НАУЧНЫЙ ЖУРНАЛ

СИСТЕМЫ СИНХРОНИЗАЦИИ, ФОРМИРОВАНИЯ И ОБРАБОТКИ СИГНАЛОВ

№5-2022 год

Учредитель:
ООО «ИД Медиа Паблишер»

Номер подписан в печать 26.08.2022 г.

СОДЕРЖАНИЕ

Зуев М.Ю., Бобина Е.А, Логинов С.С.
РЕАЛИЗАЦИЯ ФОРМИРОВАТЕЛЕЙ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ СИСТЕМЫ ЛОРЕНЦА В ПЛИС **4**

Аббасов Э.М., Строганов В.И., Юшкевич У.К., Аббасова Т.С.
СОВЕРШЕНСТВОВАНИЕ БЕСПРОВОДНОЙ ИНФРАСТРУКТУРЫ VANET ДЛЯ АВТОМОБИЛЬНЫХ ДОРОГ **12**

Борисенко Б.Б., Ерохин С.Д., Фадеев А.С., Мартишин И.Д.
О СВЯЗИ ДАТАСЕТА CSE-CIC-IDS2018 С МАТРИЦЕЙ MITRE ATT&CK **16**

Бирюкова О.В., Корецкая И.В.
ВЛИЯНИЕ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ НА РАБОТУ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНОГО МОДУЛЯ **26**

Афанасьев К.М., Сидоров К.М.
МАТЕМАТИЧЕСКАЯ (КОМПЬЮТЕРНАЯ) МОДЕЛЬ ТЯГОВОГО ЭЛЕКТРИЧЕСКОГО ПРИВОДА ЭЛЕКТРОМОБИЛЯ **35**

Куприянов Е.С., Сидоров К.М.
ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ СИНХРОННЫМ ЭЛЕКТРОДВИГАТЕЛЕМ С ВОЗБУЖДЕНИЕМ ОТ ПОСТОЯННЫХ МАГНИТОВ **40**

Глазов В.А., Илюшенко В.К., Ерусланкин С.А.
АНАЛИЗ ТЕХНИЧЕСКОГО УРОВНЯ И ТЕНДЕНЦИЯ РАЗВИТИЯ СПОСОБОВ И УСТРОЙСТВ В ОБЛАСТИ УПРАВЛЕНИЯ ТЯГОВОЙ СИСТЕМОЙ ТРАНСПОРТНЫХ СРЕДСТВ С ЭЛЕКТРОТЯГОЙ **43**

РЕАЛИЗАЦИЯ ФОРМИРОВАТЕЛЕЙ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ СИСТЕМЫ ЛОРЕНЦА В ПЛИС

Зуев Максим Юрьевич
КНИТУ-КАИ имени А.Н. Туполева, г. Казань, Россия
maxzv93@mail.ru

Бобина Елена Андреевна
КНИТУ-КАИ имени А.Н. Туполева, ассистент каф. ЭКСПИ, к.т.н., г. Казань, Россия
eabobina@yandex.ru

Логинов Сергей Сергеевич
КНИТУ-КАИ имени А.Н. Туполева, профессор каф. ЭКСПИ, д.т.н., г. Казань, Россия
sslogin@mail.ru

Аннотация
В работе приведены результаты реализации в ПЛИС алгоритма формирования псевдослучайных последовательностей, сформированных на основе модифицированной динамической системы Лоренца над конечным полем Галуа. Сопоставлены реализации формирователей на основе КР эффекта и реализованных в арифметике над полем Галуа. Показана возможность реализации формирователей псевдослучайных последовательностей на основе системы Лоренца на относительно не дорогих и простых ПЛИС. Результаты работы могут быть использованы в средствах маскирования информации, асинхронно-адресных системах передачи информации, при построении систем связи с широкополосными сигналами, в моделировании и криптографии.

Ключевые слова
Формирователь псевдослучайных последовательностей, система Лоренца, формирователь на ПЛИС, генератор хаоса, FPGA.

Введение

В современных системах передачи с целью повышения защищенности передаваемой информации от несанкционированного доступа (НСД) и снижения пик-фактора формируемых радиосигналов методом маскирования информации находят широкое применение формирователи псевдослучайных последовательностей (ПСП) [1]. Наиболее распространенными методами формирования ПСП являются методы, основанные на формировании М-последовательностей; последовательностей Голда и Касами; коды Баркера; а также формирователь, основанный на свойствах простых чисел Мерсенна.

Формирователи М-последовательностей просты в реализации и имеют хорошие авто- и взаимно- корреляционные функции (АКФ и ВКФ) [2]. Из-за своих авто- и взаимно-корреляционных функций такие последовательности часто применяются в асинхронных системах связи в качестве синхроимпульсов. Недостатком таких формирователей является ограниченный период следования ПСП, не превышающий квадрата длины регистра сдвига n. Кроме того, для восстановления М-последовательности достаточно 2n символов, вследствие чего они имеет низкую структурную скрытность, а значит плохо подходят для устройств защищенности передаваемой информации от несанкционированного доступа.

В системах множественного доступа с кодовым разделением (CDMA) чаще всего используются псевдослучайные последовательности Голда и Касами. Последовательности Голда с периодом 2^n-1 формируются из двух М-последовательностей путем их сложения по модулю. Коды Касами реализу-

ются последовательным включением трех регистров сдвига с различными обратными связями, каждый регистр формирует свою М-последовательность [3]. Преимуществом таких формирователей является меньший уровень боковых пиков АКФ, формируемых ПСП по сравнению с М-последовательностями; недостатками – ограниченный период следования ПСП, не превышающий квадрата длины регистра сдвига, и низкая структурная скрытность [3].

Последовательности Баркера – это ПСП с малым значением апериодической автокорреляционной функции. Их достоинство заключается в обеспечении синхронизации передаваемых и принимаемых сигналов за достаточно короткий промежуток времени, обычно равный длине самой последовательности. Недостатком данных последовательностей для применения в системах защиты передаваемой информации от несанкционированного доступа и снижения пик-фактора сигналов является их период.

Вихрь Мерсенна представляет собой формирователь псевдослучайных чисел, основанный на свойствах простых чисел. Он обеспечивает быструю генерацию высококачественных псевдослучайных чисел и малую корреляцию формируемых псевдослучайных чисел. В ряде работ [4, 5] показано, что период вихря Мерсенна равен 2^{19937} - 1, что вполне достаточно для большинства практических приложений. Недостаток этого формирователя в том, что он не является криптостойким, это обстоятельство ограничивает его использование в системах защиты информации от НСД. Поэтому основной областью его применения является статистическое моделирование [6].

Таким образом, ПСП, формируемые на основе логических схем, просты в генерации, могут быть реализованы на простых логических схемах, но при этом имеют низкую криптостойкость и малый период использования в средствах защиты информации от НСД.

В настоящее время активно используются формирователи ПСП на основе хаотических систем (напр. модификаций генераторов динамического хаоса, реализованных в условиях квазирезонансных воздействий на параметры временной сетки). К таким формирователям можно отнести формирователи ПСП на основе динамических систем Лоренца, Чуа, Дмитриева-Кислова, Анищенко-Астахова и др. Цифровые реализации систем на основе численного интегрирования дифференциальных уравнений позволяют получить воспроизводимость характеристик как на передающем, так и на приемном конце канала связи [7-9, 14]. Хаотические радиоэлектронные системы чувствительны к начальным условиям, и малейшие их изменения могут привести к колоссальным различиям, что в свою очередь может повлечь увеличение разнообразия форм генерируемых сигналов. Эта особенность хаотических систем при использовании их в средствах маскирования позволяет повысить защищенность передаваемой информации от НСД [10,11].

При практической реализации средств маскирования информации и снижения пик-фактора требуется учитывать объем занимаемых ресурсов в реальном устройстве (микросхеме). В связи с чем при реализации формирователей ПСП на основе хаотических систем важным является использование более простых форматов представления чисел с наименьшим возможным числом разрядов. Более простые форматы представления чисел ведут к упрощению схемотехнической реализации формирователей, а, следовательно и сокращению требуемых ресурсов программируемых логических интегральных схем в сравнении с формирователями, реализованными для форматов представления чисел типов double и float.

Таким образом, целью данной работы является сравнение объема ресурсов, занимаемых описаниями схем формирователей псевдослучайных последовательностей, реализованных с использованием цифровых систем с динамическим хаосом в программируемых логических интегральных схемах.

Для достижения поставленной цели рассмотрим схемотехническую реализацию формирователей ПСП на основе модифицированных хаотических систем, реализованных в условиях квазирезонансных воздействий на параметры временной сетки и формирователей ПСП, реализованных в арифметике над полем Галуа.

Схемотехническая реализация формирователей псевдослучайных последовательностей на основе модифицированных хаотических систем

В качестве исходной динамической системы, которая подвергалась модификациям, в работе выбрана динамическая система Лоренца [1-3]. Вид логической схемы для формирователя, работающего в условиях квазирезонансных воздействий на параметры временной сетки, приведен на рисунке 1.

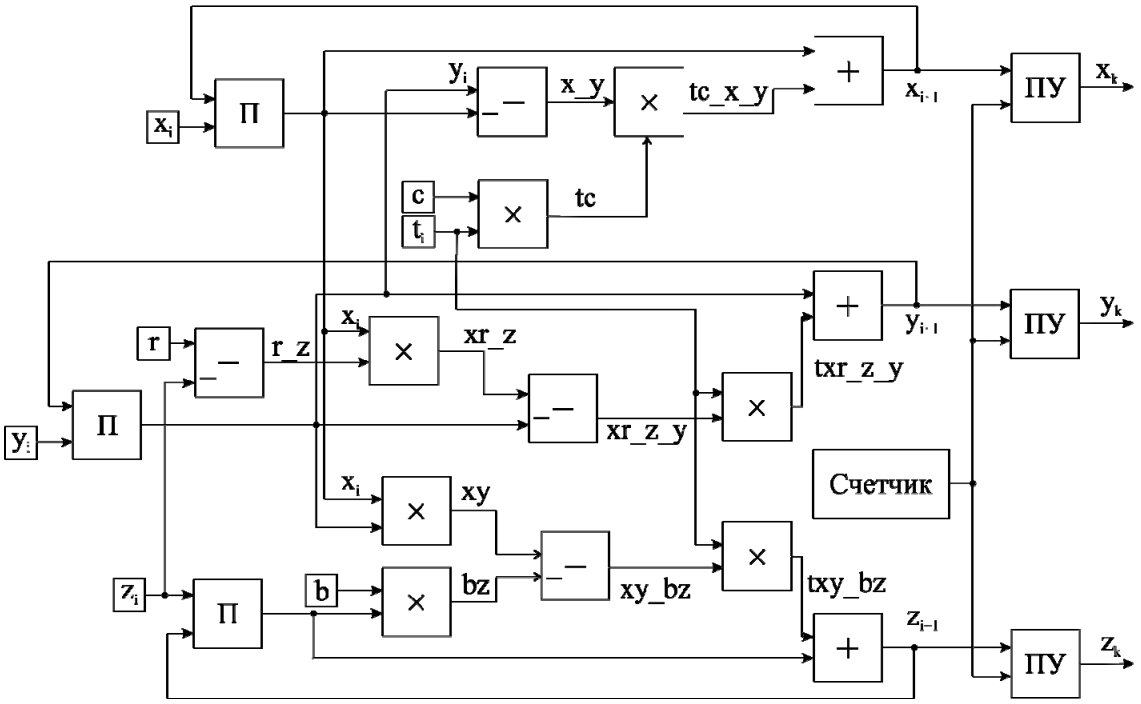


Рис. 1. Структурная схема формирователя псевдослучайных последовательностей на основе системы Лоренца в условиях квазирезонансных воздействий

На рисунке1 приведена структурная схема формирователя ПСП, в которой каждый новый элемент формируемой последовательности вычисляется с учетом значения N разрядного счетчика.

Согласно приведенной схеме с сигналами с регистров x_i, y_i, z_i производятся операции, которые можно описать численным решением дифференциальных уравнений системы Лоренца (1):

$$\begin{cases} X_{i+1} = X_i + t \cdot c(X_i + Y_i), \\ Y_{i+1} = Y_i + t(r \cdot X_i + Y_i + X_i \cdot Z_i), \\ Z_{i+1} = Z_i + t(b \cdot Z_i + X_i \cdot Y_i). \end{cases} \quad (1)$$

где t – шаг интегрирования динамической системы; r – число Рэлея, c – число Прандтля, b – геометрический параметр динамической системы.

Другим вариантом формирователя ПСП является модифицированный генератор хаоса, реализованный в арифметике над полем Галуа, рассмотренный и предложенный в работе [12, 13]. Его отличительной особенностью является наличие блока памяти примитивных полиномов, образующих поле Галуа. Такой подход позволяет увеличить период формируемых последовательностей путем периодической смены полинома, образующего поле.

$$\begin{cases} X_{i+1} = (X_{i-1} \oplus X_i) \oplus t \cdot c \cdot (X_i \oplus Y_i), \\ Y_{i+1} = (Y_{i-1} \oplus Y_i) \oplus t \cdot (r \cdot X_i \oplus Y_i \oplus X_i \cdot Z_i), \\ Z_{i+1} = (Z_{i-1} \oplus Z_i) \oplus t \cdot (b \cdot Z_i \oplus X_i \cdot Y_i). \end{cases} \quad (2)$$

Рассмотрим структурную схему формирователя ПСП, реализованного в арифметике над полем Галуа, приведенную на рисунке 2.

