ускорит процесс запуска.

При этом их можно делать на основе готовых коммерческих электронных компонентов, что относительно легко и дешево. Обычно cubesat’ы запускаются на самую низкую околоземную орбиту, а через несколько дней или недель они уже повторно входят в атмосферу, что позволяет проигнорировать плазменную оболочку и использовать обычную электронику.

Использование в Cubesat других антенн

Многие при изготовлении Cubesat используют всенаправленный монополь или дипольную антенну (рисунок 6). Данные антенны имеют малый радиус действия. Они не гарантируют передачу стабильной радиосвязи.

Следовательно, для более качественной радиосвязи, необходимо развертывать антенны с высоким коэффициентом усиления. Для этого целесообразно использование рупорной антенны.

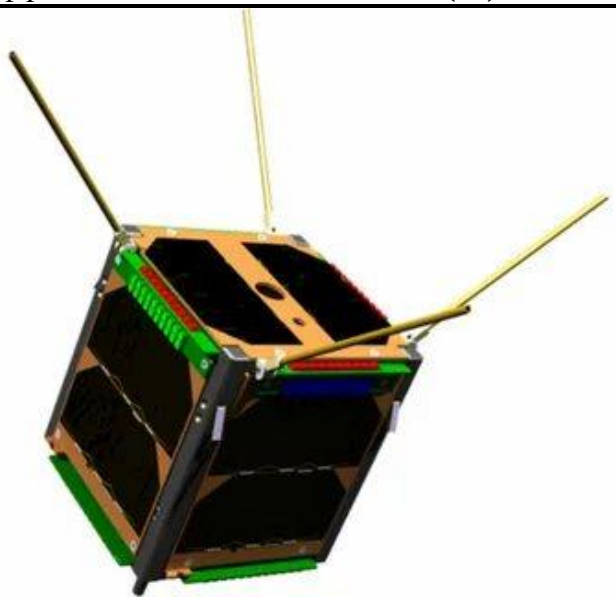

Рисунок 6 – Спутник Cubesat с дипольной антенной[2]

Вывод

Рупорная антенна подходит для использования в спутниках Cubesat. Рупорная антенна имеет высокий коэффициент усиления. Она способна обеспечить надежную радиосвязь спутника.

Список литературы

1. Ansys SIwave Signal Integrity Analysis for PCB Design. URL: https://www.ansys.com/products/electronics/ansys-siwave (дата обращения 01.12.2022);
2. CubeSat. URL: https://hd.duabhmoobtojsiab.com/1-5u-cubesat-platform-cubesat-platforms-cubesat-by-endurosat (дата обращения 01.12.2022);
3. Д. Денисов, Миниатюрные спутники для космической связи CubeSats, 01.12.2021;
4. В. П. Чернышев, Д. И. Шейнман, Распространение радиоволн антенно-фидерные устройства, «Связь», 1973.

References

1. Ansys SIwave Signal Integrity Analysis for PCB Design. URL: https://www.ansys.com/products/electronics/ansys-siwave (accessed 12/01/2022);
2. CubeSat. URL: https://hd.duabhmoobtojsiab.com/1-5u-cubesat-platform-cubesat-platforms-cubesat-by-endurosat (accessed 12/01/2022);
3. D. Denisov, Miniature satellites for space communications CubeSats, 01.12.2021;
4. V. P. Chernyshev and D. I. Sheinman, Propagation of radio waves in antenna-feeder devices, Svyaz, 1973.

Алтынников М.С. Обзор методов прогнозирования кибератак в образовательных учреждениях // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 49–53

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.89

ОБЗОР МЕТОДОВ ПРОГНОЗИРОВАНИЯ КИБЕРАТАК В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

Алтынников М.С.
Иркутский Государственный Университет Путей Сообщения, Иркутск, Россия (664074, г. Иркутск, ул. Чернышевского, д.15), e-mail: ms@altynnikov.ru

Анализ научных исследований разных стран в сфере прогнозирования кибератак показывает, что прогнозирование кибератак до их возникновения - важная, но сложная задача, поскольку поиск ранних признаков атаки из большого объема данных не является тривиальной задачей. На протяжении нескольких лет научным сообществом ведутся исследовательские работы по прогнозированию кибератак различными методами с целью создания адекватных методов заблаговременной защиты от них. В работе проеден литературный обзор на тему методов прогнозирования кибератак образовательных учреждениях. Были рассмотрены следующие методы: машинное обучение; применение предварительно известных сигнатур или прототипов определенных процессов или событий; метод интервального прогнозирования интенсивности кибератак по средствам ВНС.

Ключевые слова: прогнозирование кибератак, кибератаки, методы прогнозирования.

REVIEW OF METHODS FOR CYBER ATTACK PREDICTION IN EDUCATIONAL INSTITUTIONS

Altynnikov M.S.
Irkutsk State Transport University, Irkutsk, Russia (664074, Irkutsk, st. Chernyshevsky, 15), e-mail: ms@altynnikov.ru

Analysis of research from various countries on cyber attack prediction shows that predicting cyber attacks before they occur is an important but challenging task, as finding early warning signs of an attack from large amounts of data is not a trivial task. For several years, the scientific community has been conducting research work on predicting cyber attacks using various methods in order to create adequate methods for early protection against them. The paper reviewed the literature on methods of predicting cyber attacks in educational institutions. The following methods were considered: machine learning; application of preknown signatures or prototypes of certain processes or events; method of interval prediction of cyber attack intensity by means of PNN

Keywords: personal data, information security, security in medical institutions.

В мире более 25% утечек информации происходит из медицинских учреждений, в России доля таких утечек составляет 7%. Обращает на себя внимание высокая (в сравнении с общемировой) доля утечек, которые пришлись на банки и финансовые организации (12%). Также высоки (в сравнению с мировыми показателями) доли образовательных учреждений (14%), госорганов и силовых структур (22%) [4].

В I квартале 2022 г. количество утечек конфиденциальной информации из образовательных учреждений во всем мире выросло более чем на 15% по сравнению с

аналогичным периодом прошлого года. Хакеры и внутренние злоумышленники похищали персональные данные и другую конфиденциальную информацию [5].

Сфера образования всегда была одной из самых атакуемых отраслей. Однако, видна тенденция повышения частоты кибератак в исследуемой сфере деятельности. Часто к моменту обнаружения взлома бывает уже слишком поздно, и ущерб уже нанесен. В результате такие события заставляют задуматься о том, можно ли было предугадать эти нарушения и избежать ущерба.

Поскольку риски кибератак продолжают расти, необходимы исследования и разработки, позволяющие прогнозировать атаки вместо пассивного обнаружения вторжения. В последние годы исследователи начали использовать предиктивную аналитику, которая помогает прогнозировать будущие киберинциденты против целевых организаций до того, как они произойдут.

Машинное обучение широко используется в области кибербезопасности, в основном для обнаружения различных вредоносных действий или субъектов, например, спама и фишинга. Для целей прогнозирования они используются гораздо реже, за исключением работы [7], где текстовые данные используются для обучения классификаторов, позволяющих предсказать, может ли доброкачественная в настоящее время веб-страница стать вредоносной в ближайшем будущем. Разница между обнаружением и предсказанием аналогична разнице между диагностикой пациента, который уже может быть болен (например, с помощью биопсии), и прогнозированием того, может ли в настоящее время здоровый человек заболеть, на основе множества соответствующих факторов. Первый вариант обычно основывается на определении известных характеристик объекта, который необходимо обнаружить, а второй - на факторах, которые, как считается, коррелируют с целью прогнозирования.

Предсказание интенсивности кибератак в концепции раннего определения и предотвращения несовершенство большинства современных систем обеспеченья кибербезопасности объектов заключается в том, что при идентификации кибератак применяются предварительно известные сигнатуры или прототипы определенных процессов или событий [6]. Например, так осуществляется работа антивирусных систем, межсетевых экранов, систем обнаружения и предотвращения вторжений. В работе [6] утверждается, что подобные системы результативны только в отношении начинающих злоумышленников, которые применяют стандартные приёмы и инструменты для организации кибератак. Против опытных злоумышленников настоящие системы, часто, оказываются малоэффективными. Тут одним из перспективных направлений исследований для решения поставленной проблемы является направление по прогнозированию интенсивности кибератак на объектах средством машинного обучения. Например, такой подход удачно интегрируется в изложенную в [2,3] концепцию раннего распознавания кибератак и предупреждения о них.

Так же в [1] подробно представлен метод интервального прогнозирования интенсивности кибератак на объекты критической информационной инфраструктуры. Для организации интервального прогнозирования была избрана вероятностная нейронная сеть [8] с динамическим обновлением параметра сглаживания [9] (ВНС).

Преимущества ВНС (применительно к прогнозированию интенсивности кибератак) превалируют над недостатками [10].

Например, ВНС:

• при обучении и прогнозировании устойчива к аномальным выбросам;

• модель причисляется к моделям «ленивого» обучения и обучается предельно быстро в сравнении с моделями прочих классов;

• модель устойчива к «дисбалансу» классов обучающего множества;

• результаты работы ВНС легко поддаются интерпретации, так как работа ВНС основана на выявлении «схожих» объектов;

• не просит априорных познаний о статистических характеристиках прогнозируемого показателя.

К недостаткам можно отнести:

• «неотделимость» процесса прогнозирования от обучающих данных (в отличие, например, от параметрических моделей, где «обучение» заключается в оценке параметров моделей);

• обучающая выборка должна быть репрезентативной.

В [11] изучают отчеты, собранные с помощью антивирусных агентов McAfee, установленных на 85 000+ узлах многонационального предприятия. Используя логистическую регрессию для прогнозирования риска столкновения узлов с вредоносным ПО, они обнаружили, что узлы с высоким рейтингом сталкиваются с вредоносным ПО в 3 раза чаще по сравнению с базовым показателем. Liu, Y, Sarabi A, Zhang J, Naghizadeh P, Karir M, Bailey M, Liu M [12] собирают 258 внешних измеряемых признаков из сети организации, которые основаны на неправильно настроенных DNS (или BGP) в сети и временных рядах вредоносной активности для спама, фишинга и сканирования. Обучив классификатор Random forest, используя собранные признаки и сообщения о киберинцидентах в базе данных сообщества VERIS, Hackmageddon и Web Hacking Incidents Database, они достигли 90% точности в прогнозировании нарушений против целевой организации. Также в [13] используют журналы появления двоичных файлов и маркированные данные из антивирусных продуктов и продуктов предотвращения вторжений антивирусной компании для прогнозирования того, какие машины подвержены высокому риску заражения. Используя классификатор Random Forest и подход полусамостоятельного обучения, они достигают высокой точности (коэффициент истинных и ложных срабатываний составляет 96% и 5% соответственно) в прогнозировании риска заражения для хостов.

Заключение

Анализ научных исследований разных стран в сфере прогнозирования кибератак показывает, что прогнозирование кибератак до их возникновения - важная, но сложная задача, поскольку поиск ранних признаков атаки из большого объема данных не является тривиальной задачей. На протяжении нескольких лет научным сообществом ведутся исследовательские работы по прогнозированию кибератак различными методами с целью создания адекватных методов заблаговременной защиты от них..

Список литературы

1. Ю.М. Краковский, Б.В. Курчинский, А.Н. Лузгин. «Интервальное прогнозирование интенсивности кибератак», Доклады ТУСУР ¬– 2018 – том 21 – № 1, 2005..
2. Петренко С.А. Концепция раннего распознавания и предупреждения компьютерного нападения / С.А. Петренко, А.С. Петренко // Матер. Всерос. науч.-практ. конф. «Информационные системы и технологии в моделировании и управлении». – 2016. – С. 82–86.

3. Петренко С.А. Национальная система раннего предупреждения о компьютерном нападении / С.А. Петренко, Д.Д. Ступин. – Инополис: Изд. дом «Афина», 2017. – 440 с.
4. Аналитический центр InfoWatch. «Утечки данных. Россия. 2016 год», 2017, С. 16.
5. Аналитический центр InfoWatch. «Утечки конфиденциальной информации из сферы образования». – 2022
6. Jones M. Cyber-Attack Forecast Modeling and Complexity Reduction Using a Game-Theoretic Framework / M. Jones, G. Kotsalis, J.S. Shamma // Tarraf D. (eds) Control of Cyber-Physical Systems. Lecture Notes in Control and Information Sciences. – Heidelberg: Springer, 2013. – 380 p.
7. SO SKA, K. , CHRISTIN, N . Automatically Detecting Vulnerable Websites Before They Turn Malicious.In Proceedings of the 23rd USENIX Security Symposium(San Diego, CA, August 2014).
8. Specht D.H. Probabilistic Neural Networks / D.H. Specht // Neural Networks. – 1990. – № 3. – P. 109–118.
9. Kargapoltsev S.K. A dynamic updating algorithm of smoothing parameter values of probabilistic neural networks / S.K. Kargapoltsev, Y.M. Krakovsky, A.V. Lukyanov, A.N. Luzgin // Far East Journal of Electronics and Communications. – 2017. – Vol. 17, № 4. – P. 909–914.
10. Probabilistic neural network [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Probabilistic_ neural_network, свободный (дата обращения: 02.04.2018).
11. Yen, TF, Heorhiadi V, Oprea A, Reiter MK, Juels A (2014) An epidemiological study of malware encounters in a large enterprise In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS ’14, 1117–1130.
12. Liu, Y, Sarabi A, Zhang J, Naghizadeh P, Karir M, Bailey M, Liu M (2015) Cloudy with a chance of breach: Forecasting cyber security incidents In: Proceedings of the 24th USENIX Security Symposium (USENIX Security 15), 1009–1024.
13. Bilge, L, Han Y, Dell’Amico M (2017) Riskteller: Predicting the risk of cyber incidents In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS), 1299–1311.

References

1. Yu.M. Krakovsky, B.V. Kurchinsky, A.N. Luzgin. “Interval Prediction of Cyberattack Intensity”, TUSUR Reports ¬– 2018 – Volume 21 – No. 1, 2005..
2. Petrenko S.A. The concept of early recognition and prevention of a computer attack / S.A. Petrenko, A.S. Petrenko // Mater. Vseros. scientific-practical. conf. "Information systems and technologies in modeling and management". - 2016. - S. 82–86.
3. Petrenko S.A. National system of early warning about a computer attack / S.A. Petrenko, D.D. Stupin. - Innopolis: Ed. house "Athena", 2017. - 440 p.
4. Analytical center InfoWatch. “Data leaks. Russia. 2016”, 2017, p. 16.
5. Analytical center InfoWatch. Leaks of confidential information from the education sector. – 2022
6. Jones M. Cyber-Attack Forecast Modeling and Complexity Reduction Using a Game-Theoretic Framework / M. Jones, G. Kotsalis, J.S. Shamma // Tarraf D. (eds) Control of Cyber-Physical

Systems. Lecture Notes in Control and Information Sciences. – Heidelberg: Springer, 2013. – 380 p.

7. SO SKA, K. , CHRISTIN, N . Automatically Detecting Vulnerable Websites Before They Turn Malicious.In Proceedings of the 23rd USENIX Security Symposium(San Diego, CA, August 2014).
8. Specht D.H. Probabilistic Neural Networks / D.H. Specht // Neural Networks. - 1990. - No. 3. - P. 109–118.
9. Kargapoltsev S.K. A dynamic updating algorithm of smoothing parameter values of probabilistic neural networks / S.K. Kargapoltsev, Y.M. Krakovsky, A.V. Lukyanov, A.N. Luzgin // Far East Journal of Electronics and Communications. - 2017. - Vol. 17, No. 4. - P. 909–914.
10. Probabilistic neural network [Electronic resource]. – Access mode: https://en.wikipedia.org/wiki/Probabilistic_neural_network, free (date of access: 04/02/2018).
11. Yen, TF, Heorhiadi V, Oprea A, Reiter MK, Juels A (2014) An epidemiological study of malware encounters in a large enterprise In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS '14, 1117 –1130.
12. Liu, Y, Sarabi A, Zhang J, Naghizadeh P, Karir M, Bailey M, Liu M (2015) Cloudy with a chance of breach: Forecasting cyber security incidents In: Proceedings of the 24th USENIX Security Symposium (USENIX Security 15) , 1009–1024.
13. Bilge, L, Han Y, Dell'Amico M (2017) Riskteller: Predicting the risk of cyber incidents In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS), 1299–1311.

Рябинин П.А., Медведева С.Н. Разработка web-сервиса для организации и планирования походов по природным маршрутам // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 54–58

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

РАЗРАБОТКА WEB-СЕРВИСА ДЛЯ ОРГАНИЗАЦИИ И ПЛАНИРОВАНИЯ ПОХОДОВ ПО ПРИРОДНЫМ МАРШРУТАМ

[1]Рябинин П. А., [2]Медведева С.Н.
Казанский национальный исследовательский технический университет им. А.Н. Туполева, Казань, Россия (420000, г. Казань, ул. Карла Маркса, д.10), e-mail:
[1]Ryabinin12005@yandex.ru, [2]Medvedeva.s.005@mail.ru

В статье представлены результаты разработки программного комплекса, который позволяет упростить организацию походов по природным маршрутам и облегчает распределение походного инвентаря между участниками походов.

Ключевые слова: поход, природа, маршрут, походное снаряжение, организация походов, планирование, web-приложение, сайт.

DEVELOPMENT OF A WEB SERVICE FOR THE ORGANIZATION AND PLANNING OF HIKING ALONG NATURAL ROUTES

[1]Ryabinin P.A., [2]Medvedeva S.N.
Kazan National Research Technical University, Kazan, Russia (420000, Kazan, Karl Marx str., 10), e-mail:
[1]Ryabinin12005@yandex.ru, [2]Medvedeva.s.005@mail.ru

The article presents the results of the development of a software package that makes it possible to simplify the organization of hiking along natural routes and facilitates the distribution of hiking equipment between hiking participants.

Keywords: Hiking, nature, route, hiking equipment, hiking organization, planning, web application, website.

Разработанный программный комплекс выполнен в виде web-сервиса и имеет следующую функциональную структуру:

- регистрация пользователей
- авторизация пользователей
- подтверждение регистрации по e-mail
- создание походов
- просмотр походов, созданных другими пользователя
- просмотр кемпингов
- подача пользователем заявок на участие в походах
- просмотр прошедших походов, в которых участвовал пользователь
- распределение инвентаря между участниками похода

В настоящее время природные походы – это увлечение, которое охватывает все больше молодежи по многим причинам. Это и возможность укрепить здоровье, так как поход на природу — это альтернатива малоподвижному образу жизни за компьютером, это и возможность лучше узнать старых и завести новых хороших друзей, посидеть с ними у костра под звездным небом, это и песни под гитару, это и ни с чем не сравнимая каша из котла и чай с дымком и познание природы родного края... Но чтобы поход прошел на отлично и вспоминался яркими положительными впечатлениями, а не разочарованием из-за нужной, но забытой вещи, к походу нужно тщательно и заблаговременно подготовится, согласовать маршрут, составить список инвентаря и провизии, распределить, кто что несет и кто за что отвечает, то есть разработать групповое снаряжение похода. Правильно спланированный поход позволит хорошо отдохнуть и выполнить запланированные цели на маршруте [1-3].

Время подготовки к походу нужно провести также с пользой, общаясь с друзьями – будущими участниками похода, и современная электронная система будет совсем нелишняя, так как позволит максимально выполнить все пункты подготовки и запомнит все, что запланировано для похода и напомнит правила организации похода, например, то, что в природном походе (а это пеший поход) рюкзак с личным снаряжением и одеждой не должен весить больше 10 кг.

Таким образом, разработка электронной системы по планированию походов на природу в виде многопользовательского сайта является актуальной задачей. Web-сайт упрощает работу по организации похода, являясь электронным помощником, который обеспечивает сбор, хранение, обработку и передачу информации участникам планируемого похода [4-5].

При этом система позволяет не только планировать походы, но и вспомнить предыдущие походы, если они уже записаны в ее базу данных, что также является полезным при организации нового похода, так как помогает избежать каких-то ошибок, которые были допущены ранее. Данная разработка относится к классу многопользовательских web-сайтов. Рассмотрим принципы их разработки.

Архитектура серверной части приложения

Использование паттерна MVC позволяет отделить логику, взаимодействие с данными и представление. Инструментальное средство ASP.NET Core позволяет легко это реализовать. Однако, не смотря на такое разделение, приложение по-прежнему является одним целым. И уровень представления, и уровень логики взаимодействуют с моделями. В случае, если будет необходимо изменить представление (например, использовать WEBAPI), то изменения также будут затронуты и на уровне логики, а возможно и на уровне данных. Для решения данной проблемы можно использовать трехуровневую архитектуру приложения[6].

Классическая трехуровневая система состоит из следующих уровней, представленных на рисунке 1.

Presentation layer (уровень представления): это тот уровень, с которым непосредственно взаимодействует пользователь. Этот уровень включает компоненты пользовательского интерфейса, механизм получения ввода от пользователя. Применительно к ASP.NET MVC на данном уровне расположены представления и все те компоненты, который составляют пользовательский интерфейс (стили, статичные страницы html, javascript), а также модели представлений, контроллеры, объекты контекста запроса.