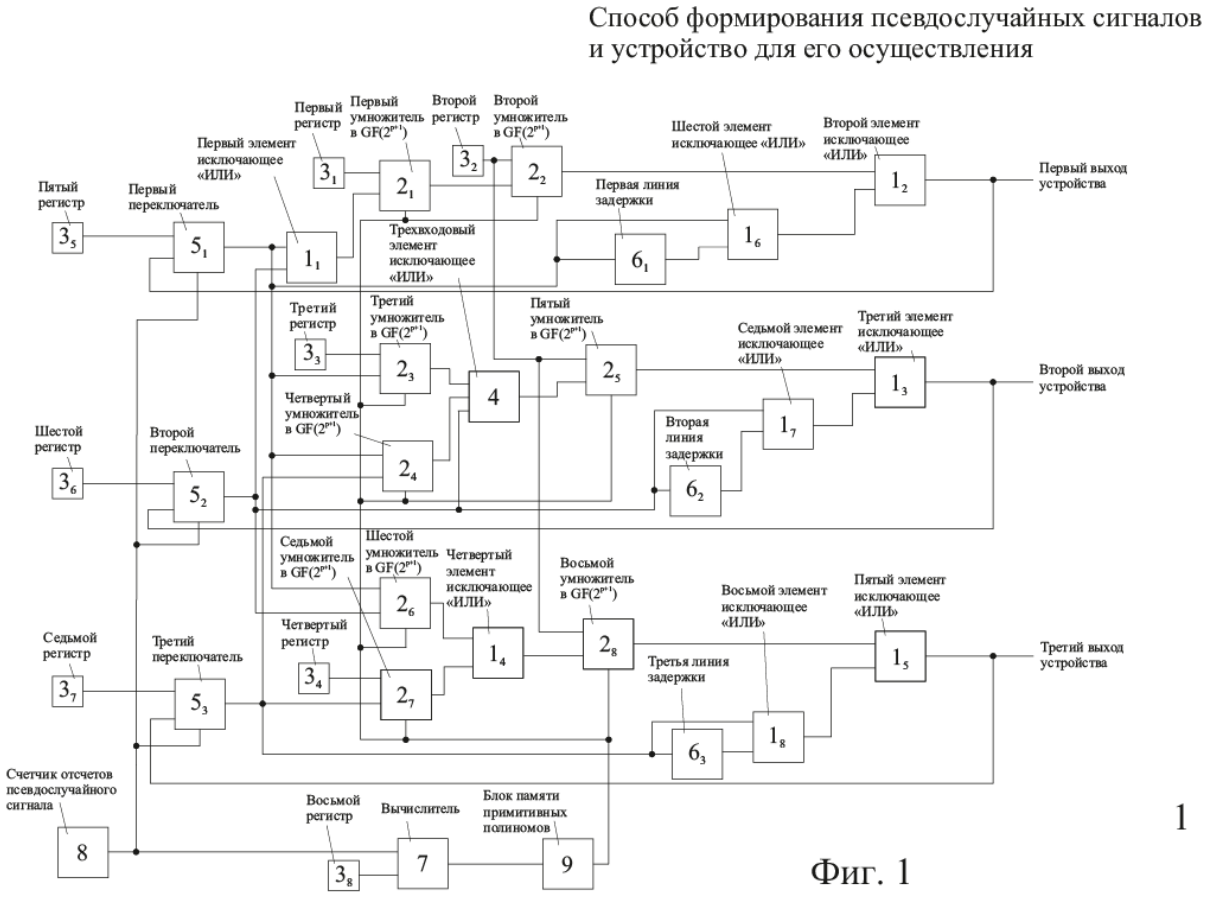


Рис. 2. Структурная схема формирователя псевдослучайных последовательностей на основе системы Лоренца, реализованной над полем Галуа [13]

Отличительной особенностью схемы формирователя, реализованного в арифметике над полем Галуа, является наличие счетчика, который используется для периодической смены полинома, образующего поле на следующий полином из блока памяти примитивных полиномов. Следует отметить, что схема, приведенная на рис.2 может быть использована для любой степени P полинома, образующего поле Галуа основанием два $GF(2^P)$.

Из системы (2) видно, что уравнения для компонент *X, Y, Z* системы могут быть вычислены параллельно, что является преимуществом при реализации устройства в ПЛИС.

Для систем уравнений (1) и (2) начальные условия могут быть различны, но даже небольшое отклонение хотя бы одного из исходных параметров приводит к колоссальным изменениям в формируемых последовательностях.

С точки зрения формируемых последовательностей интерес представляет сравнение статистических характеристик формируемых ПСП.

Статистические характеристики исследуемых формирователей

Рассмотрим анализ статистических характеристик формируемых псевдослучайных последовательностей путем реализации нелинейной хаотической системы Лоренца в условиях квазирезонансных воздействий и реализованной в арифметике над полем Галуа для 32 разрядных систем. Одними из важнейших характеристик являются тесты на «случайность» и «равномерность» формируемых последовательностей. Одним из вариантов таких тестов являются тесты FIPS-140-2, предложенные американским институтом стандартов и технологий. Результаты прохождения этих тестов на «случайность», псевдослучайными последовательностями формируемых на основе систем с динамическим хаосом при вариации параметра глубины модуляции временной сетки m приведены в Таблице 1.

Таблица 1

Результаты прохождения тестов FIPS-140-2

Система на основе	КР воздействий			Арифметики над полем Галуа		
Тест	m=1	m=3	m=9	X	Y	Z
Monobit Test	1000	1000	1000	1000	1000	1000
Poker Test	866	735	1000	957	955	952
Run Test 1	974	739	1000	665	653	624
Run Test 2	983	839	1000	995	995	999
Run Test 3	998	1000	1000	999	1000	1000
Run Test 4	1000	1000	1000	1000	1000	1000
Run Test 5	1000	999	1000	1000	1000	1000
Run Test 6+	911	978	1000	999	997	999
Все тесты	797	544	999	659	641	602

Результаты показали, что наилучшие показатели прохождения тестов достигнуты формирователем ПСП на основе системы Лоренца достигаются при параметрах глубины модуляции временной сетки *m* равным 1 и 9.

Другими не менее важными характеристиками полученных бинарных ПСП являются их АКФ и ВКФ.

В таблице 2 приведены результаты оценки статистических характеристик системы Лоренца, реализованных в условиях квазирезонансных воздействий на параметр временной сетки и в арифметике над полем Галуа $GF(2^{32})$.

Таблица 2

АКФ и ВКФ двоичных последовательностей анализируемой системы Лоренца

	На основе КР воздействий для типа float		Над полем Галуа $GF(2^{32})$	
	АКФ	ВКФ	АКФ	ВКФ
X $R_{max}\sqrt{N}$	3,121	3,274	3,110	3,298
X $m_{|R|}\sqrt{N}$	0,533	0,532	0,532	0,532

В результате моделирования выяснилось, что величина бокового пика АКФ и ВКФ для формирователя ПСП на основе квазирезонансных воздействий на параметр временной сетки и арифметики над полем Галуа различаются между собой. Согласно классификации, приведенной в работе [2], сформированные двоичные сигналы соответствуют «случайным» последовательностям.

Сравнение результатов практической реализации формирователя псевдослучайных последовательностей

С точки зрения практической реализации средств маскирования информации и снижения пик-фактора сигналов радиоэлектронных систем с ортогональным частотным мультиплексированием в цифровых устройствах требуется учитывать объем занимаемых ресурсов в реальном устройстве (микросхеме). Например, при реализации устройства на базе микроконтроллера следует учитывать объем занимаемой программой памяти, при реализации в ПЛИС как в нашем случае – количество используемых логических вентилей (логических ячеек). При разработке устройств и систем в ПЛИС особое внимание следует уделять выделенному на реализацию бюджету, т.к. особенностью младших семейств ПЛИС фирмы Xilinx (напр. spartan 3) является отсутствие поддержки блоков, позволяющих выполнять операции с плавающей запятой, что ведет к выбору ПЛИС старших и более дорогих семейств типа virtex или kintex.

На рисунке3 приведены отчеты результаты моделирования в среде ISE Xilinx формирователей, приведенных на рисунках 1 и 2.

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	9372	597200	1%
Number of Slice LUTs	8207	298600	2%
Number of fully used LUT-FF pairs	219	17360	1%

Device Utilization Summary			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Flip Flops	3,017	17,344	17%
Number of 4 input LUTs	4,952	17,344	28%
Number of occupied Slices	3,622	8,672	41%

Рис. 3. Отчеты о ресурсах ПЛИС, необходимых для реализации сравниваемых формирователей

Согласно приведенным отчетам об использовании ресурсов (рисунок 3) ПЛИС схема для формирования многоуровневых ПСП с числом разрядов 32 в случае формирователя на основе квазирезонансного эффекта для формата представления чисел типа float занимает 9372 D триггера, 8207 базовых логических элементов, 219 триггеров; схема для формирователя, реализованного в арифметике над полем Галуа, занимает 3622 D триггера, 4952 базовых логических элемента, 3017 триггеров.

Временные диаграммы ПСП, полученные в результате вычисления компонент *X, Y* и *Z* при моделировании в ПЛИС, для обоих видов формирователей соответствуют результатам, полученным при моделировании формирователей последовательностей в среде Matlab.

В приведенной практической реализации формирователя, реализованного над полем Галуа, операции XOR (побитовое «исключающее или») выполняются за 1-2 такта, операция сдвига занимает один такт, а операции умножения полиномов занимают 1024 такта, реализован 8 разрядный счетчик, используемый для смены полинома образующего поле, а также в блок памяти примитивных полиномов записано 7 полиномов 32 степени.

Заключение

В работе проведено сравнение объема ресурсов, занимаемых описаниями схем формирователей псевдослучайных последовательностей, реализованных с использованием цифровых систем с динамическим хаосом в программируемых логических интегральных схемах.

Проведено сопоставление статистических характеристик формирователей псевдослучайных последовательностей полученных с использование модифицированной динамической системы Лоренца реализованной в условиях квазирезонансных воздействий на параметр временной сетки для типа представления чисел типа float и реализованной над полем Галуа $GF(2^{32})$. Согласно полученным результатам оба формирователя подходят в качестве устройств формирования ПСП с целью маскирования информации.

Согласно полученным результатам, формирователь, реализованный в арифметике над полем Галуа, занимает в 3 раза меньше ресурсов ПЛИС по сравнению с формирователем, реализованным на основе генератора хаоса, работающего в условиях квазирезонансных воздействий на параметр временной сетки. Это обстоятельство позволяет использовать для реализовать формирователя арифметике над полем ПЛИС из линейки младшего семейства типа Spartan 3. В работе показано, что для построения формирователей псевдослучайных последовательностей на основе модифицированных динамических систем Лоренца без ущерба статистическим характеристикам формируемых последовательностей могут быть использованы простые и недорогие ПЛИС.

Литература

1. *Enzeng D.,* et al. A Chaotic Images Encryption Algorithm with the Key Mixing Proportion Factor // 2008 International Conference on Information Management, Innovation Management and Industrial Engineering. – 2008 – pp. 169-174. – DOI: 10.1109/ICIII.2008.25.

2. *Varakin L.E.* Communication systems with noise-like signals. M.: Radio and communication, 1985. 384 p.

3. *Ипатов В*. Широкополосные системы и кодовое разделение сигналов. Москва: ТЕХНОСФЕРА – 2007. 488 с.

4. *Matsumoto M., Nishimura T*. Mersenne twister: A 623-dimensionally equidistributed uniform pseudorandom number generator (англ.) // ACM Trans. on Modeling and Computer Simulations: journal. 2017. Vol. 8, no. 1, pp. 3-30. DOI: 10.1145/272991.272995.

5. *Matsumoto M., Kurita Y*. Twisted GFSR generators // ACM Trans. on Modeling and Computer Simulations. 1992. Т. 2, № 3. С. 179-194. DOI: 10.1145/146382.146383.

6. *Lerner I.M., Khairullin A.N., Kaprovich V.L., Il'in V.I. and Odintsov V.L*., "A Numerical Method to Estimate the Potential Capacity of Communication Channels Using FSK-n-Signals with ISI," 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), St. Petersburg, Russia, 2020, pp. 1-9, doi: 10.1109/WECONF48837.2020.9131510.

7. *Afanasiev V.V., Loginov S.S., Polskii Yu.E.* Statistical characteristics of binary pseudorandom signals generated on the basis of Lorentz and Chua systems // Telecommunication and Radio Engineering. Vol.72, 2013, Issue 4.20. P. 283-289. DOI: 10.7868/S0033849413040013.

8. *Zuev M.Y., Sivintseva O.A., Loginov S.S.* Pseudo-Random Signal Generator Based on the Rössler System Implemented Over a Finite Galois Field // 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) – 2020. P. 9131522. DOI: 10.1109/WECONF48837.2020.9131522.

9. *Zuev M.Y., Loginov S.S*. Generation of pseudo-random signals based on a modified Lorenz system, realized over a Galois finite field // 2018 Systems of Signals Generating and Processing in the Field of on Board Communications P. 8350594-4. DOI: 10.1109/SOSG.2018.8350594.

10. *Loginov S.S., Zuev M.Y., Agacheva Y.G*. A Pseudorandom Signal Generator Based on the Lorentz System Subjected to Quasi-Resonant Action // 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) – 2020. P. 9131530. DOI: 10.1109/WECONF48837.2020.9131530.

11. *Danilaev M.P., Afanasiev V.V., Loginov S.S., Polsky Y.E.* Diagnostics and stabilization of multimode nonlinear radio physics systems (2017) 2017 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SINKHROINFO 2017, статья № 7997516. DOI: 10.1109/SINKHROINFO.2017.7997516.

12. *Zuev M.Y., Loginov S.S*. Practical Implementation of a Pseudo-Random Signal Generator Based on the Lorenz System Realized on FPGA // 2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), 2019. P. 8814209. DOI: 10.1109/SYNCHROINFO.2019.8814209.

13. Патент № 2769539 РФ, МПК G06F 7/58 (2006.01). Способ формирования псевдослучайных сигналов и устройство для его осуществления/ С.С. Логинов, М.Ю. Зуев, О.А. Сивинцева; заявитель и патентообладатель ФГБОУ ВО «Казанский национальный исследовательский техический университет им. А.Н. Туполева-КАИ» (RU). № 2021110101: заявл. 13.04.2021: опубл. 01.04.2022.

14. Yaushev S.T., Faizullin R.R., Lerner I.M. Quasi-determined algorithm for resolution of randomly fluctuating signals and chaotic pulse interference // T-Comm. 2020. Т. 14. № 2. С. 39-44.

СОВЕРШЕНСТВОВАНИЕ БЕСПРОВОДНОЙ ИНФРАСТРУКТУРЫ VANET ДЛЯ АВТОМОБИЛЬНЫХ ДОРОГ

Аббасов Эльшан Магеррам оглы
к.т.н., МАДИ, Москва, Россия, abbapost@yandex.ru

Строганов Владимир Иванович
д.т.н., доцент, МАДИ, Москва, Россия, v.stroganov-madi@mail.ru

Юшкевич Устинья Кирилловна
магистрант, МАДИ, Москва, Россия, uyk567@gmail.com

Аббасова Татьяна Сергеевна
к.т.н., доцент, МГОТУ, Москва, Россия, abbasova_univer@mail.ru

Аннотация
Исследованы характеристики беспроводной автомобильной сети Vanet и построенная на ее основе система имитационного моделирования пропускной способности трафика. Проанализирован метод пропорционального распределения пропускной способности и способы его совершенствования на основе ON/OFF-модели трафика с целью использования в беспроводных автомобильных сетях. Усовершенствована и расширена ON/OFF-модель трафика, которая используется на входе в критический участок.

Ключевые слова: *беспроводные автомобильные сети, пропускная способность, ON/OFF модель трафика, прогноз интенсивности*.

Введение

Современные средства беспроводной мобильной связи [1-5], передачи широковещательных данных [6-19] и определения координат движущихся объектов [20-22] играют существенную роль в большинстве отраслей. Для эффективного применения инноваций в различных отраслях используются информационные системы [23-26]. Большое значение при эксплуатации автомобильного транспорта имеет организация беспроводной мобильной связи между автотранспортными средствами. Для этой цели предназначены автомобильные сети VANET, которые базируются на беспроводных технологиях и предназначены для обмена данными [27]. Так как VANET должны являться саморегулирующимися сетями, для которых характерны фрактальные процессы, необходима разработка моделей управления трафиком для таких сетей [28,29]. Одной из самых популярных моделей телекоммуникационного трафика с выраженными фрактальными свойствами является ON/OFF-модель [30]. Традиционная ON/OFF-модель формирует процесс, который может принимать два состояния: 0 или 1. Основными недостатками такой модели является то, что не учитывается, что в периоды активности каждого отдельного источника трафика передача пакетов осуществляется группами, также при этом не учитываются особенности беспроводных сетей. Таким образом, задача совершенствования данной модели для беспроводных сетей VANET, является актуальной.

Результаты исследования

Для разработки метода перераспределения пропускной способности критической участка беспроводной сети передачи данных необходимо разработать метод прогнозирования изменения интенсивности трафика и метод перераспределения пропускной способности. При работе сети в нормальном режиме служебный трафик занимает 5-10% общей пропускной способности, а при динамическом изменении топологии сети, при образовании в беспроводной сети передачи данных сегментов, которые являются критическими участками, служебный трафик может занимать 80 и более процентов общей пропускной способности на данном участке (рис. 1, 2) [30].

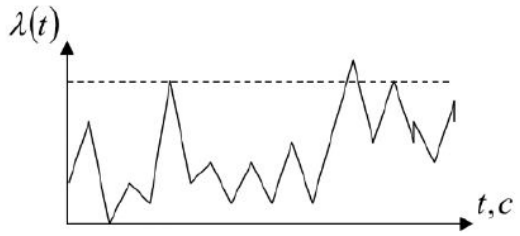


Рис. 1. Иллюстрация принципа динамического изменения пропускной способности на основе прогнозирования интенсивности трафика, статическое задание пропускной способности

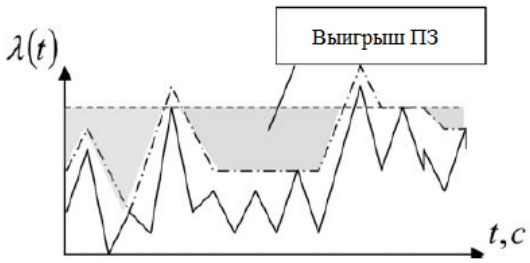


Рис. 2. Иллюстрация принципа динамического изменения пропускной способности на основе прогнозирования интенсивности трафика, динамическое задание пропускной способности

Это приводит к снижению скорости передачи пакетов информационного трафика, их потерям, а, следовательно, и к увеличению времени передачи данных. Возникает необходимость перераспределения пропускной способности на критическом участке между потоками служебного и информационного трафика таким образом, чтобы обеспечить и передачу пакетов информационного трафика, и работу сети в условиях изменения ее структуры и состава. Поиск доступного размера полосы пропускания для каждого соединения осуществляется с помощью методов, основанных на обратной связи между источником и потребителем. Протоколы с помощью алгоритмов, основанных на этих методах, определяют точку распределения на основе отвержения пакетов при превышении потоком доступной пропускной способности.

Для уменьшения времени передачи данных и установки максимального размера плавающего окна, при проявлении трафиком свойств фрактальности, возможно использование прогнозирования на основе предложенной ON/OFF модели [30].

Предложенный метод предполагает определение точки распределения на основе прогнозирования значений интенсивности на основе прогнозирования суммарного информационного трафика с помощью разработанной ON / OFF-модели. Это позволяет определить максимальные значения интенсивности информационного трафика на интервале прогнозирования. Для этого проводится анализ статистических характеристик входных потоков и их проверка на наличие свойств фрактальности. Если значение показателя Херста указывает на фрактальность трафика (0,75 = <H <1), то проводится прогнозирование с помощью разработанной усовершенствованной ON/OFF-модели трафика на входе критической области. В противном случае, точка распределения определяется по среднему значению

служебного трафика и информационного трафика или используются существующие методы поиска точки распределения [30].

Выводы

Предложен метод перераспределения пропускной способности на основе усовершенствованной расширенной ON/OFF-модели трафика на входе в критический участок автомобильной сети Vanet. Метод отличается от существующих тем, что точка распределения между служебным и информационным трафиком обеспечивает пропорциональное распределение пропускной способности, и это позволяет уменьшить количество итераций поиска точки деления на основе потери пакетов и обеспечить увеличение доли пропускной способности, предоставляемой для передачи информационного трафика автотранспортным средствам.

Литература

1. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Технологии в системах радиосвязи на пути к 5G // Москва, 2018.
2. *Харкевич А.А.* Теория информации. Опознание образов // Избранные труды в трех томах / Москва, 1973. Том 3
3. *Харкевич А.А.* Теория электроакустических преобразователей. Волновые процессы // Избранные труды в трех томах / Москва, 1973. Том 1
4. *Бакулин М.Г., Крейнделин В.Б., Шлома А.М., Шумов А.П.* Технология OFDM // Москва, 2016.
5. *Дымкова С.С.* Облачные IOT платформы и приложения для оптимизационного управления транспортом // REDS: Телекоммуникационные устройства и системы. 2020. Т. 10. № 4. С. 39-50.
6. *Варламов О.В., Варламов В.О., Долгопятова А.В.* Международная сеть DRM вещания для создания информационного поля в Арктике // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 9. С. 9-16.
7. *Варламов О.В., Нгуен Д.К., Грычкин С.Е.* Комбинирование синтетических методов высокоэффективного высокочастотного усиления // T-Comm: Телекоммуникации и транспорт. 2021. Т. 15. № 9. С. 11-16.
8. *Варламов О.В.* Максимальная мощность коммутируемого p-i-n диодами антенно-согласующего устройства диапазона ВЧ при рассогласовании нагрузки // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 10. С. 26-32.
9. *Filimonov N., Varlamov O., Itkin G.* Efficient modulation of RF signals // Патент на изобретение US 7724837 B2. Заявка № US20040546012 от 07.01.2004.
10. *Варламов О.В., Лаврушенков В.Г.* Критерии качества передающего устройства для стандарта DRM и измерительное оборудование // Broadcasting. Телевидение и радиовещание. 2004. № 3. С. 44-48.
11. *Варламов О.В.* Разработка требований к приемному оборудованию сетей цифрового радиовещания стандарта DRM // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 9. С. 39-42.
12. *Варламов О.В., Громорушкин В.Н., Лаврушенков В.Г., Чугунов И.В.* Генератор испытательных сигналов для измерительных характеристик ключевых усилителей мощности с раздельным усилением составляющих однополосного сигнала // T-Comm: Телекоммуникации и транспорт. 2011. Т. 5. № 9. С. 47-49.
13. *Gromorushkin V.N., Varlamov O.V., Dolgopyatova A.V., Voronkov A.A.* Operation problems of the EER transmitter with narrowband antenna // В сборнике: 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019. 2019. С. 8706736.
14. *Varlamov O.V.* Organization of single frequency DRM digital radio broadcasting networks. Features and results of practical tests // В сборнике: 2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2018. 2018. С. 8456925.
15. *Varlamov O.V., Gromorushkin V.N.* Class D switching power amplifier with a filter under load mismatch conditions // В сборнике: 2020 Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2020. 2020. С. 9131508.

16. *Varlamov O.V., Nguyen D.C., Grychkin S.E.* Simultaneous application of several synthetic methods for high efficiency radiofrequency amplification // В сборнике: 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings. 2021. С. 9416126.
17. *Варламов О.В.* Организация одночастотных сетей цифрового радиовещания стандарта DRM. Особенности и результаты практических испытаний // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 11. С. 4-20.
18. *Varlamov O.V.* Experimental study of a synchronous DVB-T2 network in the yaroslavl region. Problems with some manufacturers' receivers // В сборнике: 2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 - Proceedings. 2020. С. 9261562.
19. *Варламов О.В., Варламов В.О.* Распределение максимальных уровней атмосферных радиошумов в диапазонах низких частот и средних частот по территории Земли // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 5. С. 42-51.
20. *Dymkova S.* Applicability of 5G subscriber equipment and global navigation satellite systems // Synchroinfo Journal. 2021. Т. 7. № 5. С. 36-48.
21. *Dymkova S.S., Dymkov A.D.* Experimental studies of GNSS errors in rough and wooded mountainous terrain // В сборнике: 2021 International Conference on Engineering Management of Communication and Technology, EMCTECH 2021 - Proceedings. 2021. С. 9
22. *Dymkova S.S., Dymkov A.D.* Multifactorial methodology of cycling routes time calculation based on 3D maps // В сборнике: 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings. 2021. С. 9416046.
23. *Дымкова С.С.* Повышение эффективности функционирования информационных систем и процессов в высшей школе // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2017. Т. 6. № 2. С. 45-48.
24. *Дымкова С.С.* Новые принципы организации функционирования систем по продвижению результатов научных исследований // Системы синхронизации, формирования и обработки сигналов. 2017. Т. 8. № 1. С. 34-37.
25. *Дымкова С.С.* Разработка информационной системы для продвижения результатов научных исследований // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 7. С. 38-41.
26. *Артюшенко В.М., Аббасова Т.С., Стреналюк Ю.В., Васильев Н.А., Белюченко И.М., Самаров К.Л., Зиновьев В.Н., Посеренин С.П., Вокин Г.Г., Мороз А.П., Шайдуров В.С., Шаврин С.С.* Системный анализ в области управления и обработки информации // Монография / Королев, 2015.
27. *Шилин П.А.* Персональная цифровая мобильная радиосвязь посредством Vanet // Информационные технологии и телекоммуникации. 2014. Т. 2. № 3. С. 84-96.
28. *Клименко И.С.* Обзор беспроводных транспортных сетей Vanet // Современные инновации. 2018. № 5 (27). С. 16-20.
29. *Пугачев И.Н., Каменчуков А.В., Щеглов В.И., Смирнова Н.Д.* Технические, экономические и социальные аспекты, при выборе эффективного решения совершенствования дорожного движения в городах // Транспортные сооружения. 2020. Т. 7. № 2. С. 21.
30. *Кутузов О.И., Татарникова Т.М.* К оцениванию и сопоставлению очередей классических и фрактальных систем массового обслуживания // Информационно-управляющие системы. 2016. № 2 (81). С. 48-55.