Business layer (уровень бизнес-логики): содержит набор компонентов, которые отвечают за обработку полученных от уровня представлений данных, реализует всю необходимую

логику приложения, все вычисления, взаимодействует с базой данных и передает уровню представления результат обработки.

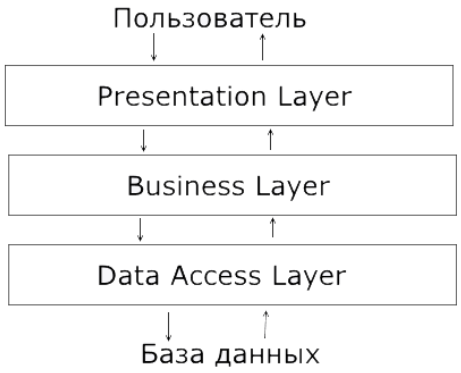

Рисунок 1 – Схема трёхуровневой системы

Data Access layer (уровень доступа к данным): хранит модели, описывающие используемые сущности, также здесь размещаются специфичные классы для работы с разными технологиями доступа к данным, например, класс контекста данных Entity Framework. Здесь также хранятся репозитории, через которые уровень бизнес-логики взаимодействует с базой данных [7-8].

Каждый уровень имеет собственные модели. Уровень представления содержит модели представления, уровень бизнес-логики использует специальные промежуточные модели для передачи данных DTO (Data Transfer Object), уровень доступа к данным собственно модели, описывающие сущности базы данных [9-10].

Крайние уровни не могут взаимодействовать между собой, то есть уровень представления (применительно к ASP.NET MVC, контроллеры) не могут напрямую обращаться к базе данных и даже к уровню доступа к данным, а только через уровень бизнес-логики. Уровень доступа к данным не зависит от других уровней, уровень бизнес-логики зависит от уровня доступа к данным, а уровень представления - от уровня бизнес-логики.

Взаимодействие с клиентской частью web-приложения

Для взаимодействия между клиентской и серверной частями приложения необходим протокол взаимодействия, а именно HTTP.

HTTP (Hypertext Transfer Protocol) представляет протокол для запроса ресурсов с веб-сервера. Когда мы обращаемся в веб-браузере к каким-либо веб-сайтам, мы как раз используем протокол HTTP. Структурная схема «Взаимодействие сайта с сервером» будет выглядеть, как представлено на рисунок 2.

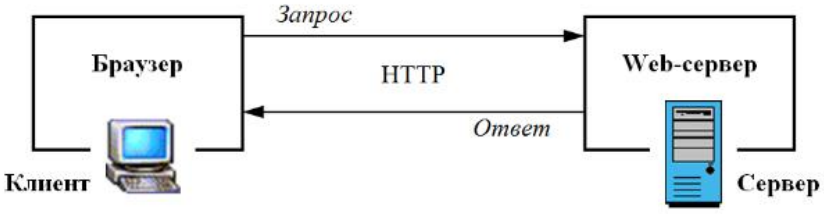

Рисунок 2 – Схема взаимодействия web-сайта с сервером

Рассмотрим алгоритм взаимодействия клиентской и серверной частей.

1. Пользователь передает данные посредством запроса.
2. С помощью протокола HTTP системой осуществляется запрос к серверу.
3. Сервер обрабатывает запрос и возвращает ответ с необходимыми данными обратно пользователю.
4. Клиентская часть обрабатывает полученные данные и отображает их на экране пользователя.

В качестве примера рассмотрим отправку запроса на получение списка походов.

1. Пользователь открывает страницу списка походов.
2. Клиентская часть формирует GET-запрос и отправляет его на API "/api/hikes".
3. Серверная часть получает запрос, получает данные из базы данных, формирует и отправляет ответ на клиентскую часть.
4. Клиентская часть получает данные и отображает их в элементах на странице веб-браузера (см. рисунок 3).

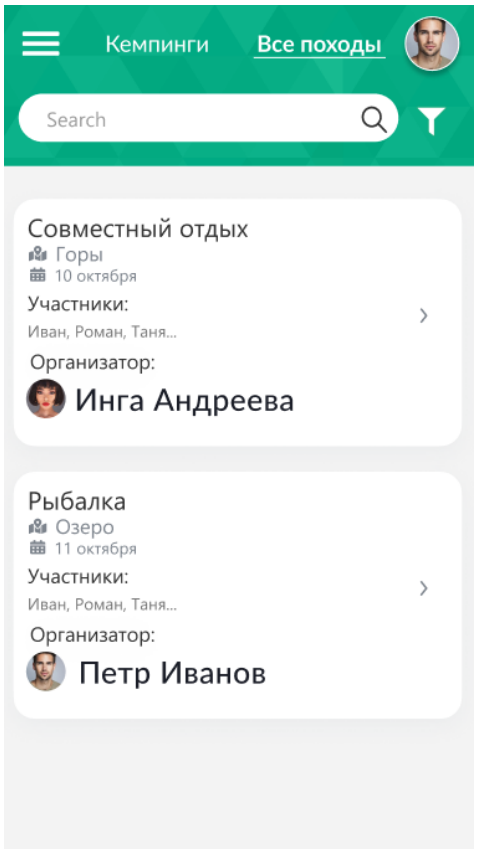

Рисунок 3 – Пример списка походов

В настоящее время продолжается работа по наполнению базы данных web-сервиса данными по организации походов по природным маршрутам [11-12].

Список литературы

1. Вандюк, Джон К. CMS Drupal. Руководство по разработке системы управления сайтом / Вандюк, Джон К., Мэтт Вестгейт,. - М.: Вильямс, 2016. - 400 с.
2. Востоков, И.Е. Классификация пешеходных маршрутов: учебное пособие / И. Е. Востоков. М.: 2000. 189 с.

3. Гаевский, А.Ю. 100% самоучитель. Создание Web-страниц и Web-сайтов. HTML и JavaScript / А.Ю. Гаевский, В.А. Романовский. - М.: Триумф, 2015. - 464 с.
4. Дронов, Владимир JavaScript и AJAX в Web-дизайне / Владимир Дронов. - Москва: Высшая школа, 2016. - 736 с.
5. Илья Кантор. Современный учебник JavaScript. Онлайн учебник - Режим доступа: URL: https://learn.javascript.ru
6. Попчиковский, В.Ю. Организация и проведение туристских походов: учебное пособие / В. Ю. Попчиковский. М.: Профиздат, 1987. 224 с.
7. Шимановский, В.С. Питание в туристском путешествии: учебное пособие /В.С. Шимановский, В. И. Ганопольский, П. И. Лукоянов. М.: Профиздат, 2006. 176 с
8. Шилдт, Г. C# 4.0. Полное руководство: пер.с англ. / Г.Шилдт. - М: Издательский дом "Вильямс", 2011. - 1056 с.
9. ASP.NET Core 5 | Полное руководство, Электронный ресурс, https://metanit.com/sharp/aspnet5/, режим доступа: свободный;
10. Руководство по ADO.NET Entity Framework 6, Электронный ресурс, https://msdn.microsoft.com/enus/library/, режим доступа: свободный;
11. Официальный сайт Microsoft Developer Network , Электронный ресурс, https://msdn.microsoft.com/enus/library/, режим доступа: свободный;
12. Руководство по Vue.js, https://metanit.com/web/vuejs/, режим доступа: свободный

References

1. Vandyuk, John K. CMS Drupal. Guide to the development of a content management system / Vandyuk, John C., Matt Westgate,. - M.: Williams, 2016. - 400 p.
2. Vostokov, I.E. Classification of walking routes: textbook / I. E. Vostokov. M.: 2000. 189 p.
3. Gaevsky, A.Yu. 100% tutorial. Creation of Web pages and Web sites. HTML and JavaScript / A.Yu. Gaevsky, V.A. Romanovsky. - M.: Triumph, 2015. - 464 p.
4. Dronov, Vladimir JavaScript and AJAX in Web design / Vladimir Dronov. - Moscow: Higher School, 2016. - 736 p.
5. Ilya Kantor. Modern JavaScript Tutorial. Online tutorial - Access mode: URL: https://learn.javascript.ru
6. Popchikovsky, V.Yu. Organization and conduct of tourist trips: a textbook / V. Yu. Popchikovsky. M.: Profizdat, 1987. 224 p.
7. Shimanovsky, V.S. Nutrition in a tourist trip: a textbook / V.S. Shimanovsky, V. I. Ganopolsky, P. I. Lukoyanov. M.: Profizdat, 2006. 176 p.
8. Schildt, G. C# 4.0. Complete guide: translated from English. / G.Schildt. - M: Williams Publishing House, 2011. - 1056 p.
9. ASP.NET Core 5 | Complete Guide, Electronic resource, https://metanit.com/sharp/aspnet5/, access mode: free;
10. ADO.NET Entity Framework 6 Guide, Online Resource, https://msdn.microsoft.com/enus/library/, access mode: free;
11. Microsoft Developer Network official site, Electronic resource, https://msdn.microsoft.com/enus/library/, access mode: free;
12. Vue.js Guide, https://metanit.com/web/vuejs/, access mode: free;)

Андреева Я. А., Василевский К. А. Сравнительный анализ рекомендательных систем и методов оценки их качества // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 59–66

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.83

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМ И МЕТОДОВ ОЦЕНКИ ИХ КАЧЕСТВА

[1]Андреева Я. А., [2]Василевский К. А.
Московский технический университет связи и информатики, Москва, Россия (123423, г. Москва, ул. Народного Ополчения, 32), e-mail: [1]andreevaya.00@mail.ru, [2]alaxtver@yandex.ru

В последние годы рекомендательные системы становятся все популярней и применяются в различных сферах: от новостной ленты до интернет-магазинов. Такое разнообразие рекомендательных систем порождает вопрос оценки их качества. В данной статье подробно описаны различные типы рекомендательных систем, их плюсы и минусы, а также принцип их работы. Особое внимание уделено математическим методам оценки качества рекомендательных систем.

Ключевые слова: рекомендательные системы, коллаборативная фильтрация, метрики, оценка качества, ранжирование.

COMPARATIVE ANALYSIS OF RECOMMENDATION SYSTEMS AND METHODS FOR EVALUATING THEIR QUALITY

[1]Andreeva Ya. A., [2] Vasilevskii K. A.
Moscow Technical University of Communications and Informatics, Moscow, Russia (123423, Moscow, Narodnogo Opolcheniya str., 32), e-mail: [1]andreevaya.00@mail.ru, [2]alaxtver@yandex.ru

In recent years, recommendation systems have become increasingly popular and are used in various fields: from news feeds to online stores. Such a variety of recommendation systems raises the question of assessing their quality. This article describes in detail the various types of recommendation systems, their pros and cons, as well as the principle of their operation. Special attention is paid to mathematical methods of evaluating the quality of recommendation systems.

Keywords: recommendation systems, collaborative filtering, metrics, quality evaluation, ranking.

Введение

Стремительный рост и разнообразие информации, доступной в Интернете, а также быстрое внедрение новых услуг электронного бизнеса (покупка товаров, сравнение товаров, аукцион и т.д.) часто ошеломляли пользователей, заставляя их принимать неправильные решения. Доступность выбора, вместо того чтобы приносить пользу, начала снижать благосостояние пользователей.

В связи с этим последние годы широкую популярность приобрело повсеместное использование интеллектуальных рекомендательных систем: в интернет-магазинах, в новостной ленте СМИ, социальных сетях, поисковых системах, стриминговых музыкальных и видео сервисах и т.д.

Рекомендательной системой или системой рекомендаций называется комплекс программ, который на основе различных данных о пользователе определяет его интересы и, в соответствии с ними, формирует различные предложения контента. Основной целью применения рекомендательных систем является персонализация контента, а также его автоматическая подстройка под текущие нужды конкретного пользователя.

Рекомендательные системы в первую очередь ориентированы на людей, которым не хватает достаточного личного опыта или компетенции, чтобы оценить огромное количество схожих элементов, которые, например, может предложить какая-либо платформа.

Релевантные рекомендации значительно сокращают время, необходимое пользователю для поиска товаров, услуг или контента, а также увеличивают возможность того, что пользователю попадутся другие объекты, которые смогут привлечь его интерес. Тем самым повышается лояльность пользователей и их удовлетворенность работой веб-сервисов. Как правило, в сервисах, где применяются рекомендательные системы, пользователи взаимодействуют с большим количеством товаров, что приводит к увеличению потребления и как следствие, росту прибыли. Благодаря тому, что область применения рекомендательных систем достаточно широкая и постоянно растет, их изучение не теряет актуальности. С каждым годом увеличивается количество рекомендательных систем и их качество.

Классификация рекомендательных систем

За последние годы технической революции основные задачи рекомендательных систем в целом не изменились. Удержание внимания пользователей и побуждение их к целевому действию все также актуальны. Для этого применяются различные прогностические методы, в основе которых лежит машинное обучение.

Современные интеллектуальные рекомендательные системы должны обладать рядом свойств:

- системе необходимо приспосабливаться под конкретного пользователя, потому что предпочтения разных людей могут кардинально отличаться;
- системе необходимо учитывать текущие предпочтения конкретного пользователя, адаптируясь под него с течением времени;
- система должна все время искать новые области информации и предоставлять их пользователю.

Всего выделяют 4 типа рекомендательных систем по методу поиска необходимого пользователю материала (рисунок 1).

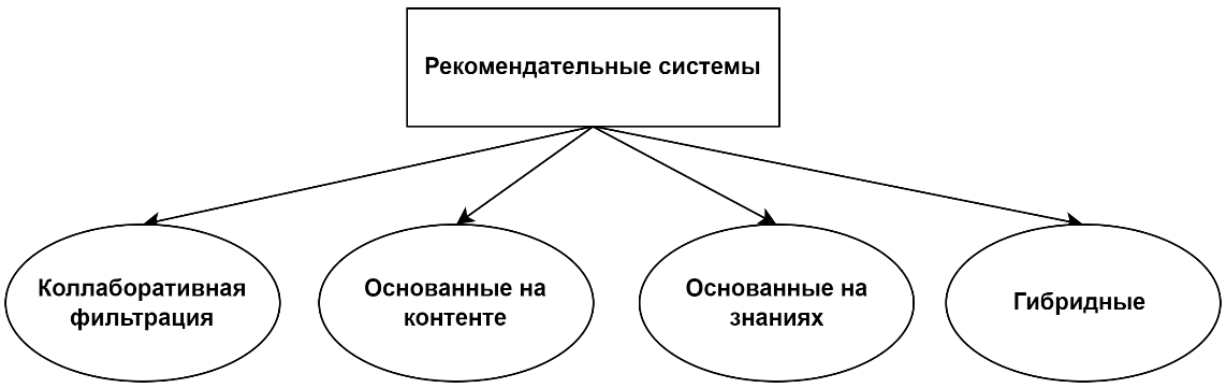

Рисунок 1 – Типы рекомендательных систем.

1. Метод коллаборативной фильтрации

Метод коллаборативной фильтрации (англ. collaborative filtering) построен на истории оценок как самого пользователя, так и других пользователей [1, 2].

В коллаборативной фильтрации используется два типа входных данных: множество объектов интереса и множество пользователей. Отношения между ними чаще всего выражаются при помощи оценок, выставленных пользователями.

К преимуществам систем, использующих коллаборативную фильтрацию относится:

- простота алгоритмов;
- простота объяснения;
- высокая точность;
- стабильность.

Существенным минусом такого типа рекомендательных систем является проблема «холодного начала». Рекомендательная система, построенная на методе коллаборативной фильтрации не будет предоставлять пользователю подходящие рекомендации, если необходимое количество пользователей системы не сообщит о своих интересах.

2. Фильтрация, основанная на контенте

Рекомендательные системы, основанные на контенте (англ. contentbased), строятся на данных о каждом конкретном объекте [3]. Пользователю предлагаются объекты, схожие с теми, которыми он интересовался до этого. Схожесть этих объектов оценивается по их содержимому.

Среди преимуществ таких рекомендательных систем можно выделить тот факт, что для начала генерации системе не требуется большое число зарегистрированных пользователей, ведь рекомендации не зависят от других пользователей этой системы [4].

Основными проблемами данного метода являются:

- отсутствие возможности рекомендовать объекты, которые не соответствуют интересам конкретного пользователя (зависимость от выбранной области);
- снижение точности;
- ограниченность полезности таких рекомендаций.

3. Фильтрация, основанная на знаниях

Рекомендательные системы, в основе которых лежат знания о предметной области (англ. knowledge-based), а не об отдельных объектах имеют достаточно высокую точность, предоставляя пользователю именно то, что ему нужно. Помимо этого, такие системы изучают и производят анализ взаимосвязей между различными объектами, а также учитывают дополнительную информацию, относящуюся к индивидуальным данным конкретного пользователя [5].

Рекомендации основываются множестве объектов и множестве правил, которые в зависимости от информации, заданной пользователем, описывают, какие объекты ему необходимо рекомендовать.

К плюсам такого подхода можно отнести отсутствие «холодного старта», а к минусам – более высокую сложность разработки системы и необходимость дополнительных данных.

4. Гибридные рекомендательные системы

Помимо базовых подходов, описанных выше, существуют гибридные рекомендательные системы (hybrid), которые объединяют в себе возможности этих методов [6]. Это позволяет нейтрализовать или минимизировать недостатки, свойственные предыдущим типам рекомендательных систем.

Методы оценки качества рекомендательных систем.

В последние годы с бурным развитием рекомендательных систем важным вопросом становится оценка их качества. Это необходимо для того, чтобы понять, насколько эффективна та или иная рекомендательная система и насколько качественные и точные рекомендации она может предложить. На сегодняшний день существует множество метрик, позволяющих оценить качество рекомендательных систем.

Метрики качества принято делить на три группы (рисунок 2).

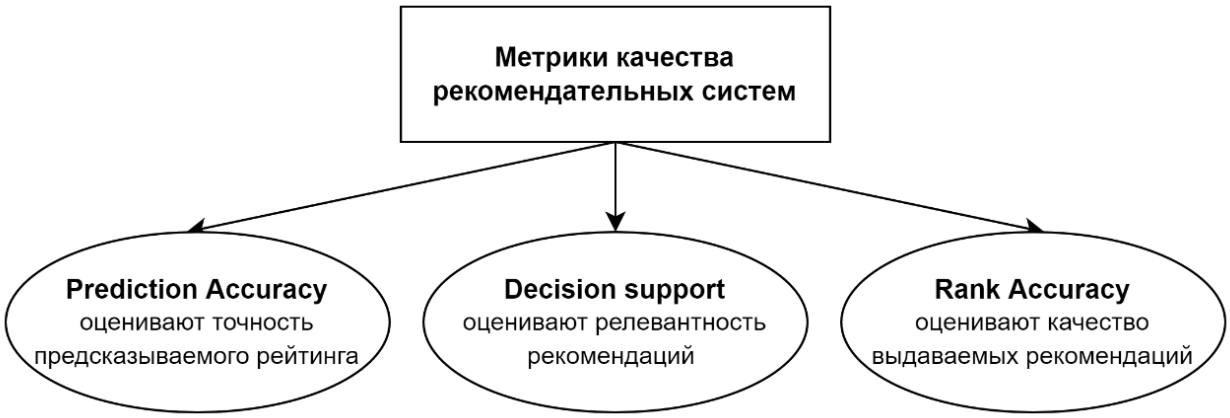

Рисунок 2 – Метрики оценки качества рекомендательных систем.

Рассмотрим подробнее некоторые из них.

Prediction Accuracy

Когда рейтинги оцениваются по непрерывной шкале (0-10), как правило, достаточно метрик класса Prediction Accuracy. Данные метрики дают возможность оценить разницу между реальной оценкой пользователя и оценкой, предсказанной системой [7].

Наиболее популярной среди метрик данного типа стала MAE (Mean Absolute Error, пер. средняя абсолютная ошибка). Помимо нее используются другие схожие метрики, например, MSE (Mean Squared Error, пер. средняя квадратичная ошибка), RMSE (Root Mean Squared Error, пер. средняя квадратичная ошибка) и другие. Метрика RMSE стала особенно популярной в последнее время после применения в конкурсе Netflix Prize.

- MAE (Mean Absolute Error)

Средняя абсолютная ошибка оценивается как абсолютная разность между предсказанием алгоритма и реальной оценкой по модулю:

$$MAE = \frac{\sum_{i \in n} |P_i - R_i|}{n} \quad (1)$$

Статистические свойства и простота вычислений сделали данную метрику наиболее популярной в оценке рекомендательных систем, хотя и существуют некоторые ограничения при оценке систем, ориентированных на рекомендации определенного количества объектов.

- MSE (Mean Squared Error)

$$MSE = \frac{\sum_{i \in n} (P_i - R_i)^2}{n} \quad (2)$$

MSE почти никогда не равна нулю, а происходит это из-за присутствия элемента случайности в данных или из-за невозможности учитывания всех факторов, позволяющих увеличить предсказательную способность.

- RMSE (Root Mean Squared Error)

$$RMSE = \sqrt{\frac{\sum_{i \in n}(P_i - R_i)^2}{n}} \quad (3)$$

Ошибки, обнаруженные с помощью метрики RMSE, могут оказать большое влияние на решение пользователя. Именно поэтому данная метрика довольно часто применяется в оценке рекомендательных систем.