О СВЯЗИ ДАТАСЕТА CSE-CIC-IDS2018 С МАТРИЦЕЙ MITRE ATT&CK

Борисенко Борис Борисович
Московский технический университет связи и информатики, ведущий научный сотрудник, к.т.н., доцент, Москва, Россия
fepem@yandex.ru

Ерохин Сергей Дмитриевич
Московский технический университет связи и информатики, ректор, к.т.н., доцент, Москва, Россия
esd@mtuci.ru

Фадеев Александр Сергеевич
Московский технический университет связи и информатики, младший научный сотрудник, Москва, Россия
aleksandr-sml@mail.ru

Мартишин Иван Дмитриевич
Московский технический университет связи и информатики, младший научный сотрудник, Москва, Россия
martishinid@gmail.com

Аннотация
В статье представлен обзор основных тактик развития сетевых атак согласно матрице MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge). MITRE ATT&CK объединяет в себе четыре группы матриц: PRE-ATT&CK, Enterprise, Mobile и ATT&CK for ICS (Industrial Control Systems). Матрица постоянно обновляется и на момент проведения анализа включает в себя 191 технику и 386 подтехник атак для ОС Windows, Linux и Mac OS. Структура матрицы MITRE ATT&CK состоит из 14 тактик: от первоначального доступа до взятия под контроль и кражи данных. В работе проведен краткий обзор существующих классов сетевых атак, представлена их классификация. Рассмотрены характеристики и особенности современных датасетов, используемых при настройке систем обнаружения вторжений (СОВ). Сопоставлены классы атак системы обнаружения вторжений, реализованной на базе датасета CSE-CIC-IDS2018 и тактик развития сетевых атак MITRE ATT&CK.

Ключевые слова
Системы обнаружения вторжений (СОВ, IDS); сетевые атаки; матрица MITRE ATT&CK; набор данных (датасет); CSE-CIC-IDS2018; модель взаимодействия открытых систем (модель ISO/OSI)

Введение

В современном мире при проведении военных кампаний противоборствующие стороны наносят удары по инфраструктуре не только с помощью военных ударов, но и с использованием сетевых атак.

С начала проведения специальной военной операции сетевым атакам подверглись российские госучреждения, СМИ, а также объекты критической информационной инфраструктуры и системы жизнеобеспечения [1]. В связи с этим резко возрастает роль СОВ.

В данной работе проводится анализ различных тактик проведения атак согласно матрице MITRE ATT&CK, по которым можно идентифицировать класс сетевой атаки, в частности, применительно к датасету CSE-CIC-IDS2018.

Основные тактики развития сетевой атаки по матрице MITRE ATT&CK

MITRE ATT&CK – основанная на реальных наблюдениях база знаний компании MITRE, содержащая описание тактик, приемов и методов, используемых киберпреступниками [2]. Данная база знаний может быть использована в качестве основы для разработки конкретных моделей угроз и других типов методологий и инструментов.

Информация в базе MITRE ATT&CK представлена в виде матриц. Каждая матрица представляет собой таблицу, в которой заголовки столбцов соответствуют тактикам киберпреступников, а содержимое ячеек – методикам реализации тактик или техникам. По матрице ATT&CK можно понять, какие тактики, техники и процедуры могут быть задействованы злоумышленником, и в дальнейшем противопоставить меры защиты.

Матрицы MITRE ATT&CK объединены в четыре группы:

– PRE-ATT&CK – тактики и техники, которые злоумышленники используют на этапе подготовки к кибератаке;

– Enterprise – тактики, техники и процедуры, которые злоумышленники применяют в ходе атаки на организации-жертвы. В этой группе доступна как сводная матрица, так и отдельные матрицы, содержащие тактики и техники кибератак на конкретные операционные системы и облачные сервисы;

– Mobile – тактики, техники и процедуры, которые злоумышленники используют в ходе атаки на мобильные устройства под управлением ОС iOS и Android;

– ATT&CK for ICS (Industrial Control Systems) – тактики, техники и процедуры, которые используются в атаках на промышленные системы управления.

На текущий момент Enterprise ATT&CK включает 191 технику и 386 подтехник атак для ОС Windows, Linux и Mac OS (последние изменения от 1 апреля 2022 года). Структура матрицы состоит из 14 тактик: от первоначального доступа до взятия под контроль и кражи данных. Каждая фаза жизненного цикла атаки состоит из множества техник, которые успешно используются различными группами киберпреступников при компрометации сети организации.

Тактика – детальное описание действий злоумышленника на разных этапах атаки, цели или задачи злоумышленника на определенном шаге. Техника – описание, каким образом злоумышленник достигает цели или решает поставленную задачу, какие использует инструменты, технологии, код, эксплойты, утилиты. Подтехника – более конкретное описание поведения злоумышленника при достижении цели. Описывает поведение на более низком уровне, чем техника. Например, злоумышленник может сбросить учетные данные, получив доступ к закрытым данным локального центра безопасности (Local Security Authority, LSA). Процедура – конкретная реализация, которую противник использует для техник или подтехник. Например, процедурой может быть использование злоумышленником PowerShell для внедрения в lsass.exe с целью сброса учетных данных путем сканирования памяти целевой системы.

Рассмотрим основные тактики атак согласно матрице MITRE ATT&CK [3,4].

Разведка (reconnaissance, TA0043) – тактика, при которой злоумышленник пытается собрать информацию, которую может использовать для планирования будущих действий. Содержит 10 техник и 32 подтехники.

Данная тактика состоит из техник, включающих активный или пассивный сбор злоумышленником информации, которая может быть использована для определения цели. Такая информация может состоять из подробных сведений об организации цели, инфраструктуре или персонале. Эти данные могут помочь злоумышленнику на других этапах, например, для использования собранной информации при планировании и осуществлении первоначального доступа, определении масштаба и приоритетности целей после компрометации или управлении и осуществлении дальнейших разведывательных действий.

Подготовка ресурсов (resource development, TA0042) – тактика, при которой злоумышленник пытается найти ресурсы, которые может использовать для поддержки своих действий. Содержит 7 техник и 31 подтехнику.

Разработка ресурсов состоит из техник, включающих создание, покупку или компрометацию/кражу ресурсов, которые злоумышленник может использовать для достижения целей. Такие ре-

сурсы включают инфраструктуру, учетные записи или возможности проникновения. Могут быть использованы злоумышленником в дальнейшем, например, использование полученных доменов для поддержки управления, учетных записей электронной почты – для фишинга в рамках первоначального доступа, или кража сертификатов цифровой подписи – для уклонения от защиты.

Первоначальный доступ (initial access, TA0001) – тактика, при которой злоумышленник пытается проникнуть в сеть. Содержит 9 техник и 10 подтехник.

Данная тактика представляет собой техники, используемые злоумышленниками для закрепления в корпоративной системе. Например, целевой фишинг с вложением (spearphishing attachment), кража учетных данных пользователя с помощью действительных учетных записей, использование скомпрометированных съемных носителей [5].

Выполнение (execution, TA0002) – тактика, при которой злоумышленник пытается запустить вредоносный код. Содержит 12 техник и 21 подтехнику.

После получения первоначального доступа к локальному или удаленному компьютеру злоумышленник может напрямую выполнить вредоносный код с помощью таких техник, как взаимодействие через интерфейс командной строки или графический интерфейс пользователя, либо дождаться выполнения пользователем для эксплуатации уязвимости. Для достижения таких целей, как исследование сети или кража данных, техники представленной тактики часто сочетаются с техниками других тактик. Например, злоумышленник может использовать удаленный доступ для запуска сценария PowerShell, выполняющего обнаружение удаленной системы.

Закрепление (persistence, TA0003) – тактика, при которой злоумышленник пытается сохранить доступ к системам-жертвам. Содержит 19 техник и 89 подтехник.

Первоначальный доступ к системе, полученный злоумышленником, может быть ликвидирован при смене пользователями паролей. Для сохранения доступа злоумышленник может взломать легитимный код в системе жертвы с целью дальнейшего продвижения в системе.

Повышение привилегий (privilege escalation, TA0004) – тактика, при которой злоумышленник пытается получить права более высокого уровня. Содержит 13 техник и 82 подтехники.

Злоумышленники часто проникают в корпоративную систему с непривилегированным доступом, при этом могут получить больше ресурсов в целевой системе, повысив свои полномочия. В частности, возможно получение повышенных привилегий с использованием уязвимостей в приложениях и серверах в рамках целевой системы. Общие подходы заключаются в использовании слабых мест системы, неправильной конфигурации и уязвимостей. Техники повышения доступа осуществляются на основе данных:

– корневого уровня (системы);

– администратора;

– учетной записи пользователя с правами администратора;

– учетных записей пользователей с доступом к определенной системе или выполнению определенных функций.

Данные методы часто пересекаются с техниками тактики закрепления, поскольку функции ОС, позволяющие злоумышленнику сохранять доступ, могут выполняться в контексте с повышенными правами.

Предотвращение обнаружения (defense evasion, TA0005) – тактика, при которой злоумышленник пытается избежать обнаружения. Содержит 42 техники и 128 подтехник.

Во избежание обнаружения и с целью обхода средств управления безопасностью, злоумышленники часто удаляют или скрывают свои следы для продолжения вредоносной деятельности.

Получение учетных данных (credential access, TA0006) – тактика, при которой злоумышленник пытается скомпрометировать имена и пароли учетных записей. Содержит 16 техник и 42 подтехники.

Использование учетных записей может дать злоумышленнику доступ к системе и затруднить его обнаружение.

Исследование (discovery, TA0007) – тактика, при которой злоумышленник пытается выяснить окружение целевой системы. Содержит 30 техник и 13 подтехник.

Получив доступ к корпоративной системе, злоумышленник может попытаться исследовать и собрать больше информации о системе для достижения своих целей. Такие попытки включают обна-

ружение возможных уязвимостей для эксплуатации, данных, хранящихся в системе, и сетевых ресурсов с помощью сканирования сетевых служб.

Перемещение внутри периметра (lateral movement, TA0008) – тактика, при которой злоумышленник пытается проникнуть в окружение системы. Содержит 9 техник и 12 подтехник.

После компрометации одного элемента корпоративной сети злоумышленник может перейти от скомпрометированной учетной записи пользователя к учетным записям других пользователей в пределах корпоративной зоны с помощью таких методов, как внутренний целевой фишинг, позволяющий использовать доверенные внутренние учетные записи.

Сбор данных (collection, TA0009) – тактика, при которой злоумышленник пытается собрать данные, представляющие интерес. Содержит 17 техник и 20 подтехник.

Данные могут быть собраны со взломанного компьютера или его периферийных устройств (например, веб-камеры или USB-накопителя). Следующим шагом может быть эксфильтрация данных (exfiltration). Основные методы сбора данных включают снимки экрана и ввод с клавиатуры.

Управление и контроль (command and control, TA0011) – тактика, при которой злоумышленник пытается связаться со скомпрометированными системами для последующего контроля. Содержит 16 техник и 22 подтехник.

Данная тактика позволяет злоумышленнику удаленно контролировать операции в целевой системе. Обычно злоумышленники пытаются имитировать обычный ожидаемый трафик во избежание обнаружения.

Эксфильтрация данных (exfiltration, TA0010) – тактика, при которой злоумышленник пытается скопировать данные. Содержит 9 техник и 8 подтехник.

Техники получения данных из целевой сети обычно включают их передачу по каналу управления и контроля или альтернативному каналу, также могут включать ограничение размера передачи.

Воздействие (impact, TA0040) – тактика, при которой злоумышленник пытается манипулировать или уничтожить данные или реализовать отказ в обслуживании системы. Содержит 13 техник и 13 подтехник.

Речь идет о нарушении конфиденциальности, целостности или доступности данных в системе, например, нарушение структуры диска или удаление содержимого диска.

Существующие классы сетевых атак

Сетевая атака – это целенаправленная деятельность злоумышленника (атакующей стороны), направленная на объекты критической инфраструктуры с целью нанесения вреда, раскрытия, изменения, уничтожения, воровства или получения доступа к ресурсам сетевой системы [6].

Сетевые атаки можно разделить на два класса: пассивные и активные. К пассивным относятся такие, как: анализ трафика, прослушивание, определение расположения данных и др. [7]. Среди активных атак различают следующие: отказ в обслуживании (DoS-атака), создание ложного потока (фальсификация), атака повторного использования (replay-атака), модификация потока данных (атака «man in the middle») и др. [8]. В [9] к вышеуказанным относят: спуфинг, DNS sinkhole, атаку Сибиллы (Sybil attack).