Однако, у данной метрики есть и несколько минусов:

- У ошибки в предсказании высокой оценки вес такой же, что и у ошибки в предсказании низкой оценки;
- Кроме предсказания рейтинга также важно преподносить пользователям объекты в необходимом порядке, то есть требуется учитывать ранжирование, а этого данная метрика не умеет.

Decision Support

Метрики класса Decision Support позволяют узнать, насколько качественно система может отличать плохие объекты от хороших. Наибольшей популярностью среди метрик данного типа пользуются такие метрики как точность, полнота и ROC-показатели.

Данные показатели можно применять для задачи поиска наиболее релевантных объектов, особенно в том случае, если предпочтения пользователей определяются бинарными оценками (0 и 1, да и нет).

В ситуации, когда рейтинги изначально откладываются на непрерывной шкале, их можно перевести в бинарный формат, применив четкое правило. К примеру, если оценка меньше 3.5, то она считается «плохой», а если больше, то «хорошей» [8]. И наоборот, если оценки пользователей находятся в широком числовом диапазоне, тогда с помощью этих показателей нельзя оценивать правильный порядок объектов в списке рекомендаций.

Данные метрики показывают хороши или нет рекомендуемые объекты и не учитывают, какой объект лучше. В этих случаях данная метрика является не лучшим вариантом решения.

- Accuracy (пер. точность)

В простейшем случае метрикой может быть доля объектов, по которым система приняла правильное решение.

$$Accuracy = \frac{P}{N} \quad (4)$$

Где P – количество объектов, по которым система приняла правильное решение,

N – размер обучающей выборки.

Главная особенность данной метрики заключается в том, что при ее использовании всем объектам присваивается одинаковый вес, что может быть не корректно в том случае, когда распределение объектов в обучающей выборке довольно сильно смещено в сторону какого-либо одного или нескольких классов.

- Precision (пер. точность) и recall (пер. полнота)

Точность и полнота являются метриками, которые применяются при оценке большей части алгоритмов извлечения информации.

Точность рекомендательной системы в пределах определенного класса – это доля объектов, действительно принадлежащих этому классу относительно всех объектов, которые система причислила к данному классу.

Полнота рекомендательной системы – это доля найденных системой объектов, принадлежащих классу относительно всех объектов этого класса в тестовой выборке.

Для расчета вышеупомянутых метрик используются бинарные матрицы ошибок.

Бинарная матрица ошибок состоит из следующих значений:

- истинно положительные (TP): Фактическое значение положительное, модель предсказывает положительное.
- ложноотрицательные (FN): Фактическое значение положительное, модель предсказывает отрицательное.
- ложноположительные (FP): Фактическое значение отрицательное, модель предсказывает положительное.
- истинно отрицательные (TN): Фактическое значение отрицательное, модель предсказывает отрицательное.

Тогда метрики точность и полнота определяются следующим образом:

$$Precision = \frac{TP}{TP + FP} \quad (5)$$

Данная метрика показывает долю рекомендаций, понравившихся пользователю.

$$Recall = \frac{TP}{TP + FN} \quad (6)$$

Метрика recall определяет долю интересных пользователю товаров, которая была показана.

- F-мера

F-мера является гармоническим средним между полнотой и точностью. Она также стремится к нулю, когда полнота или точность стремятся к нулю.

$$F1 = \frac{2PR}{P + R} \quad (7)$$

В этой формуле точности и полноте придается одинаковый вес, в связи с чем F-мера будет одинаково падать при уменьшении и точности и полноты.

- ROC-кривая

Данная метрика чаще всего используется как альтернатива точности/полноте, и обычно применяется в теории сигналов. ROC-кривая наглядно показывает поведение системы при классификации релевантных и нерелевантных объектов.

Кривая ROC является графическим представлением верной и ошибочной классификации объектов.

Rank Accuracy

Обычно рекомендации представляют собой список из определенного количества позиций. Например, список рекомендованных товаров в интернет-магазине или список фильмов, подобранных для пользователя на стриминговой площадке.

Метрики типа Rank Accuracy позволяют оценить качество ранжирования выдаваемых рекомендаций в таком списке. Рассмотрим подробнее некоторые из них.

- MRP (Mean Reciprocal Rank, пер. среднеобратный ранг)

$$MRP = \frac{1}{|Q|}\sum_{i=1}^{|Q|}\frac{1}{rank_i}) \quad (8)$$

Где $rank_i$ обозначает положение первого релевантного ответа для некоторого запроса i.

Данная метрика позволяет выяснить, на какой позиции из всего списка рекомендаций пользователь находит первую полезную.

- MAP (Mean Average Precision, пер. средняя точность)

Данная метрика является средним значение показателей точности для каждого объекта.

$$MAP = \frac{\sum_{q=1}^{Q} AveP(q)}{Q} \quad (9)$$

- nDCG (Normalized Discounted Cumulative Gain, пер. нормированный дисконтированный совокупный доход)

$$\mathrm{nDCG} = \sum \frac{R(i)}{\max(1, \log(i))} \quad (10)$$

Метрика nDCG показывает информативность выдачи с учетом ранжирования рекомендаций.

Выводы

При выборе метрики оценки качества рекомендательных систем нужно учитывать множество факторов. Например, тип решаемой задачи, тип используемой рекомендательной системы и т.д.

В статье рассмотрены различные типы рекомендательных систем и дан подробный анализ существующих методов оценки их качества: приведена их классификация и описание. Также в работе описаны основные плюсы и минусы использования той или иной метрики.

Результаты проведенного исследования могут быть полезны при разработке собственной рекомендательной системы и позволяют облегчить выбор метода оценки ее качества.

Список литературы

1. Ekstrand M. D., Riedl J. T., Konstan J. A. Collaborative Filtering Recommender Systems // Foundations and Trends® in Human–Computer Interaction, 2011. Vol. 4, No. 2. – P. 81-173.
2. Billsus D., Pazzani M.J. Learning Collaborative Information Filters // Proceeding 15th International Conference on Machine Learning, 1998. – P. 46-54.
3. Jannach D., Zanker M., Felfernig A., Friedrich G. Recommender Systems – An Introduction. Cambridge University Press, 2010. – 360 P.
4. Pazzani M., Billsus D. Learning and revising user profiles: The identification of interesting web sites // Machine Learning - Special issue on multistrategy learning, 1997. Vol. 27, Isue 3. – P. 313–331.
5. Berry M.W. Large scale singular value computations // International Journal of Supercomputer Applications, 1992. No. 6(1). – P. 13–49.
6. Николенко С.А. Рекомендательные системы. СПб: Изд-во Центр Речевых Технологий, 2012. – 53 с.
7. Воронцов К.В. Комбинаторный подход к оценке качества обучаемых алгоритмов. Математические вопросы кибернетики / Под ред. О.Б. Лупанова. – М.: Физматлит, 2004. – Т. 13. – С.5-36.
8. Вахрушева М.Ю., Евдокимов И.В. Разработка программного обеспечения аналитических информационных систем // Труды Братского государственного университета. Серия: Экономика и управление. 2014. Т. 1. № 1. – С. 196-199.

References

1. Ekstrand M. D., Riedl J. T., Konstan J. A. Collaborative Filtering Recommender Systems // Foundations and Trends® in Human–Computer Interaction, 2011. Vol. 4, no. 2. - P. 81-173.
2. Billsus D., Pazzani M.J. Learning Collaborative Information Filters // Proceeding 15th International Conference on Machine Learning, 1998. - P. 46-54.
3. Jannach D., Zanker M., Felfernig A., Friedrich G. Recommender Systems - An Introduction. Cambridge University Press, 2010. - 360 P.
4. Pazzani M., Billsus D. Learning and revising user profiles: The identification of interesting web sites // Machine Learning - Special issue on multistrategy learning, 1997. Vol. 27, Isue 3. - P. 313-331.
5. Berry M.W. Large scale singular value computations // International Journal of Supercomputer Applications, 1992. No. 6(1). – P. 13–49.
6. Nikolenko S.A. recommender systems. St. Petersburg: Center for Speech Technologies, 2012. - 53 p.
7. Vorontsov K.V. Combinatorial approach to assessing the quality of learning algorithms. Mathematical questions of cybernetics / Ed. ABOUT. Lupanova. - M.: Fizmatlit, 2004. - T. 13. - P.5-36.
8. Vakhrusheva M.Yu., Evdokimov I.V. Development of software for analytical information systems // Proceedings of the Bratsk State University. Series: Economics and Management. 2014. V. 1. No. 1. - S. 196-199.)

Шаханова М.В., Малый М.Г., Шаханова Д.С. Автоматизация процессов информационной безопасности // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 67–74

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.5

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[1]Шаханова М.В., Малый М.Г., Шаханова Д.С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

В текущих условиях цифровизации, компании, учреждения и организации вынуждены осуществлять обработку и хранение персональных данных на цифровых носителях, создавать data base типа информационных систем персональных данных (ИСПДн) и оперировать ими. Из чего следует, что возникает необходимость в защите баз данных от утечек наиболее релевантным способом. В данной статье мы разберем какие существуют действующие концепции и вынесем на рассмотрение наиболее оптимальный.

Ключевые слова: автоматизированная защита информации, защита баз данных, коммерческая цифровая безопасность, системы защиты данных, эшелонированная защита данных, automated information protection, database protection, commercial digital security, data protection systems, data protection in depth.

AUTOMATION OF INFORMATION SECURITY PROCESSES

[1] Shakhanova M. V., Malyi M.G., Shakhanova D.S.
Maritime State University named after G.I. Nevelskoy, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

In the current conditions of digitalization, companies, institutions and organizations are forced to process and store personal data on digital media, create a data base such as personal data information systems (ISPD) and operate with them. From which it follows that there is a need to protect databases from leaks in the most relevant way. In this article, we will analyze what existing concepts exist and submit the most optimal one for consideration.

Keywords: automated information protection, database protection, commercial digital security, data protection systems, data protection in depth, automated information protection, database protection, commercial digital security, data protection systems, data protection in depth.

Что же нам известно о методах защиты информации с помощью ресурсов корпоративных систем защиты, предусмотренных действующим законодательством?

Во-первых, следует разобраться в вопросе внутренней безопасности [1-3], в частности, чем обуславливаются утечки информации и какие основные угрозы краж интеллектуальной собственности компании существуют и почему компании выбирают основным стратегическим направлением развитие именно информационную безопасность, выделяя на развитие данной отрасли значительную часть своего бюджета.

Одним из факторов опасности является то, что нарушители могут быть не только внешние, не имеющие легитимного доступа к объекту защиты, но и внутренние, то есть сотрудники и руководители компании, а также юридические лица, которые в виду каких-либо

договоров имеющие доступ к атакуемым активам. И в зависимости от того, какие именно были нарушители, разнятся методы борьбы с ними.

И если внутренние угрозы практически полностью нивелируются действующим законодательством РФ [5] (а именно, достаточно подписания типового договора «О неразглашении» или «Коммерческой тайне», чтобы сотрудник опасался передачи информации в третьи руки), то с внешними угрозами все обстоит несколько иначе. Для внутренних – это ещё и технические (DLP – предотвращение утечек информации, управление учётными данными, в том числе. для борьбы с попавшими в локальную вычислительную сеть внешними атакующими), физические (система контроля и управления доступом, Closed Circuit Television), организационные.

И всё же подавляющее большинство направлении ИБ в сфере корпоративной защиты рассчитаны именно на внешние угрозы – антивирусное программное обеспечение (далее – ПО), системы авторизации и контроля доступа, а также системы идентификации пользователя по биометрическим характеристикам.

Предпринимать меры по защите своих ИСПДн и устанавливать ПО, отвечающее требованиям Федеральному закону РФ «О персональных данных», должны любые компании, которые так или иначе обрабатывают персональные данные [7, 8] (далее – ПДн).

Основной проблемой на данный момент является передача ПДн между предприятиями и третьими сторонами для последующего коммерческого использования. Таким образом, утечки информации угрожают безопасности личной жизни и становятся фактором, влияющим на социальную защищенность.

С другой стороны, все чаще крупные компании выбирают для сохранения приватности данных модель Defence In Depth (модель глубоко эшелонированной защиты), что является немаловажным фактором в развитии всей сферы информационной безопасности, позволяющую обеспечить многоуровневую защиту данных.

Остановимся на данной модели, наиболее популярной и рассмотрим ее поподробнее.

- Модель рассчитана на защиту информации, которая имеет для компании коммерческую значимость, а также ту информацию, безопасность которой компании необходимо обеспечить.
- Всего подразделяют 7 уровней защиты (Процедуры ИБ → физический периметр → сетевой периметр → внутренняя сеть компании → рабочее место сотрудника → программы и компоненты ПО → непосредственно данные)
- Непосредственно уровень данных может быть защищен шифрованием, разграничением доступа, специализированными DLP системами (контроля утечек данных).
- Защита программных продуктов обуславливается введением перечня разрешенных и запрещенных в компании программ, парольная политика и своевременное обновление брандмаузеров.
- На рабочее место сотрудников устанавливаются все новейшие обновления (обращая особое внимание на security updates), в принудительном порядке отключаются все ненужные службы.
- На уровне внутренней сети производится сегментирование – разделение сети на невзаимодействующие между собой сегменты, либо же взаимодействующие по строго регламентированным правилам. Применение IPsec – набор протоколов для

обеспечения защиты данных, передаваемых по протоколу IP, т.е. шифрование сетевого трафика. В том числе систем обнаружения вторжений – IPS/IDS или системы предотвращения вторжений, которые отличаются наличием атакующего модуля.

- Если рассматривать уровень сетевого периметра, то самыми распространенным ПО будет Firewall – фильтрующий трафик; создание DMZ-сегментов, доступ к которым повсеместен, благодаря чему разграничиваются внешние и внутренние информационные сервера компании; распространены PROXY-сервера, осуществляющие контроль доступа сотрудников за пределы корпоративной сети; разумеется, DLP-системы, проверяющие весь исходящий интернет-трафик на разглашение информации.
- К уровню физического периметра относятся все физические средства защиты (т.к. охранники, заборы, камеры наблюдения и пр.).
- Последним же уровнем является разработка политики безопасности и процедуры реагирования на кризисные ситуации, а также дополнительные меры в виде обучения сотрудников азам компьютерной грамотности и информационной безопасности.

Таким образом, можно прийти к выводу, что данная модель является на текущем этапе развитии сферы ИБ наиболее рентабельной для ее применения компаниями.

В том числе, когда речь заходит о информационной безопасности в компаниях / на предприятиях, первым делом поднимается вопрос об автоматизации данного процесса.

Зачем же она нужна? Довольно простой ответ на этот вопрос – это недостаток человеческих ресурсов и востребованность в перманентной защите данных, что непосредственно человеческий ресурс обеспечить не может.

Количество нормативной документации в области защиты информации очень велико. Большая часть процессов регламентирована [6], выделяются направления для защиты, увеличивается количество задач по мерам для обеспечения соответствия требованиям по защите информации и проведению оценки соответствия.

Перед автоматизацией стоит поговорить о задачах, стоящих перед сотрудниками отдела безопасности – это сбор и анализ данных о текущем состоянии безопасности, распределение ответственности, оценка и управление рисками, разработка и внедрение защитных мер и механизмов контроля, управление инцидентами, мониторинг введенных систем.

Часть из этих задач можно и нужно делегировать. Причины необходимости автоматизации процессов информационной безопасности кроются в нехватке квалифицированных специалистов, при большом спросе. Неоднородность системы обеспечения информационной безопасности является причиной возникновения множества конфликтов, событий и оповещений на них. Анализ и реагирование на них затрачивает ресурсы отдела. Автоматизация должна решать рутинные задачи, освобождая специалистов для более сложных или необычных задач.

Какие же процессы ИБ можно автоматизировать? Например, валидацию – принятие решения специалистом по ИБ, существенна ли угроза и как ее проще устранить, т.е. процесс обработки инцидентов. Сюда же входят оповещения об инцидентах, процессы реагирования на внешние кибератаки, которые занимают длительное время.

На практике необходимости автоматизации возникает, когда появляется крупная проблема, которую необходимо решить специалисту, но он занят рутинными задачами,

которые возможно передать на автоматическую обработку. Специалисту необходимо обрабатывать различные события, но определение приоритета этих событий можно передать на автоматизацию, таким образом специалист сфокусирован на приоритетной задаче, а не на расстановки приоритета задач или решении всех задач подряд.

Не менее важной причиной необходимости автоматизации является уменьшение влияния человеческого фактора на появление ошибки, так как человек может устать, а машина нет.

Одним из необходимых критериев для возможности введения в эксплуатацию автоматизированных процессов является налаженная работа отдела информационной безопасности.

Плюсы автоматизированных процессов.

- Главный – это уменьшение рисков, ввиду уменьшения влияния человеческого фактора.
- Уменьшение времени простоя в случае возникновения инцидента.
- Повышается управляемость процессами связанными информационной безопасностью, а также повышается эффективность.
- Благодаря переводу квалифицированных сотрудников с рутинных задач на сложные происходит оптимизация затрат.

Также, необходимо заметить, что популярность автоматизации процессов информационной безопасности главным образом связана с ростом числа рисков, инцидентов ИБ увеличиваются изо дня в день. Прогрессирующие число атакующих понимают детально принципы работы организаций, которые подвергаются атакам. Также появились более совершенные средства, методы для организации вторжений, "эксплойтов" направленных на получение конфиденциальной информации, мошеннических действий и информации ограниченного доступа.

Процессы информационной безопасности, которые возможно автоматизировать обширны, одним из таких является возможность получения специалистом контекста без ручного разворачивания всей цепочки. Системы IRP (Incident Response Platform) дают возможность выполнить ряд рутинных операций по сбору дополнительной информации, осуществить неотложные действия по сдерживанию и устранению угрозы, восстановить атакованную систему, оповестить заинтересованных лиц, а также собрать и структурировать данные о расследованных инцидентах информационной безопасности. Существуют различные виды автоматизации, разберем на примере атаки хакеров, автоматизация может дать понять специалисту об атаке и дать возможность блокировки несанкционированного проникновения, или автоматизированный процесс может сам перекрыть несанкционированный доступ.

Одним важных факторов успешной автоматизации является простота использования продукта, т.е. в после введения в эксплуатацию автоматизации не возникла необходимость найма нового специалиста, который работает только с продуктом автоматизации. Конечный вариант продукта должен быть интуитивно понятен и ускорять работу, а не замедлять её.

Для простоты понимания разделим автоматизацию на два вида:

Автоматизация не инвазивных процессов. То есть автоматизация процессов, которые активно не влияют на работу остальных процессов, это сбор данных для контекста для специалиста, расстановка приоритета задачи и т.д.

Автоматизация инвазивных процессов. То есть автоматизация процессов, которые активно влияют на работу системы, к примеру, это изоляция несанкционированного входа в систему, удаление файлов или учетной записи пользователя и т.д.

Не смотря на все плюсы автоматизации есть сегменты работы, которые невозможно автоматизировать, в виду их повышенного уровня важности для работы всей системы, это больше относится к процессам инвазивного характера. Поэтому автоматизация должна идти постепенно. Сначала в компании должны ввести в эксплуатацию не инвазивные процессы, а после, инвазивные.

Отельным пунктом необходимо выделить индустриальные компании, так как в виду повышенных рисков, в том числе и для жизни и здоровья людей, автоматизацию, на данный момент, рекомендуют проводить лишь для инвазивных процессов.

Вопросы информационной безопасности стоят в наше время перед множеством компаний, в крупных компаниях существуют собственные отделы информационной безопасности. Появляется вопрос, стоит самой компании произвести автоматизацию, или отдать это на аутсорсинг? [4]

Из плюсов собственной автоматизации можно выделить доскональное знание автоматизирующими принципов работы конкретного отдела и его нюансов.

Однако стоит отдать стоит вопрос создания автоматизированной системы компании, которая специализируется на них, в виду большего опыта в сфере, а также умения решать проблемы, возникающих при создании и интеграции такого процесса в работу.

Основные задачи, которые должна решать автоматизированная система [9]:

1. Автоматизация процессов управления информационной безопасности.
2. Мгновенный контроль состояния рисков информационной безопасности для руководства.
3. Создание и поддержание актуальной базы учёта активов и бизнес-процессов компании.
4. Классификация мер по защите информации и обработки инцидентов.
5. Управление уязвимостями, обнаруженными в ходе анализа защищённости активов компании.
6. Мониторинг изменений состояния в соответствии с внутренней политикой компании и требованиями стандартов.
7. Поддержка руководства в принятии решений по стратегическому развитию ИБ в организации.

Главная проблема внедрения автоматизации в абсолютное большинство компаний заключаются в том, что не существует общепринятого стандарта представления данных. То есть, для автоматизации, в первую очередь необходимо привести данные к стандартному виду, хотя бы внутри одной компании.

Вторая проблема проистекает из первой, недостаточно данных для создания сценария автоматизации, что уменьшает её пользу в конечно итоге или даже дает отрицательный эффект в скорости работы отдела.