Сетевые атаки также можно классифицировать исходя из действий и целей злоумышленника (нарушение функционирования, конфиденциальности, целостности), по наличию обратной связи с сетью (однонаправленная атака, атака с обратной связью), по условию начала атаки (по запросу от объекта, по выполнению определенного действия на стороне объекта, безусловные атаки), по расположению субъекта по отношению к объекту атаки (межсегментного типа, внутрисегментного типа), по уровню эталонной модели OSI.

Классификация возможностей реализации сетевых атак представляет собой совокупность возможных вариантов действий источника угроз определенными методами с использованием уязвимостей, которые приводят к реализации целей атаки [8].

В [10] используется классификация сетевых атак по назначению (отказ в обслуживании, разведка, получение доступа), ее правовой форме (кибершпионаж, кибертерроризм, киберпреступление, кибервойна), в зависимости от степени воздействия (активная, пассивная), охвата (вредоносные крупномасштабные, малый масштаб без вредоносного воздействия), вида сети.

Классификация, реализованная во многих системах обнаружения вторжений, не является исчерпывающей. Поскольку сетевые объекты различны и, например, атаки, реализуемые на компьютерах под управлением ОС Windows, могут быть бесполезны для машин с ОС семейства UNIX. Кроме того, имеет место неоднозначность и в самих названиях атак и уязвимостей. Одна и та же атака может иметь совершенно различные наименования. Для устранения разногласий и для принятия общих стандартов в названиях уязвимостей и атак в 1999 году компания MITRE Corporation выработала решение, реализованное в виде базы данных CVE (Common Vulnerabilities and Exposures).

В популярных датасетах наиболее распространенными классами атак являются [11]: атаки типа «отказ в обслуживании» (DoS), распределенные DoS-атаки (DDoS), User-to-Root (U2R), Remote-to-Local (R2L), Probe атаки, подбор по словарю, атаки-инъекции (Injection).

Особенности, которые нужно учитывать при разработке СОВ:

1. Атака одного типа может быть началом атаки другого типа. В этом случае характеристики атаки будут представлять собой комбинацию характеристик обеих атак.

2. Изменения с течением времени некоторых характеристик атак. Например, DDoS-атаки в основном понимаются как атаки с большим количеством пакетов, которые переполняют пропускную способность сети; однако DDoS-атаки на уровне приложений – это атаки не с таким существенным объемом, которые переполняют сервер, а не сеть.

3. Сходство характеристик некоторых типов атак. Например, DoS- и Probe-атаки в большинстве случаев имеют последовательный характер и включают большое количество соединений с одним и тем же узлом, в то время как атаки R2L и U2R производятся через пакеты. Поэтому отличить их внутри класса не так просто. Для повышения эффективности классификации типов атак в ряде исследований изучалось, какие признаки эффективны для обнаружения конкретных типов атак.

Признаки, используемые для обнаружения атак Probe, U2R и R2L, имеют высокую степень сходства, что объясняет, почему эти три типа атак часто неправильно классифицируются между собой [12].

Современные датасеты, используемые при настройке систем обнаружения вторжений

Для обучения СОВ, основанных на применении несигнатурных методов обнаружения, применяются специализированные наборы размеченных данных – датасеты, которые включают данные сетевого трафика, содержащие информацию о хосте, поведении пользователя, конфигурации системы и пр. [13].

Среди наиболее распространенных датасетов можно упомянуть: DARPA 1998, KDD CUP 1999, Kyoto 2006+, NSL-KDD 2009, ISCX2012, CTU-13, UNSW-NB15, CIDDS-001, UGR-16, CIC-IDS2017, CSE-CIC-IDS2018. В качестве основных характеристик датасетов, указанных в таблице 1, используются следующие [14-17]:

а) число признаков в наборе данных. Признаки, характеризующие общую информацию о соединении/потоке (например, время начала соединения, IP-адрес источника атаки; порт источника атаки и т.п.), информативные признаки (например, длительность соединения, число переданных/принятых байт и т.п.), а также признаки, которые используются для описания атаки или нормального сетевого соединения (например, метка класса трафика, описание атаки, реакция антивирусного средства на соединение);

б) природа информативных признаков. В таблице 1 используются следующие обозначения:

– ПСС – признаки, характеризующие сетевое соединение (например, длительность сетевой сессии);

– ПНП – признаки, характеризующие направление передачи данных (например, число байт, переданных в направлении сервера; среднее время между сетевыми пакетами в направлении клиента);

– ППУ – признаки, характеризующие операции, выполняемые на прикладном уровне (например, успех операции удаленной аутентификации пользователя, число операций с файлами в данном соединении и т.п.);

в) типы сетевых атак в наборе данных.

Таблица 1

Описание датасетов

№	Датасет	Количество признаков	Природа информативных признаков	Классы сетевых атак
1	DARPA 1998	10	ПСС	DoS, R2L, U2R, наблюдение/прослушка
2	KDD CUP 1999	42	ПСС, ППУ	DoS, R2L, U2R, наблюдение/прослушка
3	Kyoto 2006+	24	ПСС	Различные атаки на honeypots (backscatter, DoS, эксплойты, вредоносное ПО, сканирование портов, шеллкод)
4	NSL-KDD 2009	42	ПСС, ППУ	DoS, R2L, U2R, наблюдение/прослушка
5	ISCX 2012	19	ПСС, ПНП	Брутфорс SSH, HTTP DoS, DDoS с использованием IRC Botnet
6	CTU-13 (2011)	33	ПСС, ПНП	Ботнеты (Menti, Murlo, Neris, NSIS, Rbot, Sogou, Virut)
7	UNSW-NB15 (2015)	45	ПСС, ПНП, ППУ	Фаззеры, анализ, бэкдоры, DoS, эксплойты, Generic, разведка, шеллкод, черви
8	CIDDS-001	14	ПСС, ПНП	Сканирование портов, DoS, брутфорс, Ping-сканирование
9	UGR-16	13	ПСС, ПНП	DoS, сканирование портов, сканирование UDP-портов, сканирование SSH, ботнет, спам
10	CIC-IDS2017	85	ПСС, ПНП, ППУ	DoS Hulk, сканирование портов, DDoS, DoS GoldenEye, FTP-Patator, SSH-Patator, DoS slowloris, DoS Slowhttptest, бот, проникновение, Heartbleed, веб-атаки – брутфорс, веб-атаки – XSS, веб-атаки – SQL инъекция
11	CSE-CIC-IDS2018 и другие наборы данных, созданные в CIC	80	ПСС, ПНП, ППУ	Брутфорс, Heartbleed, ботнет, DoS, DDoS, веб-атаки

В данной работе исследуется датасет CSE-CIC-IDS2018 [18], как наиболее полный, актуальный и практически применимый. В датасете используется понятие профиля. Профиль представляет собой детальное описание атаки и абстрактное описание модели приложения, протоколов и низкоуровневых сетевых компонент. Выделяется два основных класса профилей.

B-профили (B-profiles, behaviour/benign) включают в себя поведенческие признаки пользователей системы: протокол, количество пакетов в потоке, размер передаваемых данных, время отклика. В ходе исследования анализировались протоколы HTTPS, HTTP, SMTP, POP3, IMAP, SSH и FTP. Наибольшую часть датасета представляет HTTP- и HTTPS-трафик. B-профили описывают только чистый трафик.

M-профили (M-profiles, malware) включают в себя поведенческие признаки сетевых атак. В датасете используется 7 различных сценариев атак [19-22]: Brute-force атаки, Heartbleed-атаки, DoS-атака, DDoS-атаки, атаки на web-приложение, ботнет, проникновение в сеть изнутри. Всего же в датасете 14 видов атак (табл. 2). На трафик одной атаки приходится один M-профиль. В наборе M-профили распределены по определенным IP-адресам. M-профили могут работать параллельно с B-профилями и их может быть несколько. При этом, трафики разных видов профилей не пересекаются по набору IP-адресов, поэтому не возникает проблем при самостоятельной разметке набора по расписанию.

Таблица 2

Сопоставление атак датасета CSE-CIC-IDS2018 и матрицы MITRE ATT&CK

№	Название атаки датасета	Тактика	Техника	Подтехника	Процедура
1	FTP-BruteForce	Credential Access (Получение учетных данных) TA0006	Brute Force (Перебор) T1110	Password Guessing (Подбор пароля) T1110.001	FTP Patator
2	SSH-Bruteforce	Credential Access (Получение учетных данных) TA0006	Brute Force (Перебор) T1110	Password Guessing (Подбор пароля) T1110.001	SSH Patator
3	DoS-GoldenEye	Impact (Воздействие) TA0040	Endpoint Denial of Service (Отказ в обслуживании конечной точки) T1499	Service Exhaustion Flood (Флуд сервиса) T1499.002	GoldenEye
4	DoS-Slowloris	Impact (Воздействие) TA0040	Endpoint Denial of Service (Отказ в обслуживании конечной точки) T1499	Service Exhaustion Flood (Флуд сервиса) T1499.002	Slowloris
5	DoS-SlowHTTPTest	Impact (Воздействие) TA0040	Endpoint Denial of Service (Отказ в обслуживании конечной точки) T1499	Service Exhaustion Flood (Флуд сервиса) T1499.002	Slowhttptest
6	DoS-Hulk	Impact (Воздействие) TA0040	Endpoint Denial of Service (Отказ в обслуживании конечной точки) T1499	Service Exhaustion Flood (Флуд сервиса) T1499.002	Hulk
7	DDoS attacks-LOIC-HTTP	Impact (Воздействие) TA0040	Endpoint Denial of Service (Отказ в обслуживании конечной точки) T1499	Service Exhaustion Flood (Флуд сервиса) T1499.002	LOIC
8	DDoS-LOIC-UDP	Impact (Воздействие) TA0040	Endpoint Denial of Service (Отказ в обслуживании конечной точки) T1499	Service Exhaustion Flood (Флуд сервиса) T1499.002	LOIC
9	DDOS-HOIC	Impact (Воздействие) TA0040	Endpoint Denial of Service (Отказ в обслуживании конечной точки) T1499	Service Exhaustion Flood (Флуд сервиса) T1499.002	HOIC
10	Brute Force-Web	Credential Access (Получение учетных данных) TA0006	Brute Force (Перебор) T1110	Password Guessing (Подбор пароля) T1110.001	DVWA, Selenium Framework
11	Brute Force-XSS	Initial Access (Первоначальный доступ) TA0001	Drive-by Compromise (Путевая компрометация) T1189	–	DVWA, Selenium Framework
12	SQL Injection	Initial Access (Первоначальный доступ) TA0001	Exploit Public-Facing Application (Использование публичного приложения) T1190	–	DVWA, sqlmap
13	Infiltration	Execution (Выполнение) TA0002	User Execution (Выполнение пользователем) T1204	Malicious File (Вредоносный файл) T1204.002	Dropbox, Adobe Acrobat Reader 9
		Discovery (Исследование) TA0007	Network Service Scanning (Сканирование сервисов сети) T1046	–	Nmap, portscan
14	Bot	Resource Development (Освоение ресурсов) TA0042	Acquire Infrastructure (Получение инфраструктуры) T1583	Botnet (Ботнет) T1583.005	Ares, Zeus
		Collection (Сбор данных) TA0009	Screen Capture (Скриншот) T1113	–	screenshots

Датасет CSE-CIC-IDS2018 имеет ряд ограничений, связанных с выбором данных и файлов, созданных в результате анализа сетевых потоков:

– данные, полученные в результате анализа сетевого потока, хранятся в файлах, и обработка этих файлов является достаточно трудоемкой задачей (большое количество экземпляров данных в каждом файле);

– файлы в датасете можно объединить для включения в них всех меток атак с целью обработки. Однако объединение экземпляров каждого типа атак увеличивает размер датасета, что приводит к увеличению времени вычислений и обработки;

– датасет состоит из некоторых отсутствующих и избыточных записей данных;

– датасет подвержен проблеме дисбаланса классов, что может привести к низкой точности и высокой доле ложноположительных классификаций.

Эти недостатки могут быть устранены путем предварительной обработки данных, генерации, устранения отсутствующих или избыточных записей [23-25].

Сопоставление атак датасета CSE-CIC-IDS2018 и тактик развития сетевой атаки матрицы MITRE ATT&CK

На основе имеющихся данных трафика датасета CSE-CIC-IDS2018 выделим основные типы атак [26]. Самым распространенным классом атак является DoS-атаки. В силу нацеленности на недоступность для нормального использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения, данный класс следует отнести к тактике TA0040. Применением BruteForce злоумышленник получает доступ к учетным записям сети, таким образом, данный класс реализуется тактикой TA0006. Следующий класс основан на внедрении в выполняемом приложении запроса к базе данных произвольного SQL-кода, переданного злоумышленником с использованием тактики получения первоначального доступа TA0001. Атаки, направленные на проникновение в сеть изнутри (Infiltration), состоят из двух этапов: передачи вредоносного кода и последующего исследования внутренней сети (TA0002 и TA0007).

В таблице 2 представлены атаки из набора данных CSE-CIC-IDS2018 с учетом их соответствия тактикам, техникам и подтехникам матрицы MITRE ATT&CK.