Проблемой повсеместного введения автоматизации служит опасность к атакам на саму систему автоматизации, так как получив управление над ней, можно спокойно управлять всей системой. Следовательно, появляется необходимость в защите этой системы.

Автоматизировать всё это можно различными способами, к примеру core-системы.

1. Система управления логами.
2. Система анализа логов.
3. Система проектирования и автоматизации playbook по реагированию.
4. Система, помогающая работать с threat intelligence.

Из всего этого следует, что автоматизация это не одна программа, а целый комплекс, что может быть слишком сложным для конечного пользователя. Следовательно, мы упираемся в простоту использования продукта, система автоматизации должна быть простой.

Автоматизация большого количества смежных процессов реагирования на инциденты используются системы SOAR (Security Orchestration, Automation and Response), платформы оркестрации, автоматизации и реагирования на инциденты в сфере информационной безопасности. В нём существует следующий функционал [10, 11].

1. Выполнение действий по реагированию.
2. Визуализация, отчетность, аналитика, логирование выполненных действий по реагированию, ведение базы.
3. Возможность совместной работы группы аналитиков над инцидентами.
4. Возможности по обработке данных киберразведки.
5. Возможности по обработке Big Data (структурированные и неструктурированные данные огромных объёмов), механизмы машинного обучения для автоматизации действий и помощи в принятии решений при реагировании на инциденты.

Большая часть вопросов по автоматизации применима к большим корпорация, для более мелких предприятий сама подготовка к введению автоматизации может стать непреодолимым барьеров для этого. В особенности необходимость SIEM (класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности) системы, чьё введение и эксплуатация слишком дороги. На данный момент часть компаний, занимающихся автоматизацией, работают и с отсутствием SIEM систем.

Перейдем к новым функциям, которые добавляют к программам для автоматизации. Так как данная сфера относится к информационным технологиям она развивается стремительно быстро. Теперь автоматизированный процесс имеет возможность обучаться в процессе своей работы благодаря технологиям машинного обучения и возможностям искусственного интеллекта. К примеру, он помогает в решении задачи выбора верное срабатывание или нет, сама программа автоматизации, благодаря машинному обучению, может дать некоторую оценку, помогающую в принятии решения.

Главной проблемой машинного обучения является её узкая специализация. То есть, созданная нейросеть умеет только то, для чего её создали, поэтому нейросеть обученная классифицировать события с сетевых сенсоров и выявлять компьютерные атаки на сетевое оборудование не способна работать с мобильными устройствами. И так с каждой проблемой, необходимо будет создавать каждый раз новый продукт и заново его обучать.

Из этого вытекает другая проблема, это нехватка данных для обучения. То есть, нейросеть обучили на одних данных, а на деле она должна будет работать на других, что может на деле вместо уменьшения рутинной работы только добавить её, так как она обучена на других данных.

Одной из проблем вытекающей из самой сути нейросети является неполное знание почему она решила именно так.

Помимо минусов у машинного обучения есть и плюсы, при этом существенные именно в сфере информационной безопасности – это выявление неочевидных для человека закономерностей.

Реальные кейсы успешного применения искусственного интеллекта для автоматизации в плане ускорения, а не улучшения – это когда к сотруднику-аналитику попадает алерт (программируемое оповещение о каком-либо событии), а он на основе него принимает решение, а программа обучается на этом решении. Анализируя сам алерт, его ключевые свойства и взаимосвязи в нём и как они связаны с принятием решения, программа может подсказывать с какой вероятностью это false positive. Этот вариант убирает или минимизирует её главные недостатки, так как она обучается на актуальных данных, она работает именно с тем что нужно.

Будущее автоматизации. Большинство экспертов сходятся во мнении, что существуют несколько принципов, которых будут в будущем придерживаться в разработке систем автоматизации. Это в первую очередь простота, максимально понятные интерфейса, где от пользователя будут просить лишь, согласится или отклонить. Вторым столпом будет увеличение данных при создании контента. Так же в след за увеличением автоматизированных процессов, в сфере информационной безопасности, увеличится необходимость в стандартизации всех процессов, для возможности самой автоматизации.

В данный момент автоматизация процессов просто необходима, так как количество атак растет, растёт их изощренность, поэтому специалисты должны быть разгружены для выполнения тех задач, которые машины, на данный момент, выполнить неспособны. Это сделает систему более отказоустойчивой и надежной.

Список литературы

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008.
2. Петрыкина Н. И. Правовое регулирование оборота персональных данных. Теория и практика. — М. : Статут, 2011.
3. Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». — М. : Статут, 2017.
4. Талапина Э. В. Защита персональных данных в цифровую эпоху. Российское право в европейском контексте // Труды Института государства и права РАН. — 2018. — Т. 13. — № 5.
5. Федеральный закон «Об информации, информационных технологиях и защите информации» № 149 — ФЗ от 27 июля 2006 года;
6. ГОСТ Р 6.30-2003 «Унифицированная система организационно-распорядительной документации»;
7. ГОСТ Р 7.0.8.-2013 "Делопроизводство и архивное дело — Термины и определения";
8. Доктрина информационной безопасности;
9. Астахова Л.В. Теория информационной безопасности и методология защиты информации: методическое пособие / Л.В. Астахова. – Челябинск: Изд-во ЮУрГУ, 2007. – 359 с.;
10. Юдин, Э.Г. Методология науки. Системность. Деятельность / Э.Г. Юдин. – М.: Эдиториал УРСС, 1997. – 246 с.;

11. Боровский А. С., Ряполова Е. И… Построение модели системы защиты в облачных технологиях на основе многоагентного подхода с использованием автоматной модели

References

1. Basic model of personal data security threats during their processing in personal data information systems (extract). FSTEC of Russia, 2008.
2. Petrykina N. I. Legal regulation of the circulation of personal data. Theory and practice. - M. : Statute, 2011.
3. Saveliev A. I. Scientific and practical article-by-article commentary on the Federal Law “On Personal Data”. - M. : Statute, 2017.
4. Talapina E. V. Protection of personal data in the digital era. Russian law in the European context // Proceedings of the Institute of State and Law of the Russian Academy of Sciences. - 2018. - T. 13. - No. 5.
5. Federal Law "On information, information technologies and information protection" No. 149 - FZ of July 27, 2006;
6. GOST R 6.30-2003 "Unified system of organizational and administrative documentation";
7. GOST R 7.0.8.-2013 "Office work and archiving - Terms and definitions";
8. Doctrine of information security;
9. Astakhova L.V. Theory of information security and methodology of information protection: methodical manual / L.V. Astakhov. - Chelyabinsk: Publishing House of SUSU, 2007. - 359 p.;
10. Yudin, E.G. Methodology of science. Consistency. Activities / E.G. Yudin. - M.: Editorial URSS, 1997. - 246 p.;
11. Borovsky A. S., Ryapolova E. I. Building a model of a protection system in cloud technologies based on a multi-agent approach using an automatic model

Шаханова М.В., Четвертик М.А., Шаханова Д.С. Механизмы защиты информации в беспроводных сетях // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 75–79

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.5

МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

[1]Шаханова М.В., Четвертик М.А, Шаханова Д.С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

Беспроводные технологии активно распространяются среди населения. Сети с беспроводным подключением имеют ряд недочетов, связи с чем постоянно подвергаются атакам с целью перехвата конфиденциальной информации и нарушения целостности данных. Однако технологии стремительно развиваются, создаются новые методы защиты передаваемой информации. В данной статье будут приведены основные механизмы защиты при использовании беспроводных сетей.

Ключевые слова: беспроводная сеть, защита информации, беспроводные технологии, механизм защиты.

INFORMATION PROTECTION MECHANISMS IN WIRELESS NETWORKS

[1]Shakhanova M. V., Chetverik M.A., Shakhanova D.S.
Maritime State University named after G.I. Nevelskoy, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

Wireless technologies are actively spreading among the population. Wireless networks have a number of shortcomings, and therefore are constantly being attacked in order to intercept confidential information and violate data integrity. However, technologies are rapidly developing, new methods of protecting the transmitted information are being created. This article will describe the main protection mechanisms when using wireless networks.

Keywords: wireless network, information protection, wireless technologies, protection mechanism.

Беспроводная сеть – компьютерная сеть, которая использует беспроводные соединения для передачи данных между узлами сети. [1]

Беспроводные технологии позволяют передавать сигналы на большие расстояния без электрических кабелей. Возможность быстрого обмена сигналами и независимость от места подключения привлекает людей использовать беспроводную сеть.

У беспроводной сети есть ряд недостатков.

- Отсутствие стабильности. Перебои на станциях, временные отключения доступа, ограниченная дальность действия, а также риск снижения качества подключения из-за воздействия электроприборов - приводят к нарушению стабильности и возможному отказу в обслуживании.
- Безопасность. Информацию, передаваемую по каналам беспроводной связи можно перехватить. Для решения этой проблемы стали использовать шифрование сигнала, но и это не стало гарантией полной защищенности. Старые алгоритмы шифрования легко

взламываются, а для современных алгоритмов создаются новые методы взломов. Беспроводные сети обеспечивают анонимность атаки, не позволяя без соответствующего оборудование определить местоположение.

- Скорость передачи. При большом количестве пользователей, скорость подключения делится между всеми клиентами, что приводит к ее снижению. Помехи, рельеф местности, воздействие других сетей – создают преграды в свободном распространении сигнала, приглушая его и снижая скорость. [2]

Но говоря о недостатках, нельзя исключать факт того, что беспроводные сети имеют ряд преимуществ.

- Экономичность. Общая стоимость оборудование снижается из-за отсутствия надобности в дополнительных приборах.
- Простота настройки и подключения.
- Гибкость. Беспроводные сети могу служить как добавлением, так и заменой проводных сетей.
- Мобильность. Отсутствие проводов способствует легкому и быстрому перемещению и повторной установки оборудования. Пользователь «не привязан» к месту.

Наиболее известными беспроводными технологиями являются – Wi-Fi, Bluetooth и WiMAX.

Wi-Fi – это беспроводная технология передачи данных, при которой трафик преобразуется в радиоволны и распространяется в форме радиосигнала (рисунок 1). Клиентская аппаратура расшифровывает сигнал и извлекает из него информацию. Функциональность Wi-Fi схожа с функциональностью мобильных сетей.

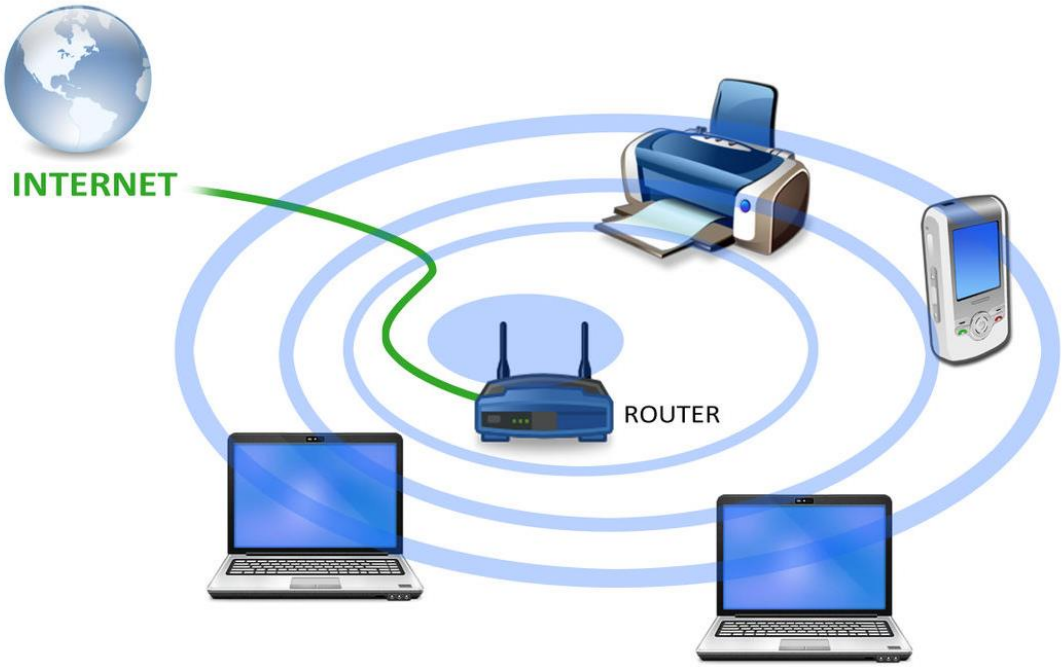

Рисунок 1 – Принцип работы Wi-Fi

Как и любая другая беспроводная сеть, Wi-Fi подвержена угрозам. Радиосигнал может быть перехвачен с целью нарушения целостности и конфиденциальности данных. Элементы защиты, предусмотренные в Wi-Fi, имеют свои недостатки. Существует несколько механизмов защиты:

- OPEN – отсутствие всякой защиты. Данные передаваемые по радиоканалам не шифруются, что становится причиной утечки данных. И если при использовании проводной сети злоумышленнику понадобится прямое подключение, то к беспроводной сети можно подключиться из любого места, что делает открытую передачу данных по сети более опасной.
- WEP – первый стандарт защиты. Данный стандарт взламывается множеством разных способов, степень его защиты немного лучше, чем открытые сети, из-за чего у пользователей часто возникало ложное чувство безопасности. Злоумышленники перехватывали пакеты, которые переносили по несколько байт временного ключа, что в условиях активного пользования сети было достаточно для раскрытия.
- WPA – второй стандарт. Он шифровал данные каждого клиента по отдельности. При проникновении в сеть отсутствовала возможность прочитать другие пакеты, сначала их нужно было перехватить.
- WPA2 – обновленная версия WPA. Стандарт поддерживает два разных режима аутентификации.
- WPS – позволяет клиенту подключиться к сети по 8-символьному коду. Но из-за допущенной ошибки в стандарте, угадать нужно всего лишь 4 [2-3].

В отличие от Wi-Fi технология WiMAX обеспечивает передачу на большие расстояния как в прямой видимости, так и вне поле зрения. Wi-Fi же обеспечивает эффективную связь лишь по прямой линии.

WiMAX – телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств [4].

Принцип работы данной технологии аналогичен работе Wi-Fi и сотовой связи. Вышки с передатчиками WiMAX свободно подключаются к Интернету. Станции покрывают большие территории и могут быть расположены на расстоянии до 50 километров. Сигналы передаются по цепочке от вышки к вышке, по крайней мере одна из которых связана с сетью провайдера при помощи проводов. С последнего передатчика на принимающую антенну с помощью зашифрованных ключей поступает сигнал (рисунок 2). Принимающей антенной может быть, как роутер, так и пользовательское устройство [4].

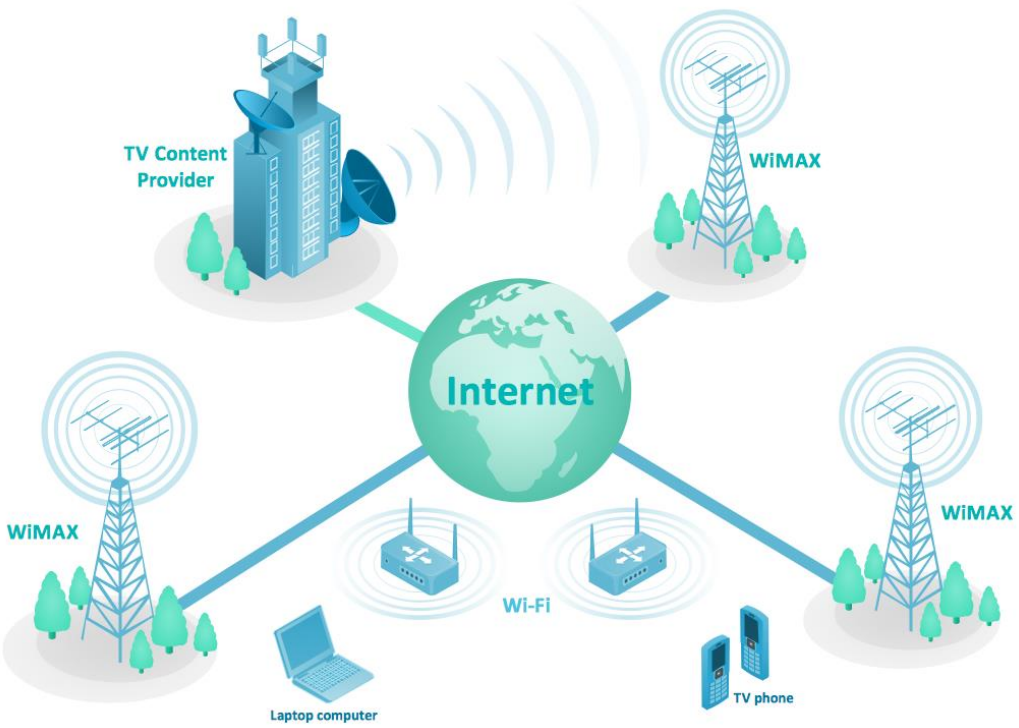

Рисунок 2 – Принцип работы WiMAX

Технология WiMAX изначально разрабатывалась со всеми учетами безопасности. Трафик должен быть зашифрован с использованием алгоритма AES, для аутентификации используется протокол на основе TLS с шифрованием открытым ключом. В стандартах технологии WiMAX изначально заложены серьезные функции безопасности:

- Аутентификация клиентского оборудования при помощи обмена сертификатами с базовой станцией для исключения неавторизированного терминала.
- Аутентификация пользователя с использованием протокола EAP.
- Кодирование передаваемых данных с использованием стандарта AES. Возможность избежать перехвата и расшифровки трафика, путем шифрования каждой из услуг собственными ключами [4].

Bluetooth – стандарт беспроводной сети, позволяющий передавать данные на небольшое расстояние при помощи радиоволн. Для передачи информации необходимо наличие у обоих устройств специального модуля. Главное отличие Bluetooth от Wi-Fi, в том, что Bluetooth используется для передачи данных между двумя устройствами без построения локальной сети [2].

Для защиты Bluetooth используется шифрование данных и авторизация устройств. Для шифрования используется ключ длиной от 8 до 128 бит. Это способствует тому, что спонтанно устройства соединяться не смогут, что снижает риск утечки данных. У технологии есть четыре режима безопасности:

- 1 режим используется по умолчанию и не предоставляет никакой защиты.
- 2 режим защищен на уровне приложения. После соединения происходит аутентификация.

- 3 режим защищен на уровне канала связи. В этом этапе после аутентификации применяется прозрачное шифрование. В данном режиме риск взлома устройство по-прежнему велик.
- 4 режим представляет собой усовершенствованный 2 режим. После установления соединения функции безопасности реализуются. Для генерации ключа используется протокол ECDH [2].

Таким образом, основной целью статьи являлось исследование методов защиты информации в беспроводных сетях. Стоит отметить, что с увеличением заинтересованности людей в использовании беспроводных сетей передачи информации увеличилось и количество случаев перехвата данных с целью нанесения вреда владельцу. При этом существующие методы не всегда справлялись с угрозой, что породило необходимость в разработке новых методов защиты информации. Понимание угроз безопасности – первый шаг к их предотвращению.

Список литературы

1. Shahrabi Alireza, Morteza Mohammadi Zanjireh, и Larijani Hadi ANCH: A New Clustering Algorithm for Wireless Sensor Networks // ResearchGate. 2013.
2. Гейер Джим Беспроводные глобальные и персональные сети // Беспроводные сети. 2005.
3. Пролетарский А. В., Басков И. В., Федотов Р.А., Бобков А. В., Чирков Д.Н., Платонов В.А. Основы протоколов безопасности беспроводных сетей и криптографии // Организация беспроводных сетей. 2006.
4. Архипкин А. Стандарт WiMAX: техническое описание, варианты реализации и специфика применения // Технологии и стандарты. 2006.

References

1. Shahrabi Alireza, Morteza Mohammadi Zanjireh, and Larijani Hadi ANCH: A New Clustering Algorithm for Wireless Sensor Networks // ResearchGate. 2013.
2. Geyer Jim Wireless global and personal networks // Wireless networks. 2005.
3. Proletarsky A. V., Baskov I. V., Fedotov R. A., Bobkov A. V., Chirkov D. N., Platonov V. A. Fundamentals of security protocols for wireless networks and cryptography // Organization of wireless networks. 2006.
4. Arkhipkin A. WiMAX standard: technical description, implementation options and application specifics // Technologies and standards. 2006.

Моделирование и расчет прочностных характеристик станочного приспособления для закрепления детали «корпус редуктора»в программном комплексе Autoleck Inventor Professional / Нейлык И.О. [и др.] // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 80–88

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.942

МОДЕЛИРОВАНИЕ И РАСЧЕТ ПРОЧНОСТНЫХ ХАРАКТЕРИСТИК СТАНОЧНОГО ПРИСПОСОБЛЕНИЯ ДЛЯ ЗАКРЕПЛЕНИЯ ДЕТАЛИ «КОРПУС РЕДУКТОРА»В ПРОГРАММНОМ КОМПЛЕКСЕ AUTOLECKINVENTORPROFESSIONAL

[1]Нейлык И. О., Щеглетов К. А., Коршунов Е. С., Ларионов И.В., Платонов А. В.
Арзамасский политехнический институт (филиал) НГТУ им. Р.Е. Алексеева, Арзамас, Российская Федерация (607227 Нижегородская обл., Арзамас ул. Калинина, 19), e-mail: [1]*nelyk20002@mail.ru*

В статье обоснована целесообразность широкого использования численных методов проектирования при разработке конструкторской документации, в частности, станочной технологической оснастки. Приведен пример исследования прочности станочного приспособления для закрепления детали «корпус редуктора» с использованием программы "Autodesk Inventor Professional".