Заключение

В работе проведен обзор основных тактик развития матрицы MITRE ATT&CK, содержащей данные о техниках и методах, примененных при успешно проведенных атаках. Рассмотрены классы сетевых атак и современные датасеты, используемые в рамках СОВ. В результате анализа современных датасетов было выявлено, что наиболее распространенными и применимыми являются следующие классы атак: атаки типа «отказ в обслуживании» (DoS), распределенные DoS-атаки (DDoS), User-to-Root (U2R), Remote-to-Local (R2L), Probe атаки, подбор по словарю, атаки-инъекции (Injection).

При построении СОВ необходимо учитывать:

1) атака одного типа может быть началом атаки другого типа;

2) с течением времени изменяются характеристики атак;

3) характеристики некоторых типов атак подобны.

В работе использован датасет CSE-CIC-IDS2018. Он имеет ряд ограничений, которые устраняются путем предварительной обработки данных, генерации, устранения отсутствующих или избыточных записей. В ходе исследования MITRE ATT&CK было выявлено, что одни и те же техники могут использоваться для разных тактик, несмотря на различные способы применения. Проведено сопоставление классов атак СОВ, реализованной на базе датасета CSE-CIC-IDS2018 с тактиками развития сетевой атаки по матрице MITRE ATT&CK, которое помогает понять, какие тактики, техники, подтехники и процедуры задействует и реализует злоумышленник.

Литература

1. В МИД РФ заявили о сотнях тысяч еженедельных хакерских атак на Россию. Интернет портал газеты Известия. URL: https://iz.ru/1320675/2022-04-14/v-mid-rf-zaiavili-o-sotniakh-tysiach-ezhenedelnykh-khakerskikh-atak-na-rossiiu (дата обращения: 19.04.2022).

2. Mitre Att&ck. ИТ-энциклопедия «Касперского», URL: https://encyclopedia.kaspersky.ru/glossary/mitre-attack/ (дата обращения: 20.02.2022).

3. Mitre Att&ck, URL: https://attack.mitre.org/ (дата обращения: 04.05.2022).

4. Матрица Mitre Att&ck Positive Technologies, URL: https://mitre.ptsecurity.com/ru-RU/techniques?utm_source=seclab&utm_medium=news (дата обращения: 04.05.2022).

5. *Xiong W., Legrand E., Åberg O.* et al. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. Softw Syst Model, 2021, URL: https://doi.org/10.1007/s10270-021-00898-7 (дата обращения: 25.02.2022).

6. *Aljabri M., Aljameel S.S., Mohammad R.M.A., Almotiri S.H., Mirza S., Anis F.M., Aboulnour M., Alomari D.M., Alhamed D.H., Altamimi H.S.* Intelligent Techniques for Detecting Network Attacks: Review and Research Directions. Sensors 2021, 21, 7070, URL: https://doi.org/10.3390/s21217070 (дата обращения: 30.03.2022).

7. *Inayat Z., Gani A., Anuar N.B., Anwar S., Khan M.K*. Cloud-Based Intrusion Detection and Response System: Open Research Issues, and Solutions. Arab. J. Sci. Eng. 2017, 7, pp. 1-25.

8. *Ажмухамедов И.М*. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования: монография, Астрахань, 2012, 344 с.

9. *Pawar M.V., Anuradha J*. Network Security and Types of Attacks in Network, Procedia Computer Science, 48, 2015, pp. 503-506.

10. *Uma M., Ganapathi P*. A survey on various cyber attacks and their classification, International Journal of Network Security, 15, 2013, pp. 390-396.

11. *Gümüşbaş D., Yıldırım T., Genovese A., Scotti F.* A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems, in IEEE Systems Journal, vol. 15, no. 2, 2021, pp. 1717-1731, URL: https://doi.org/10.1109/JSYST.2020.2992966 (дата обращения: 27.01.2022).

12. *Mishra P., Varadharajan V., Tupakula U., Pilli E. S.* A detailed investigation and analysis of using machine learning techniques for intrusion detection, IEEE Commun. Surveys Tuts., vol. 21, no. 1, 2019, pp. 686–728.

13. *Koch R*. Towards Next-Generation Intrusion Detection. 2011 3rd International Conference on Cyber Conflict, pp. 151-168.

14. *Thakkar A., Lohiya R.* A Review of the Advancement in Intrusion Detection Datasets, Procedia Computer Science, Volume 167, 2020, Pages 636-645, ISSN 1877-0509, URL: https://doi.org/10.1016/j.procs.2020.03.330 (дата обращения: 17.01.2022).

15. *Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А*. Методика сбора обучающего набора данных для модели обнаружения компьютерных атак // Труды ИСП РАН. Т. 33, вып. 5, 2021. С. 83-104, URL: https://doi.org/10.15514/ISPRAS-2021-33(5)-5 (дата обращения: 17.01.2022).

16. *Sharafaldin I., Gharib A., Lashkari A.H., Ghorbani A.A*. Towards a reliable intrusion detection benchmark dataset. Software Networking, 2018(1), pp. 177–200, URL: https://doi.org/10.13052/jsn2445-9739.2017.009 (дата обращения: 17.01.2022).

17. *Ерохин С.Д., Журавлев А.П.* Сравнительный анализ открытых наборов данных для использования технологий искусственного интеллекта при решении задач информационной безопасности // Системы синхронизации, формирования и обработки сигналов, т. 11, № 3, 2020, с. 12-19.

18. CSE-CIC-IDS2018 on AWS. A collaborative project between the Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC), URL: https://www.unb.ca/cic/datasets/ids-2018.html (дата обращения: 17.03.2022).

19. *Ravikumar D*. Towards Enhancement of Machine Learning Techniques Using CSE-CIC-IDS2018 Cybersecurity Dataset, 2021, Thesis, Rochester Institute of Technology.

20. *Volkov S., Kurochkin I.* Network attacks classification using Long Short-term memory based neural net-works in Software-Defined Networks // 9th International Young Scientist Conference on Computational Science (YSC 2020), Procedia Computer Science, 178, 2020, pp.394-403, URL: https://doi.org/10.1016/j.procs.2020.11.041 (дата обращения: 18.03.2022).

21. *Borisenko B.B., Erokhin S.D., Fadeev A.S., Martishin I.D.* Intrusion detection using multilayer perceptron and neural networks with long short-term memory // Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021 - Conference Proceedings, Svetlogorsk, Kaliningrad Region, 2021, URL: https://doi.org/10.1109/SYNCHROINFO51390.2021.9488416 (дата обращения: 18.03.2022).

22. *Erokhina O.V., Borisenko B.B., Martishin I.D., Fadeev A.S.* Analysis of the multilayer perceptron parameters impact on the quality of network attacks identification // Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021 - Conference Proceedings, Svetlogorsk, Kaliningrad Region, 2021, URL: https://doi.org/10.1109/SYNCHROINFO51390.2021.9488344 (дата обращения: 18.03.2022).

23. *Li J., Cheng K., Wang S., Morstatter F., Trevino R.P., Tang J., Liu H.* Feature selection: a data perspective // ACM Computing Surveys, 2017, vol. 50, no. 6, article 94, 45 p., URL: https://doi.org/10.1145/3136625 (дата обращения: 18.03.2022).

24. *Erokhin S., Borisenko B., Fadeev A*. Reducing the dimension of input data for ids by using match analysis // 28th Conference of Open Innovations Association (FRUCT), Moscow, Russia, 2021, pp. 96-102, URL: https://doi.org/10.23919/FRUCT50888.2021.9347629 (дата обращения: 18.03.2022)

25. *Ерохин С.Д., Борисенко Б.Б., Мартишин И.Д., Фадеев А.С*. Анализ существующих методов снижения размерности входных данных // T-Comm: Телекоммуникации и транспорт. Т.16, №1, 2022. С. 30-37.

26. *Ерохин С.Д., Борисенко Б.Б., Фадеев А.С., Мартишин И.Д*. О разработке датасета для обнаружения сетевых атак // REDS: Телекоммуникационные устройства и системы. Т.12, №1, 2022. С. 18-25.

ВЛИЯНИЕ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ НА РАБОТУ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНОГО МОДУЛЯ

Бирюкова Ольга Витальевна
ФГБОУ ВО «Национальный исследовательский университет «МЭИ», старший преподаватель, Москва, Россия
BiriukovaOV@mpei.ru

Корецкая Ирина Валерьевна
ФГБОУ ВО «Национальный исследовательский университет «МЭИ», старший преподаватель, Москва, Россия
KoretskyaIV@mpei.ru

Аннотация
Работа посвящена оптимизации системы сбора и обработки информации, работающей в условиях внешних электромагнитных помех, и является логическим продолжением исследования типовой схемы полевого измерительного комплекса с целью поиска возможных причин неустойчивой работы и способов их устранения. Рассмотрено назначение основных рабочих узлов и порядок их взаимодействия. Сформулированы условия бесперебойной работы оборудования. Подробно рассмотрены меры по защите от помех внутренних и внешних каналов связи. Выделены общие физические методы защиты от внешних помех. Проанализированы применяемые протоколы последовательной передачи данных. Непосредственное измерение аналогового сигнала выполняется аналого-цифровым преобразователем под управлением контроллера и использует протокол SPI (Serial Peripheral Interface – последовательный периферийный интерфейс). Передача данных между контроллером и ПК осуществляется по протоколу UART/USART (Universal Synchronous/Asynchronous Receiver and Transmitter – UART или USART). Кроме стандартных, для внутреннего обмена данными, использован протокол собственной разработки. По каждому протоколу приведены примеры программной реализации всех этапов использования: инициализации, реинициализации при сбое, передачи данных, контроля передачи. Рассмотрены возможности оптимизации протоколов обмена информацией. Предложены методы контроля, самоконтроля и самовосстановления оборудования.

Ключевые слова
Микроконтроллер, последовательные протоколы, UART/USART, помехоустойчивость, измерительный прибор, самоконтроль, статическое зондирование.

Введение

Современный мир перенасыщен различными электромагнитными излучениями от средств беспроводной мобильной связи [1-5] и передачи широковещательных данных [6-19]. Вопросы создания помех от радиосредств друг другу регулируются соответствующим частотно-территориальным планированием. Однако возникающие интермодуляционные излучения могут создавать помехи при определении координат движущихся объектов [20-22] и проведении различных научных экспериментов. Для эффективного использования большого количества накопленных в мировой литературе данных целесообразно применение информационных систем [23-26].

Всякое оборудование, призванное сопровождать исследования, должно быть адаптировано к условиям проводимого эксперимента. Если речь идет о длительных наблюдениях в природных или городских условиях, необходимо обеспечивать работоспособность оборудования в автономном режиме. Для этого следует разрабатывать максимально простые алгоритмы контроля и самоконтроля взаимодействующих систем.

Проведем анализ типовой схемы полевого измерительного комплекса с целью поиска возможных причин неустойчивой работы и способов их устранения.

Работа посвящена оптимизации системы сбора и обработки информации, работающей в условиях внешних электромагнитных помех, и является логическим продолжением исследования [27].

Анализ схемы

На рисунке 1 приведена блок-схема исследуемого измерительного комплекса. Исследования проводились на базе комплекта аппаратуры ПИКА-19 производства НТЦ ПИКА-ТЕХНОСЕРВИС, но подход к анализу и основные выводы могут быть перенесены на контрольно-измерительные модули, работающие с аналоговыми и цифровыми сигналами. В общем случае система состоит из трех основных взаимодействующих частей: измерительного прибора, блока контроля и системы внешнего управления. Каждая из этих частей оснащена своим набором датчиков, отслеживающих изменения окружающих объектов. Вся информация аккумулируется измерительным прибором и в режиме реального времени передается ПК для обработки, интерпретации и визуализации. Возможна работа без использования ПК в режиме реального времени, тогда вся информация должна быть сохранена во внутренней энергонезависимой памяти измерительного прибора.

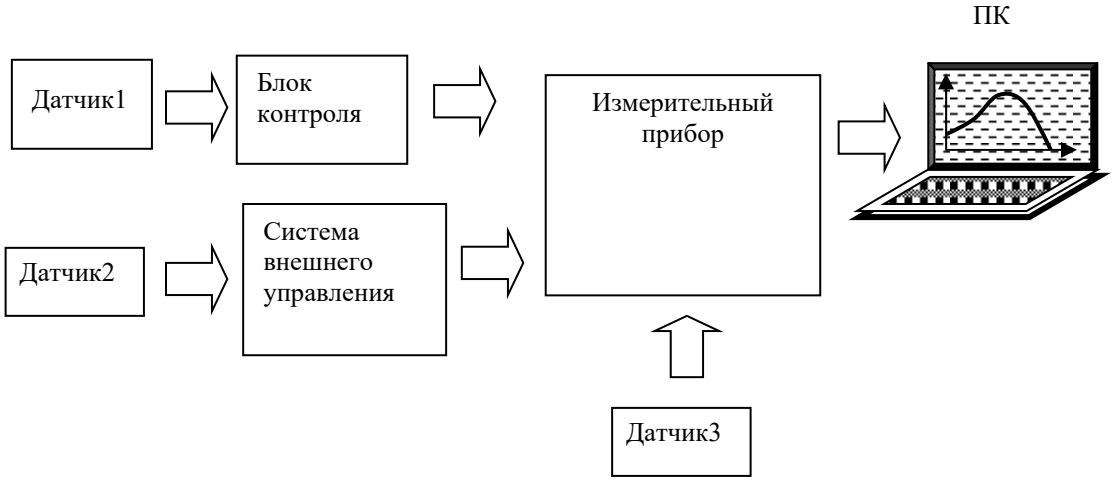


Рис. 1. Блок-схема

Для бесперебойной работы оборудования необходимо обеспечить:

- условия работы датчиков;
- стабильность источников и схем питания;
- защиту от помех внутренних и внешних каналов связи;
- оптимизацию протоколов обмена информацией;
- Последние два пункта рассмотрим подробно.