Ключевые слова: автоблокировка на перегоне, датчики контроля, бортовой локомотивный самостоятельный центр управления безопасности, единый функциональный комплекс микропроцессорной сигнализации, каналы связи.

MODELING AND CALCULATION OF THE STRENGTH CHARACTERISTICS OF THE MACHINE DEVICE FOR FIXING THE PART "REDUCER BODY" IN THE AUTOLECKINVENTORPROFESSIONAL SOFTWARE COMPLEX

[1]Neylyk I.O., Shchegletov K.A., Korshunov E.S., Larionov I.V., Platonov A.V.
Arzamas polytechnic institute (branch) NGTU named after R.E. Alekseeva, Arzamas, Russia (607227 Nizhny Novgorod region, Nizhny Novgorod region, Arzamas, Kalinina str, 19), e-mail: [1]*nelyk20002@mail.ru*

The article substantiates the expediency of widespread use of numerical design methods in the development of design documentation, in particular, machine tools. An example of a study of the strength of a machine tool for fixing the part "gearbox housing" using the program "Autodesk Inventor Professional" is given.

Keywords: machine tool; numerical design methods; 3D modeling; strength calculations; static analysis.

Autodesk Inventor Professional – система проектирования, предназначенная для организаций, разрабатывающих сложные машиностроительные изделия. Данная программа предоставляет единое интегрированное решение, которое позволяет инженерам-конструкторам, работающим в области механики и электрики, значительно повысить производительность проектирования, контроля и документирования таких изделий.

Средства статического анализа и расчета напряжений дают возможность изучить поведение изделий в реальных условиях, при этом нет необходимости заниматься проработкой различных вариантов конструкций приспособлений. При выполнении расчетов с использованием численных методов выявляется степень воздействия на исследуемые объекты параметров внешней среды, в частности, от воздействия механической обработки и закреплений. В статье[1] показано, что цифровое проектирование изделий и процессов производства с использованием специальных программ позволяет существенно снизить затраты на подготовку производства новых изделий, что является одной из основных проблем современной экономики. Вопросы исследования конструкции приспособления с использованием программы *SOLIDWORKS Simulation* рассмотрены в статье [2], здесь, также, выполнены исследования, позволившие выполнить оптимизацию конструкции, что позволило уменьшить массу приспособления. Подобные задачи решались в статьях [3, 4].

Проводится моделирование и статический анализ деформаций (смещений) и расчет на прочность станочного приспособления для закрепления заготовки детали «Корпус редуктора» (рисунок 1). Для этого создается 3D модель приспособления в программе Autodesk Inventor Professional (рисунок 2).

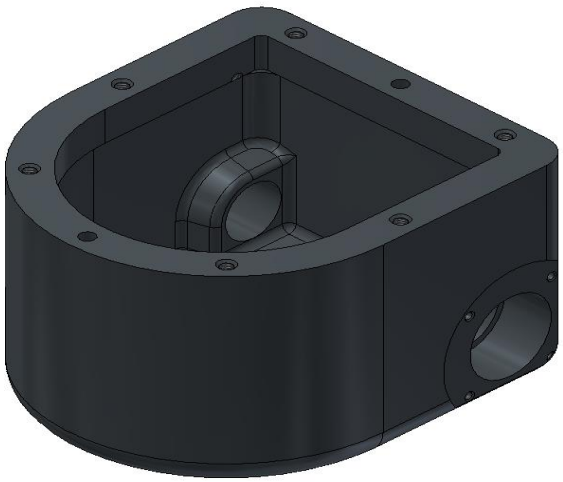

Рисунок 1 – 3D – модель детали «Корпус редуктора»

Для 3D – модели станочного приспособления выполняется статический анализ напряжений (деформаций) и расчет на прочность станочного приспособления, закрепленного на столе горизонтального обрабатывающего центра при действии: максимальной осевой силы резания P_0 = 2839 Н, максимального крутящего момента $M_{кр}$ = 99 Нм, усилия зажима заготовки в приспособлении W = 7880Н и усилия закрепления приспособления на станке.

Представляются физические параметры станочного приспособления (рисунок 3).

Производится моделирование.

Определяются общая цель и параметры моделирования (рисунок 4).

Выполняются настройки сети (рисунок 5).

Определяются физические и механические свойства материалов деталей приспособления и заготовки детали «Крышка» и создаются рабочие условия:

1.Сила закрепления станочного приспособления на столе станка (2 болта М12) (рисунок 6).

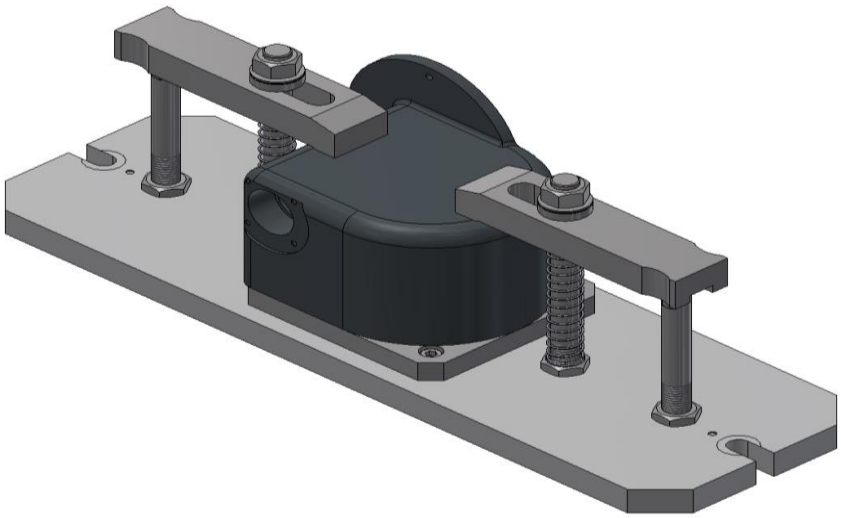

Рисунок 2 – 3D – модель станочного приспособления

Масса	22,8242 кг
Площадь	506591 мм^2
Объем	2965430 мм^3
Центр масс	x=-2,19342 мм y=0,498985 мм z=43,5819 мм

Рисунок 3 - Физические параметры приспособления

Цель проектирования	Одноточечный
Тип моделирования	Статический анализ
Дата последнего изменения	22.09.2022, 21:35
Обнаружить и устранить моды жесткого тела	Нет
Разделить поперечные напряжения контактных поверхностей	Нет
Анализ нагрузок движения	Нет

Рисунок 4 – Общая цель и параметры

Средний размер элемента (дробное значение от диаметра модели)	0,1
Минимальный размер элемента (дробное значение от среднего размера)	0,2
Коэффициент разнородности	1,5
Макс. угол поворота	60 град
Создать изогнутые элементы сетки	Нет
Использовать для сетки сборки измерение на основе деталей	Да

Рисунок 5 – Настройки сети

Тип нагрузки	Сила
Величина	5800.000 H
Вектор X	0.000 H
Вектор Y	0.000 H
Вектор Z	-5800.000 H

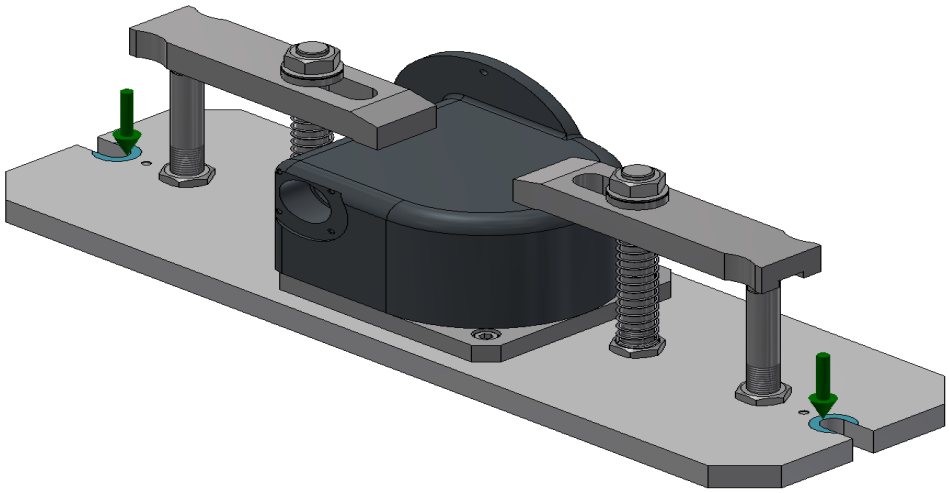

Рисунок 6– Действие усилия закрепления приспособления (зеленые стрелки) на столе станка при механической обработке поверхностей заготовки детали «Корпус редуктора»

2.Усилие зажима заготовки детали «Корпус редуктора» в приспособлении (рисунок 7).

Тип нагрузки	Сила
Величина	7880.000 H
Вектор X	0.000 H
Вектор Y	0.000 H
Вектор Z	-7880.000 H

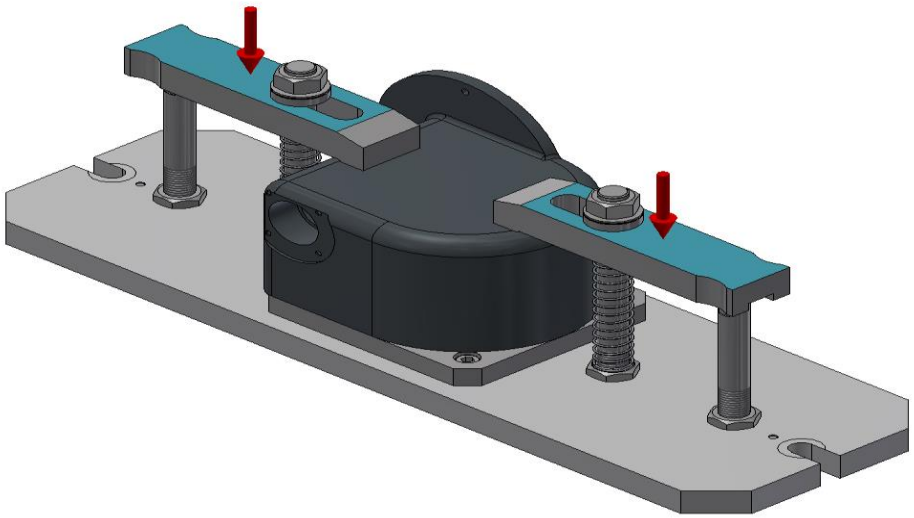

Рисунок 7 – Действие усилия зажима заготовки (красные стрелки) детали «Корпус редуктора» в приспособлении при механической обработке поверхностей

3.Удаленная сила - осевая сила резания при механической поверхности детали «Корпус редуктора» в приспособлении (рисунок 8).

Тип нагрузки	Сила
Величина	2839.000 Н
Вектор X	-0.000 Н
Вектор Y	2839.000 Н
Вектор Z	0.000 Н

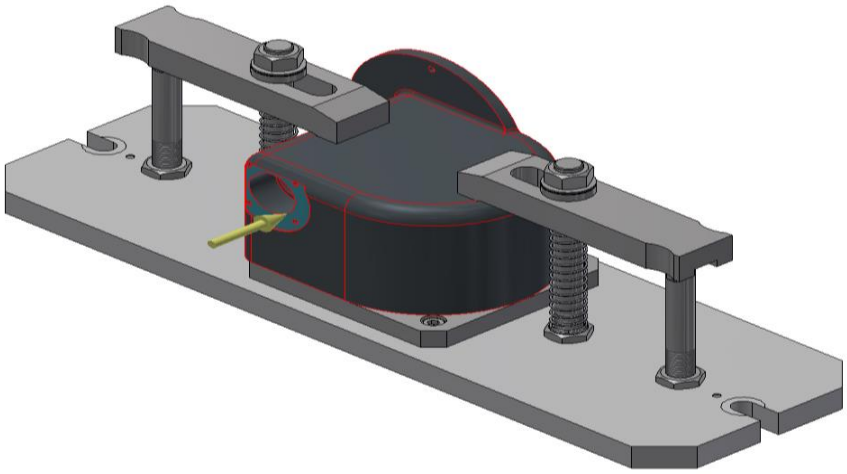

Рисунок 8 – Действие осевой силы резания инструмента (желтая стрелка) на заготовку детали «Корпус редуктора» закрепленной в приспособлении при механической обработке поверхности

4. Удаленная сила – крутящий момент инструмента (рисунок 9).

Тип нагрузки	Момент
Величина	99000.000 Н мм
Вектор X	-0.000 Н мм
Вектор Y	99000.000 Н мм
Вектор Z	-0.000 Н мм

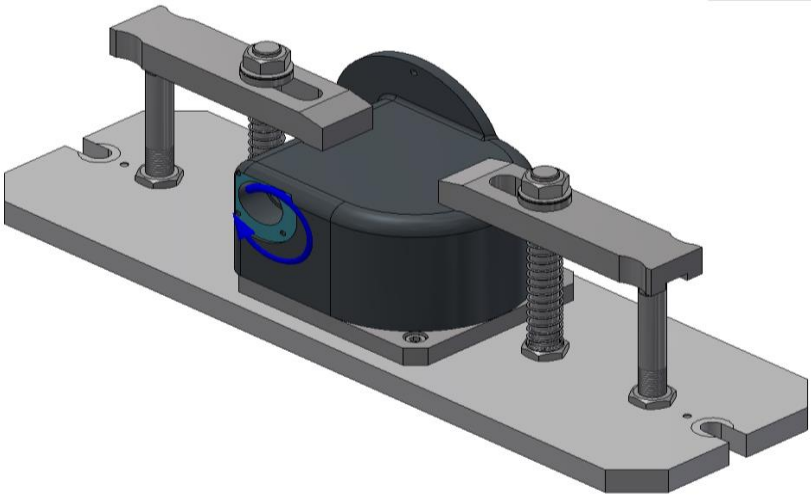

Рисунок 9 – Действие крутящего момента инструмента (синяя стрелка) на заготовку детали «Корпус редуктора» закрепленной в приспособлении при механической обработке поверхности.

Определяются поверхности и грани (рисунок 10) станочного приспособления при закреплении его на столе горизонтального обрабатывающего центра модели при механической обработке поверхностей в детали «Корпус редуктора».

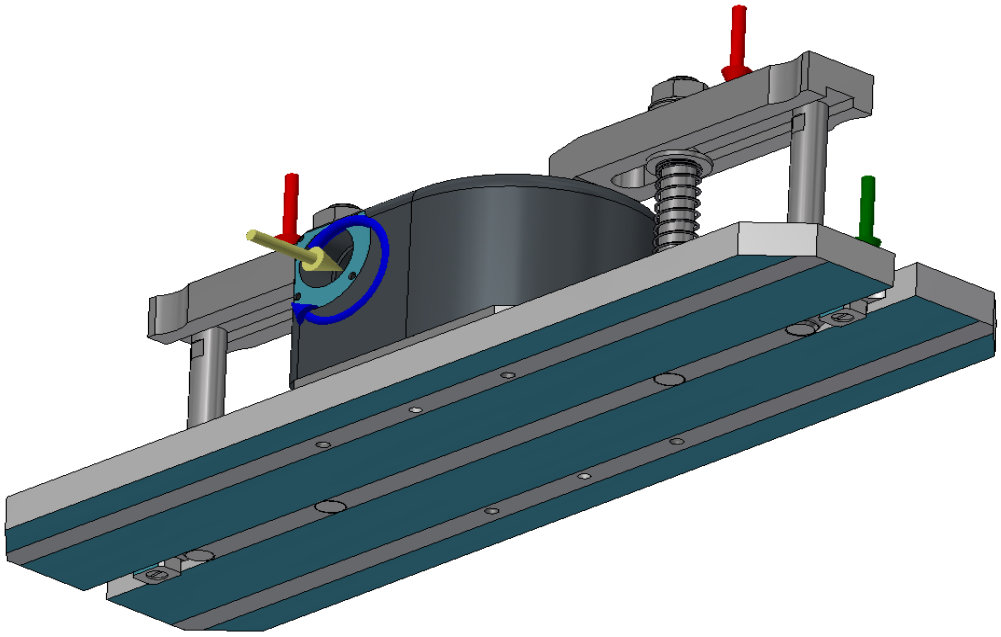

Рисунок 10 – Выбранные поверхности и грани станочного приспособления при закреплении его на столе станка

Для закрепления станочного приспособления на столе станка используются шпонки (рисунок 11).

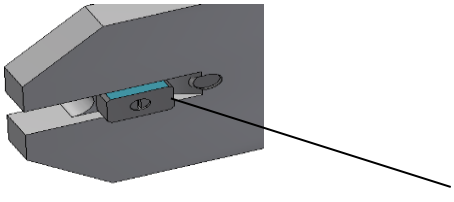

Рисунок 11 – Шпонка, закрепленная на основании приспособления

Для корректного проведения статического анализа напряжений (деформаций) и расчета на прочность станочного приспособления назначаются контакты между деталями приспособления и метизами, которые предназначены для закрепления деталей в приспособлении.

В результате проведенного статического анализа станочного приспособления получены следующие результаты:

1. Сила и момент реакции в зависимостях (рисунок 12);

Имя зависимости	Сила реакции		Реактивный момент	
	Величина	Компонент (X,Y,Z)	Величина	Компонент (X,Y,Z)
Зависимость фиксации:1	13761,3 Н	-213,098 Н	338,651 Н м	293,16 Н м
		-2839 Н		-128,801 Н м
		13463,6 Н		110,235 Н м

Рисунок 12 - Сила и момент реакции в зависимостях

2. Результат статического анализа и расчета (рисунок 13).

Имя	Минимальная	Максимальная
Объем	2965440 мм^3	
Масса	22,8242 кг	
Смещение	0 мм	0,147754 мм
Коэфф. запаса прочности	1,52051 бр	15 бр

Рисунок 13 – Таблица полученных результатов

Деформации (смещения) и запас прочности станочного приспособления, закрепленного на столе горизонтального обрабатывающего центра при действии рабочих условий на заготовку детали «Корпус редуктора» показаны на рисунках 14 и 15 соответственно.

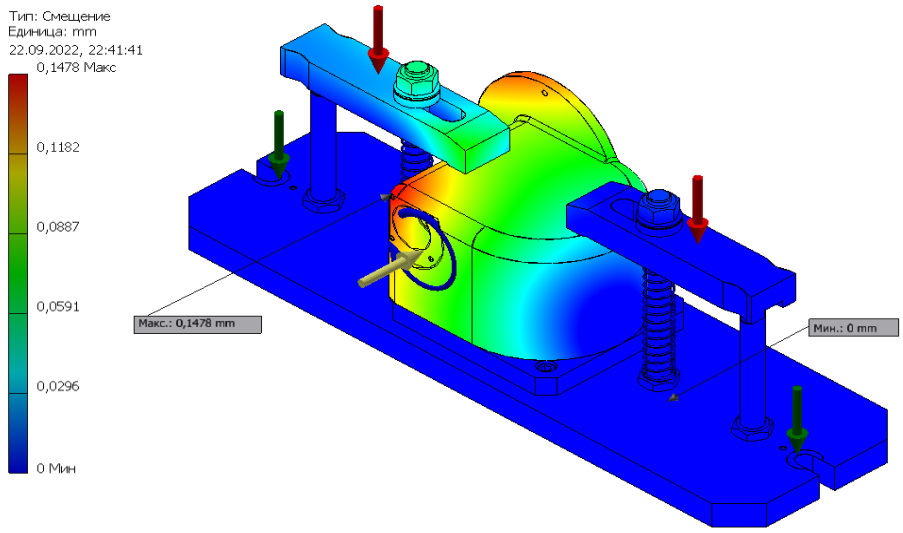

Рисунок 14 – Деформации (смещения) станочного приспособления, закрепленного на столе обрабатывающего центра при действии рабочих условий

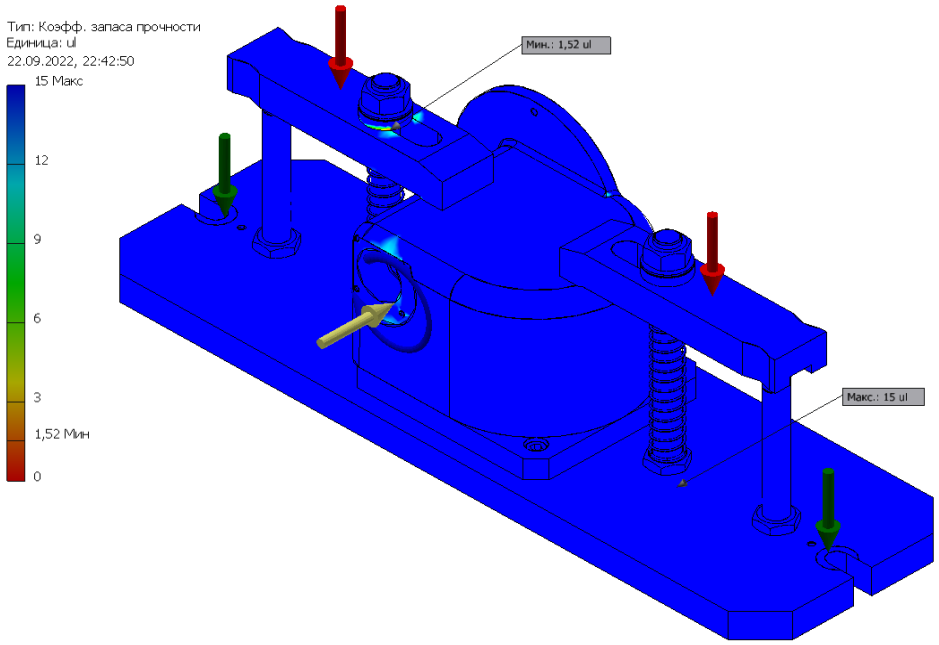

Рисунок 15 – Запас прочности станочного приспособления, закрепленного на столе обрабатывающего центра при действии рабочих условий

Таблица результата (рисунок 13) и рисунки 14 и 15 показывают, что максимальное смещение составляет всего 0,15 мм, коэффициент запаса прочности равен 1,52. Масса приспособления 23 кг.

Проведенные моделирование и статический анализ и расчет подтверждают прочность и надежность станочного приспособления, обеспечивающего точность изготовления детали «Корпус редуктора».

Список литературы

1. Левенцов В.А., Левенцов А.Н. Цифровое проектирование изделия и процессов производства как фактор повышения эффективности // Современные наукоемкие технологии. – 2021. – № 5. – С. 63-67; URL: https://top-technologies.ru/ru/article/view?id=38659 (дата обращения: 13.11.2022).
2. Мигунова Т.В.Использование имитационного моделирования для анализа точности и работоспособности станочного приспособления // Наука молодых: сборник научных статей участников XIII Всероссийской научно-практической конференции (26–27 ноября 2020 г.) / Ассоциация ученых г. Арзамаса, Арзамасский филиал ННГУ, АПИ (филиал) НГТУ им. Р.Е. Алексеева. – Арзамас: Арзамасский филиал ННГУ, 2020. – С . 25-28.
3. Кошелев А.В., Платонов А. В., Куманеев М.А.,Щеглетов К. А., Баранов А.В., Гараев М.П. Исследование влияния рабочего профиля кулачка на прочность системы «патрон-деталь» токарного станка // Методика имитационного моделирования при исследовании конструкции приспособления типа «Разжимная оправка» токарного станка. Часть 1. Оптимизация конструктивных параметров // Кузнечно-штамповочное производство. Обработка материалов давлением: научно-технический и производственный журнал. № 2-2020, С. 28-36.

4. Платонов А. В., Рябикина Т.В., Лещева О.В., Старостина О.Н., Клоков И.И., Куманеев М.А., Звонарев Г.В. Щеглетов К.А. Моделирование технологической операции обработки заготовки, закрепленной в сборно-разборном приспособлении//Кузнечно-штамповочное производство. Обработка материалов давлением: научно-технический и производственный журнал. № 3-2022, С. 20-31.
5. Функционал и полное описание программы Autodesk Inventor Professional. https://www.pointcad.ru/product/autodesk-inventor/podrobnoe-opisanie-autodesk-inventor (дата обращения 12.11.2022)

References

1. Leventsov V.A., Leventsov A.N. Digital design of products and production processes as a factor in increasing efficiency // Modern science-intensive technologies. - 2021. - No. 5. - P. 63-67; URL: https://top-technologies.ru/ru/article/view?id=38659 (accessed 11/13/2022).
2. Migunova T.V. Using simulation to analyze the accuracy and performance of a machine tool // Science of the Young: a collection of scientific articles by participants in the XIII All-Russian Scientific and Practical Conference (November 26–27, 2020) / Association of Scientists of Arzamas, Arzamas branch UNN, API (branch) NSTU im. R.E. Alekseev. - Arzamas: Arzamas branch of UNN, 2020. - P. 25-28.
3. Koshelev A.V., Platonov A.V., Kumaneev M.A., Shchegletov K.A., Baranov A.V., Garaev M.P. Investigation of the influence of the working profile of the cam on the strength of the “chuck-part” system of a lathe. Part 1. Optimization of design parameters // Forging and stamping production. Processing of materials by pressure: scientific, technical and industrial journal. No. 2-2020, pp. 28-36.
4. A. V. Platonov, T. V. Ryabikina, O. V. Leshcheva, O. N. Starostina, I. I. Klokov, M. A. Kumaneev, and G. V. Zvonarev, Russ. Shchegletov K.A. Simulation of the technological operation of processing a workpiece fixed in a collapsible device // Forging and stamping production. Processing of materials by pressure: scientific, technical and industrial journal. No. 3-2022, pp. 20-31.
5. Functionality and full description of the program AutodeskInventor Professional. https://www.pointcad.ru/product/autodesk-inventor/podrobnoe-description-autodesk-inventor (accessed 11/12/2022)

Эффект Пельтье. Элемент Пельтье. Достоинства и недостатки. Применение элементов Пельтье в современной электронике / Шинкарев В.В. [и др.] // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 89–96

Международный журнал информационных технологий и энергоэффективности

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

УДК 621.38

ЭФФЕКТ ПЕЛЬТЬЕ. ЭЛЕМЕНТ ПЕЛЬТЬЕ. ДОСТОИНСТВА И НЕДОСТАТКИ. ПРИМЕНЕНИЕ ЭЛЕМЕНТОВ ПЕЛЬТЬЕ В СОВРЕМЕННОЙ ЭЛЕКТРОНИКЕ

[1]Шинкарев В. В., [2]Дубовсков К. Ю., [3]Кошкин Ф.В., [4]Селезнёв И. В., [5]Карагодин Н. В., [6]Юлусов К. С.

Оренбургский Государственный Университет, Оренбург, Российская Федерация (460005 г.Оренбург, ул. Шевченко, 28), e-mail: [1]maildlyvsegoo56@mail.ru, [2]kdubovskov@mail.ru, [3]fedor.koschkin@yandex.ru, [4]vanya_seleznev_2018@mail.ru, [5]karagodin19062002@gmail.com, [6]Kirill.yulusov@gmail.com

В данной статье рассмотрено явление эффекта Пельтье, а также принцип работы элементов Пельтье. Целью статьи является изучение элементов Пельтье, анализ сфер применения в современной жизни, а также выявление достоинств и недостатков этих элементов. В ходе работы собрана основная информация по принципу действия элементов Пельтье, приведена историческая справка. Проанализировали положительные и отрицательные аспекты применения термоэлектрических охладителей в электронике. Изучили сферы применения элементов Пельтье на сегодняшний день. Сделали заключение по проделанной работе над научной статьёй.

Ключевые слова: эффект Пельтье, элемент Пельтье, термоэлектрический охладитель, нагрев, охлаждение

PELTIER EFFECT. THE PELTIER ELEMENT. ADVANTAGES AND DISADVANTAGES. APPLICATION OF PELTIER ELEMENTS IN MODERN ELECTRONICS

Shinkarev V.V., **Dubovskov K.Yu.**, **Koshkin F.V., Seleznev I. V., Karagodin N.V., Yulusov K.S.**
*Orenburg State University, Orenburg, Russia (*460005 *Orenburg, Shevchenko str, 28), e-mail: [1]maildlyvsegoo56@mail.ru, [2]kdubovskov@mail.ru, [3]fedor.koschkin@yandex.ru, [4]vanya_seleznev_2018@mail.ru, [5]karagodin19062002@gmail.com, [6]Kirill.yulusov@gmail.com*

This article discusses the phenomenon of the Peltier effect, as well as the principle of operation of Peltier elements. The purpose of the article is to study the elements of Peltier, to analyze the fields of application in modern life, as well as to identify the advantages and disadvantages of these elements. In the course of the work, basic information was collected on the principle of the Peltier elements, and a historical reference was given. The positive and negative aspects of the use of thermoelectric coolers in electronics were analyzed. We have studied the scope of application of Peltier elements to date. We made a conclusion on the work done on the scientific article.

Keywords: Peltier effect, Peltier element, thermoelectric cooler, heating, cooling.

История открытия эффекта Пельтье

В 1834 году французский учёный Жан-Шарль Пельтье проводил эксперимент. Суть исследования заключалось в том, что он соединил пластину, сделанную из висмута, с медными проводами, а затем пропустил электрический ток. В результате эксперимента он обнаружил

интересное свойство: соединение висмут-медь нагревается, то есть имеет положительную температуру, а другое охлаждается, то есть имеет отрицательную температуру.

В 1838 году более подробно физический процесс удалось описать русскому физику Э.Х. Ленцу. Он провёл собственный эксперимент, в ходе которого смог доказать явление эффекта Пельтье. Взяв два стержня из разного материала (висмута и сурьмы), Ленц поместил каплю воды в углубление на стыке этих стержней [6, с.14]. Затем он пропустил электрический ток в 100 А в одном направлении и обнаружил, что вода начала застывать и превратилась в лёд. После этого Ленц поменял направление тока и обнаружил, что лёд начал таять. Данный эксперимент позволил установить, что от направления тока, протекающего в элементе Пельтье, помимо тепла от нагрева самого элементач выделяется или поглощается дополнительное тепло, которое получило название «тепла» Пельтье. По своим свойствам можно сделать вывод: эффект Пельтье является обратным эффекту Зеебека.

Возникновение эффекта Пельтье

Разность потенциалов возникает в месте соединения двух различных веществ при прохождении электрического тока. Разность потенциалов создаёт внутреннее контактное поле. Если направление тока противоположно направлению контактного поля, то происходит нагрев контактов, так как внешний источник затрачивает дополнительную энергию. Если направление тока совпадает с направлением контактного поля, то в этом случае место соединения контактов охлаждается.

Эффект Пельтье[3] — термоэлектрическое явление, при котором при прохождении электрического тока происходит перенос энергии в месте соединения (контакта или спайки) двух различных проводников (рисунок 1). Эффект Пельтье чаще всего применяется в полупроводниках. За счёт свойств, которые возникают при явлении тепла Пельтье, создаются элементы Пельтье.

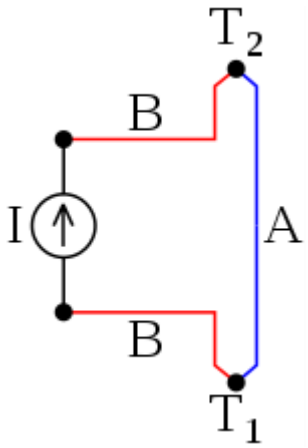

Рисунок 1 – Схема эффекта Пельтье

Элемент Пельтье[4] — это термоэлектрический преобразователь, в котором при протекании электрического тока возникает разность температур на противоположных пластинах элемента. При пропускании тока тепло переносится с одной стороны на другую. Элементы Пельтье обозначаются сокращённо маркировкой «TEC» (от англ. Thermoelectric Cooler – термоэлектрический охладитель).

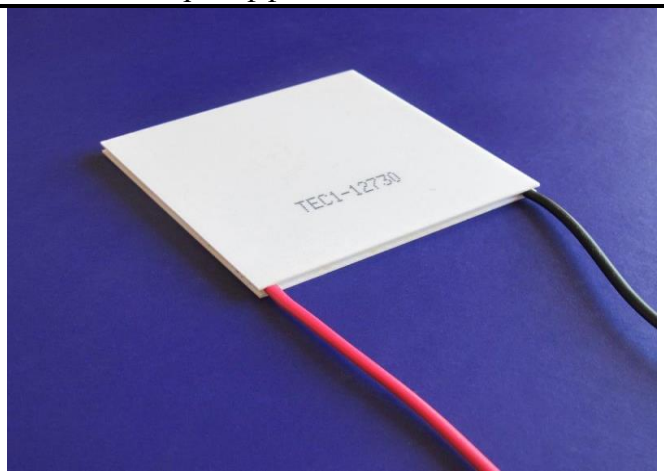

Рисунок 2 - Внешний вид элемента Пельтье

Величина перемещённой энергии и направление её переноса зависят от вида контактирующих веществ и от направления и силы протекающего электрического тока:

$$Q = \Pi_{AB} It = (\Pi_B - \Pi_A) It \quad (1)$$

где Q — количество выделенного или поглощённого тепла;
I — сила тока;
t — время протекания тока;
П — коэффициент Пельтье, который связан с коэффициентом термо-ЭДС α вторым соотношением Томсона $\Pi = \alpha T$, где Т — абсолютная температура в ºK [1, с.140].

Принцип действия

В качестве проводников в элементах Пельтье используются полупроводниковые материалы. Между ними находится зона проводимости с электронами с разными энергетическими уровнями. При прохождении электрического тока электрон приобретает энергию и затем переходит в зону проводимости выше другого полупроводника. При поглощении энергии место контакта охлаждается. Если изменить направление тока, то место контакта будет нагреваться, а также сам элемент будет нагреваться (рисунок 3 [5, с.10]).

Металлические проводники не эффективно использовать в качестве элементов Пельтье, так как эффект Пельтье будет минимальным из-за нагрева и явлений теплопроводности. На практике чаще всего применяют контакт двух полупроводниковых материалов.

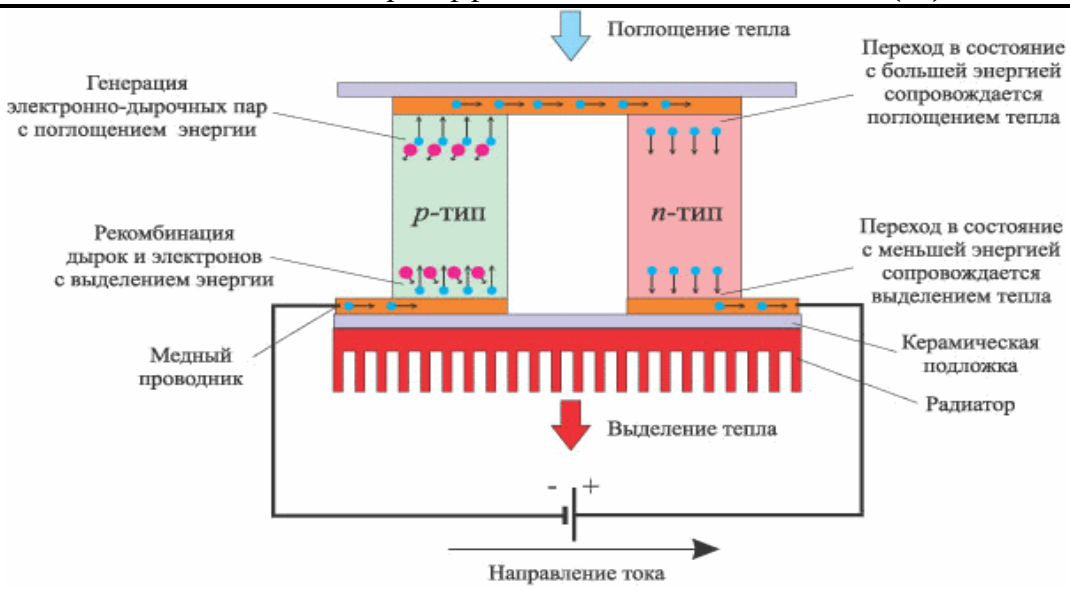

Рисунок 3 – Принцип работы элемента Пельтье

Элемент Пельтье состоит из одной или более пар небольших полупроводниковых параллелепипедов – одного n-типа и одного p-типа в паре (обычно теллурида висмута Bi2Te3 и твёрдого раствора SiGe), которые попарно соединены при помощи металлических перемычек. Данные металлические перемычки служат термическими контактами между полупроводниками. Перемычки изолированы непроводящей плёнкой или керамической пластинкой. Пары параллелепипедов соединяют последовательно, и в результате получается последовательное соединение многих пар полупроводников с разным типом проводимости. При этом соблюдается условие: вверху находятся соединения последовательности (n->p), а снизу - противоположные (p->n). Электрический ток протекает последовательно через все параллелепипеды. От направления электрического тока зависит либо охлаждение верхних контактов, при этом происходит нагрев нижних контактов, либо нагрев верхних контактов и охлаждение нижних (рисунок 4 [8]). Таким образом электрический ток переносит тепло с одной стороны элемента Пельтье на противоположную и создаёт разность температур.

Рисунок 4 – Элемент Пельтье в разрезе

При работе элемент Пельтье начинает нагреваться из-за проходящего по нему току. Чтобы устройство не вышло из строя, его необходимо охлаждать. Охлаждение элемента Пельтье происходит следующим образом: на нагревающую сторону устанавливается радиатор

или вентилятор. В результате температура холодной стороны становится ниже. Разность температур может достигать 70°С.

Достоинства и недостатки отражены в таблице 1.

Таблица 1 – Достоинства и недостатки элементов Пельтье

Достоинства	Недостатки
1. Компактность и относительно небольшие размеры позволяет монтировать элементы Пельтье на различные платы с электронными компонентами	1. Низкий КПД по сравнению с компрессорными холодильными установками, работающими на фреоне
2. Отсутствие подвижных частей, газов и жидкостей	2. Большая потребляемая мощность для достижения разности температур
3. В зависимости от направления тока возможно охлаждение или нагревание (термостатирование)	3. В элементах Пельтье с высоким КПД свободные электроны в веществе являются носителями как электрического тока, так и выделяемого тепла
4. Отсутствие шума при работе элементов Пельтье	4. Не работает при отсутствии постоянного источника питания
5. Широко применяются в технике и различных устройствах, так как благодаря им есть возможность получить температуры ниже 0°С	5. При большом тепловом потоке элемент Пельтье не успевает самоохлаждаться и может выйти из строя из-за перегрева

Материал, из которого будет сделан элемент Пельтье, имеет важное значение, так как от этого фактора зависит эффективность элементов. Высокие показатели эффективности достигаются, если материал обладает двумя взаимоисключающими свойствами — хорошая проводимость электрического тока, и плохая теплопроводность.

Для повышения эффективной работы элементов Пельтье необходимо стабилизировать температуру. Для этого используют импульсные источники питания. Однако следует сглаживать токовые пульсации в результате чего повышается эффективность работы элемента Пельтье, а также продливается срок службы. Неэффективной работа элемента Пельтье становиться при стабилизации температуры с использованием широтно-импульсной модуляции тока.

Применение

Свойство эффекта Пельтье широко используется в микросхемах для охлаждения процессоров. По сути любое устройство, содержащее в себе процессор, охлаждается не только воздухом, но и за счёт элемента Пельтье. К примеру, такой тип охлаждения применяется в компьютерах. На процессор устанавливают элемент Пельтье «холодной» стороной (рисунок 5), а «горячая» сторона охлаждается за счёт воздуха или кулера [9].

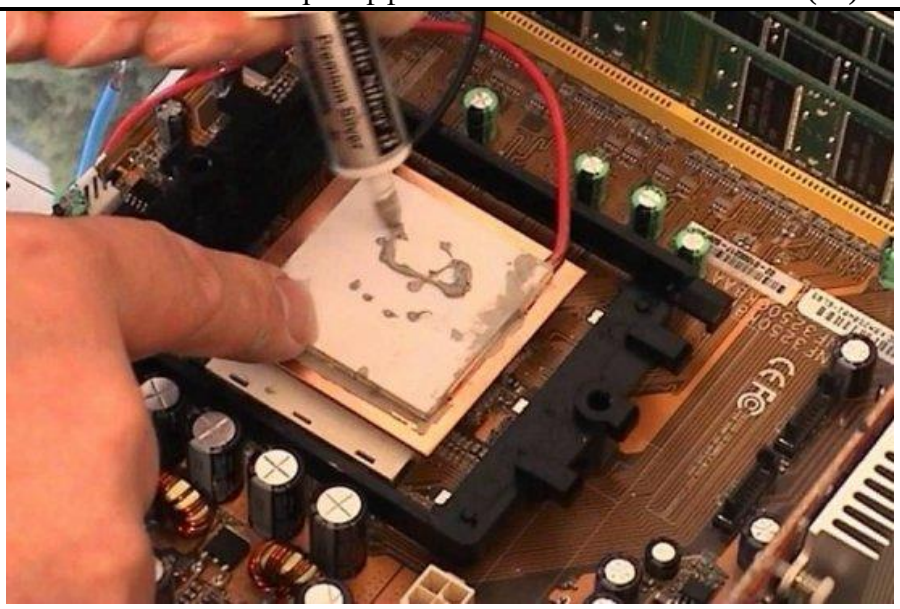

Рисунок 5 – Охлаждение процессора компьютера за счёт элемента Пельтье

В медицине элементам Пельтье также нашли применение. Сегодня они используются в амплификаторе (рисунок 6) – устройстве, обеспечивающим периодический нагрев или охлаждение пробирок.