Защита от помех внутренних и внешних каналов связи

Под внутренними каналами связи будем понимать соединения между электронными компонентами, обменивающимися информацией и находящимися на одной монтажной плате или внутри одного приборного корпуса, под внешними – проводные или беспроводные системы обмена данными между различными приборами, входящими в состав контрольно-измерительного комплекса

Помехи по своему происхождению могут быть внутренними (взаимное влияние сигналов внутри комплекса) и внешними. Внутренние помехи анализируются, минимизируются или устраняются применением грамотных схемотехнических и программных решений. К внутренним, например, мож-

но отнести «дребезг» сигналов кнопок управления, вызывающий двойное или многократное срабатывание. Внешние помехи также могут вызывать паразитные срабатывания, приводить к возникновению заведомо ложных результатов или нарушению работоспособности регистрирующей части оборудования.

Общими физическими методами защиты от внешних помех являются:
- Использование металлических или металлизированных корпусов;
- Вывод общего провода на корпус прибора;
- Использование коаксиальных кабелей для проводной передачи информации;
- Использование ферритовых колец для проводных информационных коммуникаций.

Наиболее чувствительной к помехам является последовательная передача информации.

Оптимизация протоколов обмена информацией

На разных этапах использованы разные протоколы последовательной передачи данных. Непосредственное измерение аналогового сигнала выполняется аналого-цифровым преобразователем под управлением контроллера и использует протокол SPI (Serial Peripheral Interface – последовательный периферийный интерфейс). Передача данных между контроллером и ПК осуществляется по протоколу UART/USART (Universal Synchronous/Asynchronous Receiver and Transmitter – UART или USART). Кроме этого обмен данными между блоком контроля и измерительным прибором, а также между системой внешнего управления и измерительным прибором осуществляется с использованием однопроводного канала собственной разработки. Общие сведения о инициализации и использовании названных протоколов можно найти в работе [29], а примеры реализации обмена данными в работе [30].

Рассмотрим подробно особенности каждого протокола.

1. Последовательный интерфейс SPI.

Для связи двух устройств – ведущего (Master) и ведомого (Slave) – требуется четыре провода. Реализуется синхронный режим передачи. Синхронизация осуществляется за счет общего тактового сигнала, который формируется ведущим устройством. Еще два провода используются для обмена данными, помещенными в сдвиговые регистры связывающихся устройств. Четвертый провод – выбор микросхемы (Chip Select) – служит для активизации ведомого устройства. В описании используемого контроллера [28] подробно описаны все настройки интерфейса и приведены временные диаграммы, необходимые для понимания происходящих процессов.

В исследуемой схеме последовательный протокол SPI используется на следующих участках: при обмене информацией между АЦП и контроллером (в блоке контроля и измерительном приборе) и при записи и чтении энергонезависимой памяти. Кроме того, синхронный последовательный интерфейс используется при внутрисхемном программировании контроллеров. Во всех внутренних обращениях используются настройки SPI, приведенные на рисунке 2.

```
// SPI initialization
// SPI Type: Master
// SPI Clock Rate: 921,600 kHz
// SPI Clock Phase: Cycle Half
// SPI Clock Polarity: Low
// SPI Data Order: MSB First
SPCR=0x51; // 0101 0001 слева направо
// 0 - прерывание от SPI запрещено
// 1 - модуль SPI включен, задействованы выводы MOSI, MISO, SCR, SS
// 0 - (порядок передачи) первым передается MSB
// 1 - (выбор режима работы) режим ведущего (Master)
// 0 - (полярность тактового сигнала) во время ожидания на SCK присутствует низкий уровень
// 0 - (фаза тактового сигнала) данные считываются по нарастающему фронту SCK
// 01 - (скорость передачи) частота SCK равна CK/16 14,7456/16 = 0,9216 МГц.
```

Рис. 2. Настройка SPI

В случае взаимодействия с АЦП требуется еще один провод, по которому контроллеру поступает сигнал от АЦП о готовности данных. Этот сигнал вызывает внешнее прерывание контроллера. При обработке этого прерывания происходит считывание регистра данных АЦП. Так как сдвиговый регистр используемого контроллера является восьмиразрядным, а результат на выходе АЦП шестнадцатиразрядным, программно реализуется двойное обращение к АЦП.

Пример кода приведен на рисунке 3.

```
//Чтение регистра АЦП
unsigned int registerADC_read(void)
{
 unsigned int dbin;
 PORTB.2=0; //выбор АЦП (cs=0)
 #asm("nop\nop")
 dbin=0;
 //записываем в коммуникационный регистр
 SPDR=0x38|(tcan&0x01);
 //1ый канал активный,следующая операция чтение регистра данных
 while(!SPSR.7);
 SPDR=0x00;
 while(!SPSR.7);
 #asm("nop")
 dbin=SPDR;//присваиваем переменной содержимое регистра данных
 dbin=dbin<<8;//сдвигаем на 8 разрядов влево
 SPDR=0x00;
 while(!SPSR.7);
 dbin=dbin|SPDR;//читаем следующие 8 разрядов и объединяем с прочитанными ранее
 //получаем 16 разрядный результат с АЦП
 #asm("nop")
 PORTB.2=1;// cs=1 отмена выбора АЦП
 return(dbin);
}
```

Рис. 3. Пример кода чтения регистра АЦП

Таким образом, время чтения результата составит

$$t_1 = 16T_1 + \Delta t = \frac{16}{f_1} + \frac{N}{f_2} = \frac{16}{921600} + \frac{13}{14745600} = 18 \cdot 10^{-6}\,\text{с},$$

где T_1 – время передачи одного разряда; Δt – дополнительное время, затраченное контроллером на инициализацию процесса передачи и т.п., это время можно оценить по числу выполняемых операций N в предположении, что каждая операция выполняется за время одного тактового импульса.

Согласно коду, приведенному на рис. 3, в нашем случае $N = 13$; f_2 – частота контроллера, определяемая используемым внешним кварцевым резонатором.

Это время непосредственного использования интерфейса SPI, а, следовательно, максимальной чувствительности к помехам меньшей длительности.

При работе с АЦП обновление данных и формирование сигнала о готовности данных (DRDY), вызывающего внешнее прерывание контроллера, происходит каждые

$$t_2 = \frac{500}{f_{ADC}} = \frac{500}{2457600} = 203 \cdot 10^{-6}\,\text{с}.$$

Обрабатывается этот сигнал только при наличии соответствующей управляющей команды. Ес-

ли внешняя помеха вызвала изменение значения на выходе АЦП, достаточно продублировать передачу значения и выполнить сравнение для констатации сбоя. Если внешняя помеха привела к нарушению канала связи (зависанию) необходимо выполнить переинициализацию АЦП. Так как диагностировать зависание в процессе работы проблематично, целесообразно выполнять перезагрузку АЦП периодически. Такой прием был использован в программе блока контроля, где требовалось проводить измерения с интервалом 300 мс и сдвигом между двумя каналами АЦП в 30 мс.

Пример рабочего кода, реализующего сброс и перезагрузку АЦП в определенные моменты времени, приведен на рисунке 4.

```
if  (tickcount == 850)
{
// аппаратный сброс АЦП
PORTB.0=0; // подаем "0" на RESET ADC
#asm("nop\nop")
PORTB.0=1;
#asm("nop")
ADC_init();  // инициализация АЦП_1
pereklcan();
GICR|=0x40;  // разрешаем прерывание от АЦП (INT0)
}
```

Рис. 4. Пример кода перезагрузки АЦП

При работе с энергонезависимой памятью, для программного контроля за процессом записи, в алгоритм была заложена следующая последовательность действий:

1. получить значение от измерительного преобразователя;
2. записать значение по указанному адресу;
3. считать значение по указанному адресу;
4. сравнить исходное и прочитанное значение;
5. при совпадении значений подать кратковременный сигнал на систему индикации.

Такой алгоритм не защищает от влияния помех, но позволяет быстро обнаруживать неисправность.

2. Последовательный интерфейс UART(USART).

Для связи двух устройств используется два провода. В рассмотренном случае этот протокол применялся для передачи данных между контроллером измерительного прибора, контроллером памяти и ПК. В зависимости от схемы подключения информация могла передаваться от измерительного преобразователя параллельно контроллеру (для записи в память) и на компьютер в режиме реального времени или от контроллера памяти на компьютер (см. рис. 5).

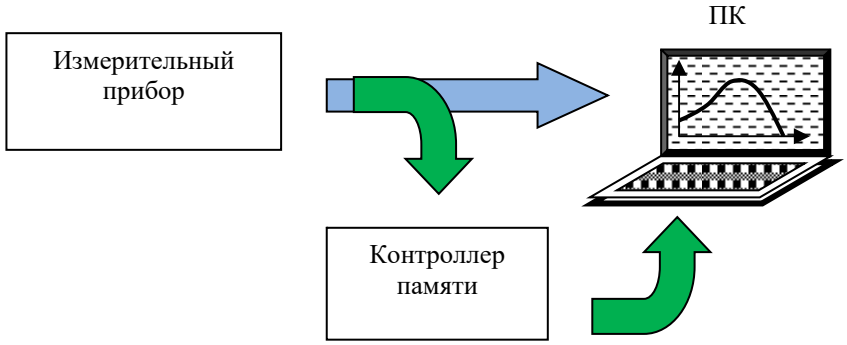


Рис. 5. Использование USART

Модуль USART осуществляет посылку 8-битных пакетов данных, добавляя к ним в начале старт-бит (ноль) и в конце – бит четности и стоп-бит (единица). Если при передаче произойдет сбой в

одном бите (нуль изменится на единицу или наоборот), то бит четности перестанет соответствовать байту данных и приемник сможет определить, что пакет передан неверно. Для передачи пакет помещается в сдвиговый регистр и биты последовательно перемещаются на выход передатчика (TXD). Одновременно приемник модуля USART проверяет состояние входа RXD, причем на каждый принимаемый бит приходится 16 отсчетов. Считывание значения бита происходит по трем выборкам в середине его передачи, это снижает требования к фронтам принимаемых сигналов. Последним считывается стоп-бит. Если при его считывании две выборки из трех не равны единице регистрируется ошибка кадрирования.

Используемые настройки протокола USART приведены на рисунке 6.

```
// USART initialization
// Communication Parameters: 8 Data, 1 Stop, No Parity
// USART Receiver: Off
// USART Transmitter: On
// USART Mode: Asynchronous
// USART Baud Rate: 9600
UCSRA=0x00;
UCSRB=0x00; //
UCSRC=0x86; // формат посылки
UBRRH=0x00; // скорость
UBRRL=0x5F; // 9600 бит/с
```

Рис. 6. Инициализация USART

При инициализации USART значение регистра управления UCSRB не устанавливается – приемник/передатчик выключен. Включение режима передатчика или приемника осуществляется непосредственно перед выполнением передачи. На рис. 7 приведен код отправки двух шестнадцатиразрядных значений.

```
UCSRB=0x08; // разрешает передатчик
if((ctbyte < 4)&(time_send > 12))
{
       switch(ctbyte){

              case 0x00: {time_send = 0; UDR = (lob & 0xFF); ctbyte++; break;} // передаем 8 младших бит
              case 0x01: {time_send = 0; UDR = (lob >> 8); ctbyte++; break;} // передаем 8 старших бит
              case 0x02: {time_send = 0; UDR = (bok & 0xFF); ctbyte++; break;} // передаем 8 младших бит
              case 0x03: {time_send = 0; UDR = (bok >> 8); ctbyte++; break;} // передаем 8 старших бит
              default : {break;}
              } // switch
              UCSRB=0x00; // запрещает передатчик
} // if
```

Рис. 7. Передача данных по USART

Контроллер возвращается к процессу передачи в непрерывном цикле каждый раз, когда сформирована следующая пара значений. Между посылками выдерживается пауза 12 мс. Это время отводится на все подготовительные операции и непосредственно передачу и завершение всех переходных процессов, с ней связанных. Для скорости 9600 бит/с заданный промежуток времени на порядок превышает время 10 битной посылки.