Рисунок 6 – Амплификатор (термоциклер, ПЦР-машина)

В быту элементы Пельтье применяются в устройствах, в которых охлаждение происходит на минимальную разницу температуры. В такой технике энергетическая эффективность охладителя имеет маленький КПД. К примеру, это могут быть: автомобильные мини-холодильники, охлаждаемые банкетные тележки, применяемые в ресторанах и кафе. Кроме того, элементы Пельтье применяются для охлаждения устройств с зарядовой связью в цифровых фотокамерах. За счёт этого достигается заметное уменьшение теплового шума при длительных экспозициях (астрофотография).

В военной отрасли применяются многоступенчатые элементы Пельтье, которые предназначены для охлаждения приёмников излучения в инфракрасных сенсорах (в ракетах ЗРК, ПЗРК "Джавелин", "Стингер" и другие). Ещё одно применение элементов Пельтье – это

охлаждение и термостатирование диодных лазеров с тем, чтобы стабилизировать температуру излучателя, а также длину волны излучения.

Однако элементы Пельтье не являются основным источником для охлаждения электронных компонентов. Зачастую они используются как вторая или третья ступень охлаждения. Это позволяет достичь температур на 30—40 градусов ниже, чем с помощью обычных компрессионных охладителей (до −80 °C для одностадийных холодильников и до −120 °C для двухстадийных). Также элементы Пельтье получили применение в устройствах охлаждения электротехнических шкафов и другого оборудования, работающего на постоянном токе.

«Электрогенератор Пельтье» [2] (более корректно было бы «генератор Зеебека», но неточное название устоялось, рисунок 7) — модуль для генерации электричества, термоэлектрический генераторный модуль, аббревиатура GM, TGM. Данный термогенератор состоит из двух основных частей:

- преобразователь температуры в электричество;
- источник тепловой энергии для нагрева преобразователя.

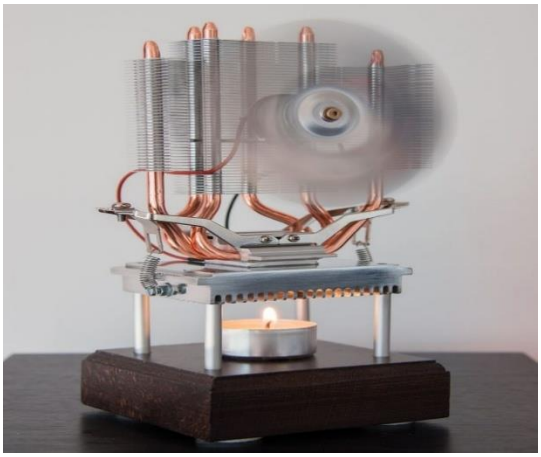

Рисунок 7 – Термоэлектрический генератор на элементах Пельтье

Заключение

В эпоху микропроцессорной электроники элементы Пельтье нашли своё применение. На сегодняшний день без них не обходится ни один процессор компьютера, так как для их нормальной работы необходим постоянный отвод тепла. В виду того, что современная техника и электроника стремится к компактности, то есть уменьшению размеров электронных компонентов, то для них в любом случае необходимо охлаждение, которое возможно благодаря элементам Пельтье. Несмотря на то, что эффект Пельтье был открыт ещё в 19 веке, широкое применение ему нашли относительно недавно. В будущем потребность в оснащении приборов элементами Пельтье будет только возрастать, что указывает на их значимость в электронике.

Список литературы

1. Физика твердого тела Учеб. пос. / А. А. Василевский – М.: Дрофа, 2010. – 206 с;

2. Термоэлектрический генератор своими руками [Электронный ресурс] - https://uk-parkovaya.ru/smarthouse/equipment/termoelektriceskij-generator-svoimi-rukami-video-foto-instrukcia.html;
3. Эффект Пельтье [Электронный ресурс] - https://ru.wikipedia.org/wiki/Эффект_Пельтье;
4. Элемент Пельтье [Электронный ресурс] –https://ru.wikipedia.org/wiki/Элемент_Пельтье;
5. Булат Л.П., Бузин Е.В. Термоэлектрические охлаждающие устройства: Метод. указания для студентов спец. 070200 “Техника и физика низких температур”. – СПб.: СПбГУНиПТ, 2001. – 41 с;
6. Булат Л. П., Ведерников М. В., Вялов А. П. и др. Термоэлектрическое охлаждение. Текст лекций под общей ред. Л. П. Булата. СПб.: СПбГУНиПТ, 2002;
7. Иоффе А. Ф., Стильбанс Л. С., Иорданишвили Е. К., Ставицкая Т. С. Термоэлектрическое охлаждение. М.: АН СССР, 1956;
8. Иорданишвили Е. К. Термоэлектрические источники питания. М.: Советское радио, 1968;
9. Системы охлаждения компьютеров [Электронный ресурс] - http://electricalschool.info/spravochnik/poleznoe/2227-sistemy-ohlazhdeniya-kompyutera.html.

References

1. Solid State Physics Proc. settlement / A. A. Vasilevsky - M .: Bustard, 2010. - 206 p.;
2. Do-it-yourself thermoelectric generator [Electronic resource] - https://uk-parkovaya.ru/smarthouse/equipment/termoelektriceskij-generator-svoimi-rukami-video-foto-instrukcia.html;
3. Peltier effect [Electronic resource] - https://ru.wikipedia.org/wiki/Peltier effect;
4. Peltier element [Electronic resource] – https://ru.wikipedia.org/wiki/Peltier element;
5. Bulat L.P., Buzin E.V. Thermoelectric Cooling Devices: Method. instructions for students spec. 070200 “Technique and physics of low temperatures”. St. Petersburg: SPbGUNIPT, 2001. 41 p.;
6. Bulat L.P., Vedernikov M.V., Vyalov A.P. et al. Thermoelectric cooling. The text of the lectures under the general editorship. L. P. Bulat. St. Petersburg: SPbGUNIPT, 2002;
7. Ioffe A. F., Stilbans L. S., Iordanishvili E. K., Stavitskaya T. S. Thermoelectric cooling. M.: AN SSSR, 1956;
8. Iordanishvili E.K. Thermoelectric power sources. M.: Soviet radio, 1968;
9. Computer cooling systems [Electronic resource] - http://electricalschool.info/spravochnik/poleznoe/2227-sistemy-ohlazhdeniya-kompyutera.html.

Шаханова М.В., Швец Е.Е., Шаханова Д.С. Обеспечение информационной безопасности на предприятии // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 97–103

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

[1]Шаханова М.В., Швец Е.Е., Шаханова Д.С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

Безопасность бизнес-информации является важнейшей задачей управления предприятием при управлении рисками. Современная эра технологической безопасности для бизнеса получает все большее признание, особенно в бизнес-стратегиях. Разъединение процедур информационной безопасности и коммерческих стратегических бизнес-целей для контроля расходов на безопасность и связанных с ними рисков, инцидентов и убытков. Операционная корпоративная система требует согласования методов обеспечения безопасности путем внедрения управления рисками информационной безопасности в организацию, однако она сталкивается с серьезными проблемами, связанными с поддержкой и запуском бизнеса. Выравнивание безопасности в бизнес-процессе — одна из самых больших проблем в хорошей организации, поскольку она требует вспомогательных ресурсов и управления временем, а также способов согласования безопасности для достижения бизнес-целей. Таким образом, роль управления информационной безопасностью важна как руководство по обеспечению безопасности деловой информации. Кроме того, систематическое управление безопасностью представляет собой бизнес-модель для защиты критической информационной инфраструктуры. Структура и стратегия организации, люди, процессы и технологии — элементы модели, которые играют эффективную роль в обеспечении информационной безопасности, но для этого требуется баланс между ними.

Ключевые слова: информационная безопасность бизнеса, управление рисками информационной безопасности, управление информационной безопасностью (ISM), information security serves for business.

ENSURING INFORMATION SECURITY AT THE ENTERPRISE

[1]Shakhanova M. V., Shvets E.E., Shakhanova D.S.
Maritime State University named after G.I. Nevelskoy, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

The security of business information is the most important task of enterprise management in risk management. The modern era of technological security for business is becoming increasingly recognized, especially in business strategies. Separation of information security procedures and commercial strategic business objectives to control security costs and related risks, incidents and losses. The operational corporate system requires the coordination of security methods by implementing information security risk management in the organization, but it faces serious problems related to the support and launch of the business. Aligning security in a business process is one of the biggest challenges in a good organization, as it requires support resources and time management, as well as ways to align security to achieve business goals. Thus, the role of information security management is important as a guide to ensuring the security of business information. In addition, systematic security management is a business model for protecting critical information infrastructure. The structure and strategy of the organization, people, processes and technologies are elements of the model that play an effective role in ensuring information security, but this requires a balance between them.

Keywords: business information security, information security risk management, information security management (ISM), information security serves for business.

В настоящее время важность информационной безопасности в корпоративной среде имеет огромное значение. Информационная безопасность стала более важной для большинства организаций при принятии мер по снижению рисков. Деятельность по защите бизнеса должна быть первым и главным достижением любой программы безопасности. Эта точка зрения была поддержана специалистами по безопасности, подходами к обеспечению безопасности и используемыми государственными процессами. Призвание к информационной безопасности выросло из профессии проверки, групп соответствия и регулирования, а также агентств общественной безопасности, которые имеют профессию как безопасность, ориентированную на риски. Из-за некоторых проблем несколько предприятий не сделали это основной компетенцией. Это связано с тем, что ограничение организации должно открыть для некоторых организаций понимание важности их безопасности для достижения жизненно важных бизнес-целей и активного вовлечения заинтересованных сторон бизнеса в проблему безопасности. В результате она превратилась в развязанную программу, вялую и во многом безуспешную. Таким образом, есть много организаций, которые должны бороться, чтобы достичь решающего выравнивания. Согласование программ безопасности с предприятием требует глубокого понимания технической области, например, того, как различные вычислительные технологии позиционируются на предприятии и их значения для бизнеса, а также того, как конкретная защита поддерживает конкретные цели бизнес-стратегии.

Информационная безопасность в соответствии с управлением предприятием

Интересно отметить, что большая часть организаций использует подход, ориентированный на риски, для обеспечения безопасности и инвестиций. В основном риск может возникать из-за уязвимостей, угроз и связанных с ними рисков. Стратегия Business Security дает лучшие результаты по сравнению ориентированной на риски за счет использования подхода.

Однако существует предел того, какую защиту может предложить ИТ-отдел без комплексного бизнес-подхода — лучший в мире брандмауэр не помешает сотрудникам отправлять критически важные данные за пределы организации. Таким образом, роль ISM (управление информационной безопасностью) заключается в поддержке и управлении бизнес-деятельностью. Например, бизнес-анализ дает обслуживание анализа рисков информационной безопасности. Глубокое знание предприятия необходимо для поддержки настройки лучших руководств по упражнению в подходящем и эффективном исполнении, которое будет «принимать» в этой конкретной среде, культуре, бизнесе и организационной структуре. Менеджеры по информационной безопасности должны осознавать жизненный цикл информационных активов организации и планы на будущее, а бизнес-риски необходимо измерять, чтобы удостовериться, что риски оцениваются и должным образом снижаются на каждом этапе жизненного цикла. Чем успешнее это будет сделано, тем больше вероятность того, что функция ISM будет признана законной для предоставления ценности предприятию. Кроме того, должны быть разработаны политика ISM и ISMS (система управления информационной безопасностью), чтобы обеспечить защиту данных на всех этапах.

Чтобы достичь четкого и эффективного набора методов ISM, организация должна выполнить следующие шаги [1]:

1. знать политику и планы безопасности бизнеса;

2. понимание текущих и будущих требований безопасности бизнеса;
3. документирование всех мер безопасности и их работу, техническое обслуживание и связанные с ними риски;
4. управление всеми нарушениями безопасности и происшествиями;
5. управление поставщиками и контрактами в отношении доступа к системам и услугам в сочетании с функцией управления;
6. упреждающее улучшение средств контроля безопасности и управления рисками безопасности.

Проблемматика

Проблема информационной безопасности характеризуется сложностью и взаимозависимостью. Что содержит значительное количество факторов и элементов, которые взаимосвязаны друг с другом. Присутствие человеческого фактора еще больше усложняет ситуацию, поскольку люди обладают свободой воли и всегда будут действовать в своих интересах. Более того, растущая зависимость от Интернета практически во всех сферах деловой активности делает безопасность серьезной проблемой для многих заинтересованных сторон (частных лиц, предприятий, правительств и т. д.).

Существенным элементом любой системы защиты информации являются затраты, связанные с ее проектированием, разработкой, внедрением и выводом из эксплуатации. Необходимы значительные инвестиции для создания и обслуживания высоконадежных, быстро реагирующих и заслуживающих доверия систем информационной безопасности. Хотя очень немногие будут утверждать, что информация, хранящаяся, обрабатываемая и передаваемая в компьютерных системах, не сопряжена со значительными рисками, доводы в пользу инвестиций в надлежащие меры безопасности по-прежнему трудно обосновать. Можно утверждать, что основной причиной уделения информационной безопасности приоритетного внимания в повестке дня корпораций в последнее десятилетие были повышенные и строгие требования к соблюдению нормативных требований, предъявляемые к коммерческим организациям. Кроме того, крупный бизнес развил разумное понимание последствий плохой защиты информационных систем. Следовательно, большая часть бизнес-бюджетов была выделена на улучшение защиты корпоративных цифровых активов.

Хотя эти инвестиции и инициативы, безусловно, уменьшат угрозы, исходящие от современного электронного рынка, другие аспекты проблемы остаются в значительной степени нерешенными. Сложность и взаимозависимость проблем безопасности в Интернете серьезно ограничивают эффективность любой инициативы, предпринятой в конкретных организационных или географических контекстах.

Из-за серьезного отсутствия осведомленности о негативных последствиях проблем и угроз информационной безопасности среди малых и средних предприятий (МСП), в дополнение к восприятию менее строгих нормативных требований и очень высоких относительных затрат на защиту цифровой информации, информационные и коммуникационные инфраструктуры этих фирм остаются крайне незащищенными и уязвимыми.

Взаимосвязанность становится все более важным требованием для делового общения. Крупные организации полагаются на услуги, предоставляемые множеством более мелких партнеров и подрядчиков, расположенных за пределами географических границ. Этим более

мелким фирмам следует предоставить определенные уровни доступа к информационным системам крупных организаций для выполнения своих деловых контрактов. Получая доступ к информационным системам организации, партнеры и подрядчики фактически становятся частью корпоративной сети. Учитывая возможность возникновения угроз безопасности и атак с любой машины, подключенной к глобальной сети, малые и средние предприятия выступают в роли «самого слабого звена» в сети. Самое слабое звено в любой сети является привлекательной точкой входа для злоумышленников, желающих взломать систему, и любая сеть так же безопасна, как и ее самое слабое звено. Это означает, что для надлежащей защиты глобальной сети Интернет необходимо применять более целостный подход, уделяя особое внимание самому слабому звену: МСП.

Проблема информационной безопасности в МСП не может быть решена только за счет повышения осведомленности о серьезности ее последствий. Однако многие другие факторы еще больше усложняют ситуацию; и призыв к немедленным действиям жизненно важен. Даже при соответствующей осведомленности и полном понимании вопросов безопасности МСП не обладают необходимыми ресурсами (человеческими, денежными или техническими), которые следует инвестировать для решения проблемы. МСП обычно работают в условиях очень ограниченного бюджета; имеют серьезно ограниченную рабочую силу, и многие потребности конкурируют за очень ограниченный запас ресурсов, что приводит к тому, что информационная безопасность отодвигается на второй план в списке приоритетов. Здесь действует цикл отрицательной обратной связи: меньшая осведомленность о проблеме информационной безопасности отодвигает ее вниз по списку приоритетов, что, в свою очередь, уменьшает выделяемые на нее ресурсы, что приводит к еще более низкой осведомленности (рисунок 1).

Рисунок 1 – Цикл отрицательной обратной связи в отношении осведомленности об информационной безопасности в МСП

Хотя вышеупомянутые проблемы обычно не возникают в контексте крупных организаций, они, безусловно, оказывают существенное влияние на проблему безопасности внутри этих фирм. Взаимосвязанность Интернета подразумевает, что, хотя эти проблемы могут быть связаны с небольшими предприятиями, они также оказывают существенное влияние на другие организации. Большинство инициатив, начатых с целью повышения информационной безопасности в крупных организациях, имели локальный характер, предполагая, что развитие общекорпоративной инфраструктуры безопасности информации и связи повысит статус безопасности во всей организации. Это предположение игнорирует тот важный факт, что электронные атаки и угрозы безопасности могут исходить из любой точки земного шара. Повышенная защита периметра корпоративной сети больше не является эффективным вариантом из-за необходимости трансграничной связи и совместной работы. К безопасности следует подходить с комплексной точки зрения, учитывающей взаимозависимый и взаимосвязанный характер современных глобальных коммуникаций.

Кроме того, из-за серьезной нехватки квалифицированных технических специалистов и опыта информационная безопасность обычно воспринимается как высокая стоимость, которая должна быть достаточно хорошо обоснована, чтобы ее можно было продолжать. Крупные и многонациональные организации и конгломераты изо всех сил пытаются добиться одобрения и распределения своих собственных бюджетов на безопасность, даже несмотря на то, что дело, которое они приводят, весьма привлекательно. При такой предполагаемой высокой стоимости безопасности она будет чрезмерной

Целостный подход к информационной безопасности

Было разработано несколько методологий и стандартов для решения все более важных вопросов информационной безопасности (примеры включают CRAMM [2] и ISO17799 [3]).

Перед разработкой любой системы управления информационной безопасностью необходимо четко определить и сформулировать предполагаемые цели системы. На данном этапе важно признать изменяющуюся бизнес-среду, в которой обычно работают МСП. Это потребует адаптации целей безопасности в соответствии с новыми бизнес-требованиями. Таким образом, гибкость в определении и переопределении целей с минимальными требованиями к ресурсам имеет решающее значение для успеха предлагаемого подхода. Чтобы четко и однозначно определить требования, мы предлагаем использовать методологию мягких систем (SSM). SSM был предложен Питером Чеклендом [4] как «общий подход к решению проблем, подходящий для систем человеческой деятельности» (см. рисунок 2).

Управление безопасностью всегда следует воспринимать как непрерывный процесс. В условиях современного динамичного рынка уже недостаточно внедрять отличные меры безопасности без оценки изменений в бизнес-среде и требованиях. Особенно это касается малых и средних предприятий. Небольшие организации гораздо более гибкие, чем их более крупные коллеги, и они обычно извлекают выгоду из этой гибкости, чтобы выходить на различные рынки и адаптировать методы ведения своего бизнеса.

Последний этап связан с изменением характера деловой среды. Он направлен на адаптацию реализации СМИБ [5] для реагирования на изменения бизнес-требований. Когда какое-либо серьезное изменение требует значительного изменения в СУИБ компании, можно использовать тот же процесс, описанный выше, чтобы адаптировать решение для удовлетворения новых потребностей.

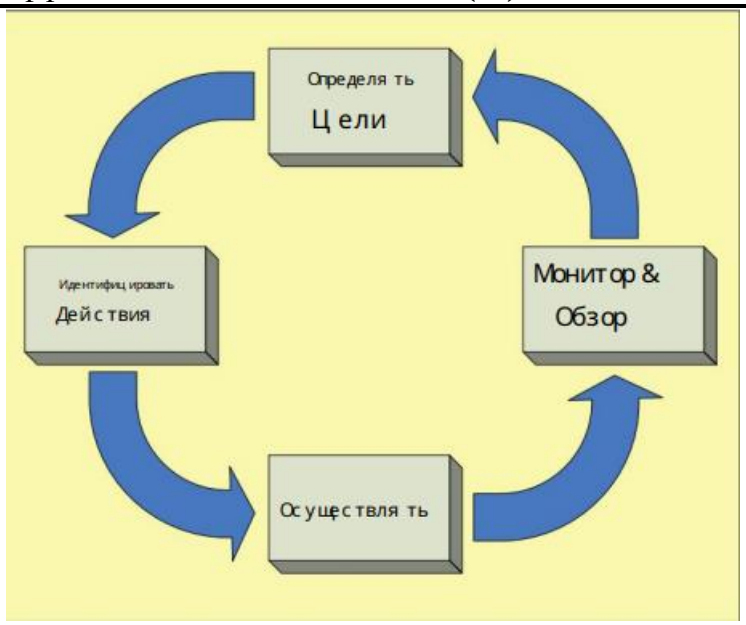

Рисунок 2 – Четыре этапа процесса управления безопасностью малого и среднего бизнеса

Выводы

Большое внимание уделяется проблеме защиты цифровой информации на современном технологическом рынке. Информация, собираемая, хранящаяся, обрабатываемая и передаваемая организациями, может быть очень конфиденциальной и повлечь за собой серьезные негативные последствия, если ее целостность, конфиденциальность или доступность будут нарушены. Организации любого размера должны проявлять должное усердие в защите информации, которой они располагают. В то время как крупные организации вложили разумные средства в повышение стандартов информационной безопасности в своей деятельности, малые и средние предприятия сталкиваются со многими проблемами в достижении повышенных уровней безопасности.

В этой статье представлены некоторые проблемы, препятствующие развитию информационной безопасности в МСП. Эти проблемы включают, но не ограничиваются ограниченными бюджетами, ограниченными человеческими ресурсами и постоянно меняющейся бизнес-средой. Был предложен целостный подход к управлению информационной безопасностью на малых и средних предприятиях, основанный на методологии мягких систем, который признает и решает эти проблемы. Этот структурированный подход включает четыре этапа: определение целей безопасности предприятия, определение действий, осуществление действий, а также мониторинг и анализ реализации безопасности.

Список литературы

1. Бэйси фон Солмс, «Управление информационной безопасностью и соответствием требованиям по сравнению с операционным управлением», Компьютеры и безопасность, 24, Elsevier, стр. 443-447, 2005.
2. Инструментарий управления рисками CRAMM. http://www.cramm.com
3. ISO17799 Информационные технологии. Методы обеспечения безопасности. Свод практических правил по обеспечению информационной безопасности

4. Checkland, P. (1999) Системное мышление, системная практика. Уайли, Западный Суссекс, ВЕЛИКОБРИТАНИЯ.
5. Институт защиты информационной инфраструктуры (I3P) (2003 г.), Программа исследований и разработок в области кибербезопасности.

References

1. Basie von Solms, "Information Security and Compliance Management Versus Operational Management", Computers and Security, 24, Elsevier, pp. 443-447, 2005.
2. CRAMM risk management tools. http://www.cramm.com
3. ISO17799 Information technology. Security methods. Code of Practice for Information Security
4. Checkland, P. (1999) Systems thinking, systems practice. Wylie, West Sussex, UK.
5. Institute for Information Infrastructure Protection (I3P) (2003), Cybersecurity Research and Development Program..

Руденко Н.В. Анализ технических решений и основных направлений повышения безопасности движения по автомобильным дорогам// Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 104–108

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.3

АНАЛИЗ ТЕХНИЧЕСКИХ РЕШЕНИЙ И ОСНОВНЫХ НАПРАВЛЕНИЙ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ДВИЖЕНИЯ ПО АВТОМОБИЛЬНЫМ ДОРОГАМ

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

В данной статье проведен анализ технических решений и основных направлений повышения безопасности движения по автомобильным дорогам. Актуальность работы заключается в том, что в современном мире бурно развивается сфера информационных технологий и телекоммуникаций, что дает возможность применения их на автомобильных дорогах и повышению безопасности движения по ним.

Ключевые слова: анализ, безопасность дорожного движения, автомобильные дороги, технические средства, аварийность.

ANALYSIS OF TECHNICAL SOLUTIONS AND THE MAIN DIRECTIONS OF IMPROVING 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

This article analyzes technical solutions and the main directions of improving traffic safety on highways. The relevance of the work lies in the fact that the sphere of information technologies and telecommunications is rapidly developing in the modern world, which makes it possible to use them on highways and improve traffic safety on them.

Keywords: analysis, road safety, highways, technical means, accident rate.

Оценка возможности применения существующих технических решений для обеспечения безопасности движения требует их классификации, которая приведена на рисунке 1.

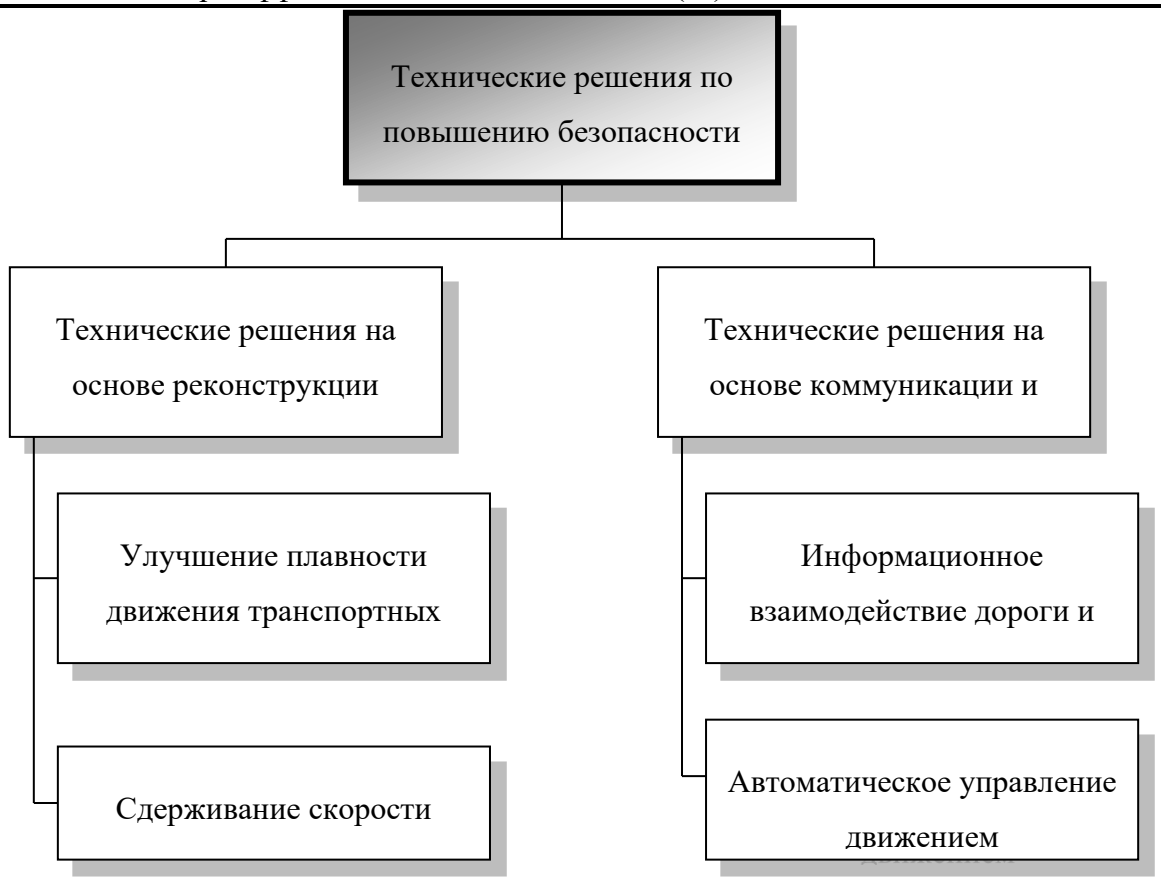

Рисунок 1 – Классификация технических решений по повышению безопасности дорожного движения

В результате анализа установлено, что технические решения, связанные с реконструкцией дорожной сети, требуют больших затрат денежных, материальных, временных и людских ресурсов.

Мощный импульс для повышения безопасности движения создают быстро развивающиеся средства коммуникаций и информационные технологии. С их применением открываются практические перспективы для повышения безопасности движения на новом качественном уровне, обеспечивающие «интеграцию» участников движения и системы управления движением на автомобильных дорогах при помощи средств телематики (телекоммуникации + информация), что способствует повышению организованности транспортных потоков, снижению перегруженности автомобильных дорог, повышению пропускной способности сети автомобильных дорог, снижению издержек и потерь при реализации задач транспортного обеспечения [10].

Бурное развитие цифровой телекоммуникационной техники обуславливает возможность ее применения для повышения безопасности движения на автомобильных дорогах. Анализ имеющихся технических средств контроля и управления движением, передачи данных, их технико-эксплуатационных характеристик в сопоставлении с задачами организации безопасного движения позволяет сделать вывод о том, что основу технических средств по управлению движением на автомобильных дорогах должны составить мобильные автоматизированные комплексы управления движением (АКУД-М). Их состав будет зависеть от объемов задач по организации движения и условий функционирования комплекса. Однако

можно предположить, что в его состав должны войти центральный компьютер с программным обеспечением, предназначенным для управления дорожным движением; периферийные исполнительные устройства управления движением (электронные светофоры, дорожные знаки и указатели, шлагбаумы и т.д.); устройства фиксации движущегося транспорта (различные датчики); периферийные устройства наблюдения и охраны (видеокамеры, датчики движения, сигнальные устройства); средства коммуникации центрального компьютера с периферийными устройствами (кабели или радиостанции); устройства обеспечения безопасности передаваемой информации (шифраторы и дешифраторы); устройства электропитания центрального компьютера и всех периферийных устройств и др.

Наиболее сложными элементами автоматического комплекса управления движением будут беспроводные модули передачи данных. Эти электронные устройства производятся в соответствии со стандартами Международного института инженеров электроники (IEEE 802.11 и 802.16), называемыми стандартами беспроводного доступа (эти стандарты совместимы между собой). К сожалению, комплектующие к таким устройствам отечественной промышленностью не производятся. Широкий выбор данных устройств предлагают такие крупные производители компьютерной и коммуникационной электроники как Siemens, D-Link, Linksys, ZyXEL, Motorolla, Proxim, Alvarion и др. Основой устройств данных производителей являются высокоскоростные чипсеты, производимые компаниями Intel, Fujitsu, Nokia, AT&T, Nanoradio, Samsung, Atheros и т.д.

Для связи на расстояния до 400 метров используются устройства так называемого стандарта WiFi (Wireless Fidelity – буквально «беспроводная точность»). Анализ показал, что им присущи как положительные, так и отрицательные свойства. Они обладают небольшими размерами, легкие, не требуют специализированных выносных антенн, затрачивают минимальное количество электроэнергии, а также обладают относительной дешевизной. Но имеющиеся недостатки, такие, как небольшой радиус действия, требуемые положительные температуры окружающей среды и низкий процент влажности, наличие прямой видимости подчиненных устройств, ограничивают возможности их применения. Такие устройства целесообразно использовать в качестве ретрансляторов (репитеров или повторителей), в радиусе расположения которых будут находиться исполнительные устройства, снабженные адаптерами WiFi. Требование наличия прямой видимости является большим недостатком технологии WiFi.

Данного недостатка лишена продукция, выпущенная по технологии WiMAX (World Interoperability for Microwave Access – «Международное взаимодействие для микроволнового доступа»). Все устройства, поддерживающие стандарт WiMAX, делятся на базовые станции, абонентские станции и антенны. Компании, предлагающие данную продукцию, как правило, стараются предложить законченное технологическое решение, включающее топологию системы беспроводного доступа, набор базовых и абонентских станций с антеннами. Это, возможно, будет наименее затратным вариантом [7]. В этом стандарте присутствуют и российские компании. В настоящее время не представляется возможным сравнить стоимость отечественных и зарубежных вариантов, но, скорее всего, проще и дешевле использовать продукцию российских производителей.

Как вариант можно выбрать InfiNet Wireless SkyMAN, WiMIC-6000, тем более что цена на один из них известна, что позволит обосновать экономическую эффективность внедрения данного оборудования.

Исполнительные устройства комплекса – светофоры, электронные дорожные знаки и указатели, шлагбаумы, также широко представлены производителями и дистрибьюторами. Так как эти устройства должны быть в мобильном исполнении, то они должны обладать небольшой массой, низким энергопотреблением при адекватных размерах и яркости. На сегодняшний момент такими характеристиками обладают светофоры со светодиодными апертурами [1].

Устройства управления проездами (шлагбаумы, барьеры) также должны быть мобильного исполнения, иметь съемные и складные рабочие органы.

Электронные дорожные знаки и указатели на сегодняшний день широко представлены на рынке технических средств управления движением [10]. Их технические характеристики определяются ГОСТ Р 52290-2004 «Технические средства организации дорожного движения. Знаки дорожные. Общие технические требования».

Для работы комплекса требуются технические средства сбора и обработки информации, являющиеся детекторами – датчиками различного вида в зависимости от типа информации, которую они принимают. По этому признаку различают индукционные, емкостные, лазерные, инфракрасные, оптические датчики. Наиболее сложные и дорогостоящие – оптические (видеодетекторы). Они выполняют наиболее широкий спектр задач.

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

Список литературы

1. Евстигнеев И.А. Основы создания интеллектуальных транспортных систем на автомобильных дорогах федерального значения России. – М.: Издательство «Перо», 2016 г. – 260 с.
2. СНиП 2.05.02-85. Автомобильные дороги. – Госстрой СССР, 1986 (1997 г.). – 51 с.
3. ГОСТ Р 50597-93. Автомобильные дороги и улицы. Требования к эксплуатационному состоянию, допустимому по условиям обеспечения безопасности движения.
4. ГОСТ Р 51256-99. Технические средства организации дорожного движения. Разметка дорожная. Типы и основные параметры. Общие технические требования.
5. ГОСТ Р 52289-2004. Технические средства организации дорожного движения. Правила применения дорожных знаков, разметки, светофоров, дорожных ограждений и направляющих устройств.
6. «Технические требования к оборудованию комплексов весогабаритного контроля на автомобильных дорогах общего пользования федерального значения», Росавтодор, Исх. №01-1135 от 08.08.2013.
7. Артынов, А.П. Автоматизация управления транспортными системами / А.П. Артынов [и др.] / отв. ред. А.А. Воронов. – М., 1984. – 272 с.
8. Рэнкин, В. У. Автомобильные перевозки и организация дорожного движения: Справочник. Пер. с англ. / В.У. Рэнкин [и др.]. – М., 1981. – 592 с.
9. Бабков, В.Ф. Дорожные условия и безопасность движения: учеб. для вузов / В.Ф. Бабков. – М.: Трансп., 1993. – 271 с.
10. 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. Evstigneev I.A. Fundamentals of creating intelligent transport systems on federal highways in Russia. - M .: Publishing house "Pero", 2016 - 260 p.
2. SNiP 2.05.02-85. Car roads. - Gosstroy of the USSR, 1986 (1997). – 51 p.
3. GOST R 50597-93. Highways and streets. Requirements for the operational state, admissible under the terms of ensuring traffic safety.
4. GOST R 51256-99. Technical means of organizing traffic. Road marking. Types and basic parameters. General technical requirements.
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. "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.
7. Artynov, A.P. Automation of transport systems management / A.P. Artynov [and others] / otv. ed. A.A. Voronov. - M., 1984. - 272 p.
8. Rankin, VU Automobile transportation and organization of traffic: a Handbook. Per. from English. / V.U. Rankin [i dr.]. - M., 1981. - 592 p.
9. Babkov, V.F. Road conditions and traffic safety: textbook. for universities / V.F. Babkov. - M.: Transp., 1993. - 271 p.
10. 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 p.

Газетдинов Т.А., Аксенов С.Г. Обеспечение пожарной безопасности при функционировании пожаровзрывоопасного объекта// Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 4(26) часть 1 с. 109–111

Международный журнал информационных технологий и энергоэффективности

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

УДК 614.84

ОБЕСПЕЧЕНИЕ ПОЖАРНОЙ БЕЗОПАСНОСТИ ПРИ ФУНКЦИОНИРОВАНИИ ПОЖАРОВЗРЫВООПАСНОГО ОБЪЕКТА

[1] Газетдинов Т. А., [2]Аксенов С. Г.
ФГБОУ ВО «Уфимский университет науки и технологий», Уфа, Россия (450076, Республика Башкортостан, г Уфа, ул. Заки Валиди, д. 32), e-mail: [1] gazetdinov12035@yandex.ru, [2]2556668@mail.ru

В статье приведено описание машиностроительного предприятия как пожаровзрывоопасного объекта. Проведен прогноз событий развития аварийной ситуации при разгерметизации газопровода котельной. Произведено планирование превентивных и аварийно-спасательных и других неотложных работ в котельной при ликвидации чрезвычайной ситуации, вызванной разгерметизацией газопровода машиностроительного предприятия.

Ключевые слова: аварийно-спасательные работы, взрыв, газопровод, котельная, машиностроительное предприятие.

ENSURING FIRE SAFETY DURING FUNCTIONING OF A FIRE AND EXPLOSIVE FACILITY

[1] Gazetdinov T.A., [2] Aksenov S.G.
Ufa University of Science and Technology, Ufa, Russia (450076, Republic of Bashkortostan, Ufa, st. Zaki Validi, 32), e-mail: [1] gazetdinov12035@yandex.ru, [2]2556668@mail.ru

The article provides a description of a machine-building enterprise as a fire and explosion hazardous facility. A forecast of the development of an emergency in case of depressurization of the gas pipeline of the boiler house was carried out. Planning of preventive and emergency rescue and other urgent work in the boiler house during the liquidation of an emergency caused by depressurization of the gas pipeline of a machine-building enterprise.

Keywords: rescue operations, explosion, gas pipeline, boiler house, machine-building enterprise.

Машиностроение — это базовая отрасль обрабатывающей промышленности страны. Инфраструктура машиностроительного предприятия представляет потенциально опасный объект, который в аварийном режиме, способен привести к ЧС, представляя угрозу безопасности населения и территории, а также значительному материальному ущербу, особенно в условиях расположения в историческом центре мегаполиса.

На предприятии функционирует котельная, которая в свою очередь может служить причиной пожара (взрыва) при разгерметизации газопровода или ошибке обслуживающего персонала.

На рисунке 1 представлено дерево событий аварийного разрушения наружного наземного газопровода котельной машиностроительного предприятия.

Рисунок 1 – Дерево событий аварийного разрушения газопровода котельной машиностроительного предприятия

Проведен прогноз возможных событий развития аварийной ситуации при разгерметизации газопровода котельной по следующим сценариям: наиболее опасному; с наиболее неблагоприятными экологическими последствиями; и наиболее вероятному. Рассчитанный показатель реализации наиболее вероятного сценария с истечением газа без мгновенного воспламенения, образованием ГВС и с дальнейшим разрушением котельной составляет 7· 10-4 год-1.

Смоделировав аварию по наиболее вероятному сценарию, выявили, что свободный объем помещения котельной равен 9734,4 м3, а объем выброшенного газа при разгерметизации составляет 973,4 м3. Соответственно концентрация газа в помещении будет равна 10 %, что допускается в концентрационный предел взрываемости природного газа [1].

Оценены показатели оценки индивидуального и социального рисков для наиболее вероятного сценария – мгновенная разгерметизация.

Значение индивидуального риска меньше допустимого, в связи с тем, что условие безопасности людей выполнено (33·10-9≤10-6). Для дополнительного снижения риска необходимо внедрение систем пожаропредупреждения и пожарозащиты, разработка мер по снижению вероятности возникновения рассматриваемой чрезвычайной ситуации, проведение пожарно-тактических учений с участием работающего персонала.

Социальный риск в газовой котельной для персонала предприятия будет равен нулю, значит эксплуатация газопровода высокого давления в помещении котельной может быть допущена.

Был проведен расчет времени выдвижения сил и средств, количества спасателей и спасательной техники. Таким образом, общее время ликвидации при возникшей ЧС составляет 24 ч.

Для ликвидации ЧС в кратчайшие сроки, с привлечением минимальных сил и средств, организуется планирование аварийно-спасательных и других неотложных работ [2]. В работах задействовано 145 человек, из которых 2 врача, 9 медсестер, 6 пожарных; личный состав, который разбирает завалы и выполняет тяжелую, III категорию работ – 30 человек; личный состав, занимающийся восстановлением коммуникации и ведущий неотложные аварийно-восстановительные работы, выполняют работы средней тяжести II категории – 56 человек; формирования, занимающиеся перевозкой грузов, эвакуацией пострадавшего персонала, относятся к легкой категории работ – 8 человек; ремонтная группа по электросетям, с штатной численностью 22 человека; 12 человек с Аварийно-спасательного отряда.

Таким образом, в результате взрыва наружного наземного газопровода в зоне сильных разрушений произойдет повреждение теплопроводов от тепловых котлов при разгерметизации газопровода котельной. Поэтому персонал, находящийся под завалами получит ожоги различной степени тяжести. В ликвидации ЧС, вызванной разгерметизацией газопровода участвовали 145 человек личного формирования предприятия и привлеченных сил.

Список литературы

1. Приказ Ростехнадзора от 11.04.2016 № 144 Об утверждении Руководства по безопасности «Методические основы по проведению анализа опасностей и оценки риска аварий на опасных производственных объектах».
2. Обеспечение мероприятий и действий сил ликвидации чрезвычайных ситуаций: учебник в 3-х частях: часть 2. Инженерное обеспечение мероприятий и действий сил ликвидации чрезвычайных ситуаций: в 3-х книгах: книга 2. Оперативное прогнозирование инженерной обстановки в чрезвычайных ситуациях. / Под общ. ред. С.К. Шойгу/ В. А. Акатьев, С.С. Волков, В.С. Гаваза и др. - М.: ЗАО «ПАПИРУС», 1998. 176 с.

References

1. Order of Rostekhnadzor No. 144 dated April 11, 2016 On Approval of the Safety Guide “Methodological Framework for Hazard Analysis and Accident Risk Assessment at Hazardous Production Facilities”.
2. Provision of measures and actions of emergency response forces: a textbook in 3 parts: part 2. Engineering support of measures and actions of emergency response forces: in 3 books: book 2. Operational forecasting of the engineering situation in emergency situations. / Under the total. ed. S.K. Shoigu / V.A. Akatiev, S.S. Volkov, B.C. Gavaza and others - M .: CJSC "PAPIRUS", 1998. 176 p.