Передача данных с использованием протокола USART является наименее помехозащищенной и требует предусматривать возможность восстановления связи при ее нарушении. Так как программа контроллера согласуется с драйвером данных, запускаемым на ПК, то для восстановления передачи данных в случае «зависания» необходимо одновременно остановить обращения к COM порту со стороны прибора и ПК. В интерфейсе драйвера предусмотрена команда «ПАУЗА». При ее вызове программа обращается к последовательному порту, как к файлу, и закрывает его, если он открыт. После этого возможна перезагрузка контроллера и АЦП прибора по команде с прибора, которая происходит

без потери данных и нарушения связи.

Еще одним потенциальным источником нарушения работоспособности является приемная часть аппаратуры, призванная реагировать на импульсные сигналы. Рассмотрим схему, приведенную на рис. 1. Она предназначена для проведения регистрации сигналов с датчиков 1 и 3 по команде, которая в свою очередь формируется при обработке сигналов с датчика 2. Принцип действия системы подробно разобран в работе [31]. Состоит он в выполнении следующей последовательности операций:

1. Передающее устройство, входящее в состав датчика 2, формирует пакет импульсов.
2. Приемное устройство датчика 2 получает пакет импульсов.
3. По времени распространения определяется расстояние, пройденное сигналом.
4. Расстояние преобразуется в число и передается измерительному прибору.
5. Измерительный прибор сравнивает расстояние с заданным и при совпадении формирует команду на измерения сигналов с датчиков 1 и 3.
6. Сигнал с датчика 1 преобразуется блоком контроля в число и передается измерительному прибору.
7. Сигнал с датчика 3 непосредственно поступает на измерительный прибор.
8. Все значения передаются ПК.

Сигналы с датчиков 1 и 3 – аналоговые и плавно изменяющиеся. Численное значение сигнала с датчика 1 обновляется каждые 0,3 с и передается в непрерывном цикле, а по команде на измерения происходит фиксация текущего значения для дальнейшей передачи его ПК.

Система прекрасно показала себя на лабораторном стенде и оказалась неработоспособной при испытании на помехозащищенность.

На этапе отладки были выявлены причины отказов и предложены методы их устранения. Основной причиной стало нарушение работы приемника импульсных сигналов. В результате отклика на помеху приемник вызывал паразитное срабатывание прерывания по захвату контроллера. Время распространения сигнала, определяемое контроллером, принимало случайное значение, как следствие, команда на измерения сигналов с датчиков не формировалась вообще или возникала в произвольные моменты времени.

Для восстановления контрольно-измерительных функций модуля было предложено:

- отказаться от последовательного канала передачи численного значения расстояния и заменить его формированием команды на регистрацию данных непосредственно системой внешнего управления;
- ввести программный контроль за длительностью сигнала, вызывающего прерывание контроллера по захвату.

В совокупности с методами стабилизации последовательных интерфейсов обмена данными внутри модуля эти меры позволили контрольно-измерительному модулю пройти полевые испытания.

Заключение

В работе рассмотрены основные проблемы работы электронной аппаратуры при наличии электромагнитных помех. Основным условием устойчивой работы является временное согласование отдельных функциональных узлов. Это согласование обеспечивается грамотным выбором настроек протоколов обмена данными. Проанализированы используемые в выбранной схеме последовательные интерфейсы, приведены примеры их инициализации и использования. Названы физические способы защиты передачи данных и предложены методы самовосстановления системы. Исследование проведено на базе полевого измерительного комплекта аппаратуры ПИКА-19, выпускаемого ООО «Научно-технический центр ПИКА-ТЕХНОСЕРВИС».

Литература

1. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Технологии в системах радиосвязи на пути к 5G // Москва, 2018.
2. *Харкевич А.А.* Теория информации. Опознание образов // Избранные труды в трех томах / Москва, 1973. Том 3

3. *Харкевич А.А.* Теория электроакустических преобразователей. Волновые процессы // Избранные труды в трех томах / Москва, 1973. Том 1
4. *Бакулин М.Г., Крейнделин В.Б., Шлома А.М., Шумов А.П.* Технология OFDM // Москва, 2016.
5. *Дымкова С.С.* Облачные IOT платформы и приложения для оптимизационного управления транспортом // REDS: Телекоммуникационные устройства и системы. 2020. Т. 10. № 4. С. 39-50.
6. *Варламов О.В., Варламов В.О., Долгопятова А.В.* Международная сеть DRM вещания для создания информационного поля в Арктике // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 9. С. 9-16.
7. *Варламов О.В., Нгуен Д.К., Грычкин С.Е.* Комбинирование синтетических методов высокоэффективного высокочастотного усиления // T-Comm: Телекоммуникации и транспорт. 2021. Т. 15. № 9. С. 11-16.
8. *Варламов О.В.* Максимальная мощность коммутируемого p-i-n диодами антенно-согласующего устройства диапазона ВЧ при рассогласовании нагрузки // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 10. С. 26-32.
9. *Filimonov N., Varlamov O., Itkin G.* Efficient modulation of RF signals // Патент на изобретение US 7724837 B2. Заявка № US20040546012 от 07.01.2004.
10. *Варламов О.В., Лаврушенков В.Г.* Критерии качества передающего устройства для стандарта DRM и измерительное оборудование // Broadcasting. Телевидение и радиовещание. 2004. № 3. С. 44-48.
11. *Варламов О.В.* Разработка требований к приемному оборудованию сетей цифрового радиовещания стандарта DRM // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 9. С. 39-42.
12. *Варламов О.В., Громорушкин В.Н., Лаврушенков В.Г., Чугунов И.В.* Генератор испытательных сигналов для измерительных характеристик ключевых усилителей мощности с раздельным усилением составляющих однополосного сигнала // T-Comm: Телекоммуникации и транспорт. 2011. Т. 5. № 9. С. 47-49.
13. *Gromorushkin V.N., Varlamov O.V., Dolgopyatova A.V., Voronkov A.A.* Operation problems of the EER transmitter with narrowband antenna // В сборнике: 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019. 2019. С. 8706736.
14. *Varlamov O.V.* Organization of single frequency DRM digital radio broadcasting networks. Features and results of practical tests // В сборнике: 2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2018. 2018. С. 8456925.
15. *Varlamov O.V., Gromorushkin V.N.* Class D switching power amplifier with a filter under load mismatch conditions // В сборнике: 2020 Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2020. 2020. С. 9131508.
16. *Varlamov O.V., Nguyen D.C., Grychkin S.E.* Simultaneous application of several synthetic methods for high efficiency radiofrequency amplification // В сборнике: 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings. 2021. С. 9416126.
17. *Варламов О.В.* Организация одночастотных сетей цифрового радиовещания стандарта DRM. Особенности и результаты практических испытаний // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 11. С. 4-20.
18. *Varlamov O.V.* Experimental study of a synchronous DVB-T2 network in the yaroslavl region. Problems with some manufacturers' receivers // В сборнике: 2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 - Proceedings. 2020. С. 9261562.
19. *Варламов О.В., Варламов В.О.* Распределение максимальных уровней атмосферных радиошумов в диапазонах низких частот и средних частот по территории Земли // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 5. С. 42-51.
20. *Dymkova S.* Applicability of 5G subscriber equipment and global navigation satellite systems // Synchroinfo Journal. 2021. Т. 7. № 5. С. 36-48.
21. *Dymkova S.S., Dymkov A.D.* Experimental studies of GNSS errors in rough and wooded mountainous terrain // В сборнике: 2021 International Conference on Engineering Management of Communication and Technology, EMCTECH 2021 - Proceedings. 2021. С. 9

22. *Dymkova S.S., Dymkov A.D.* Multifactorial methodology of cycling routes time calculation based on 3D maps // В сборнике: 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings. 2021. С. 9416046.
23. *Дымкова С.С.* Повышение эффективности функционирования информационных систем и процессов в высшей школе // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2017. Т. 6. № 2. С. 45-48.
24. *Дымкова С.С.* Новые принципы организации функционирования систем по продвижению результатов научных исследований // Системы синхронизации, формирования и обработки сигналов. 2017. Т. 8. № 1. С. 34-37.
25. *Дымкова С.С.* Разработка информационной системы для продвижения результатов научных исследований // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 7. С. 38-41.
26. *Артюшенко В.М., Аббасова Т.С., Стреналюк Ю.В., Васильев Н.А., Белюченко И.М., Самаров К.Л., Зиновьев В.Н., Посеренин С.П., Вокин Г.Г., Мороз А.П., Шайдуров В.С., Шаврин С.С.* Системный анализ в области управления и обработки информации // Монография / Королев, 2015.
27. *Biriukova O., Koretskaya I.* Using an ultrasonic sensor to monitor position, transfer control commands and work information // Systems of Signals Generating and Processing in the Field of on Board Communications INSPEC, 2019.
28. Datasheet Atmega8(L) ©Atmel Corporation http://www.microchip.com.
29. *Morton J.* AVR: an introductory course, Newnes, 2002. 254 p. ISBN 78-0-7506-5635-1.
30. Программирование на языке С для AVR и PIC микроконтроллеров./ Сост. *Ю.А. Шпак.* 2-е издание, переработанное и дополненное – М: Корона-Принт, 2016, 544 с. ISBN 978-5-7931-0842-3.
31. *Biryukova O.V., Koretskaya I.V.* Signal recording system control // 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, 16-18 March 2021 Moscow, Russia Conference.

МАТЕМАТИЧЕСКАЯ (КОМПЬЮТЕРНАЯ) МОДЕЛЬ ТЯГОВОГО ЭЛЕКТРИЧЕСКОГО ПРИВОДА ЭЛЕКТРОМОБИЛЯ

Афанасьев Константин Михайлович
студент, МАДИ, Москва, Россия

Сидоров Кирилл Михайлович
к.т.н., доцент, МАДИ, Москва, Россия
electro@madi.ru

Аннотация
В статье рассматривается компьютерная модель тягового электрического привода электромобиля, сформированная в среде математического моделирования. В результате расчетных исследований получены основные зависимости, характеризующие работу основных компонентов силовой установки транспортного средства, в том числе тяговой батареи, силового инвертора и электрической машины. Для условий движения электромобиля в смешанном цикле определены энергетические показатели работы электрического привода.

Ключевые слова: *электромобиль, электрический привод, инвертор, моделирование.*

Математическое (компьютерное) моделирование сегодня занимает неотъемлемую часть практически любой научно-исследовательской работы, повсеместно используется при решении задач инженерного проектирования. Современные средства компьютерного моделирования позволяют воспроизвести работу сложных систем в своего рода виртуальной лаборатории. Так, в рамках настоящей работы сформирована компьютерная модель тягового электрического привода легкового электромобиля [1-8] в специализированной программной среде Matlab&Simulink [9]. Структурная схема комплексной модели представлена на рисунке 1.

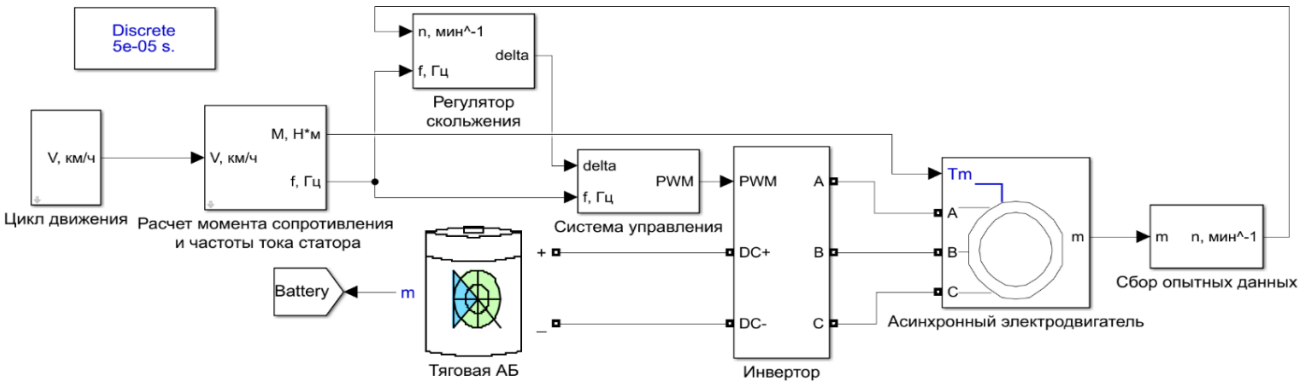


Рис. 1. Структурная схема модели тягового электрического привода электромобиля

Модель объединяет в своем составе следующие блоки:

– модель тяговой аккумуляторной батареи, математическую основу которого составляет уравнение Шеферда [10];

– модель асинхронного электродвигателя с короткозамкнутым ротором, основанную на системе дифференциальных уравнений, описывающих электромеханическое преобразование энергии;

– блок автономного инвертора напряжения, включая силовую часть и систему управления с регулятором скольжения [11];

– блок задания цикла движения;

– блок расчета момента сопротивления на валу двигателя и необходимой частоты тока статора;

– вспомогательные блоки.

Исходными данными для моделирования служат параметры транспортного средства, условий движения, характеристики тяговой аккумуляторной батареи и электрической машины, которые вносятся в диалоговые окна настроек каждого блока. Согласно заданным исходным данным в модели ведется расчет основных механических, электрических и энергетических показателей работы силовой установки электромобиля. Часть расчетных параметров служит входными данными для работы составляющих моделей. Так, например, отдельным блоком осуществляется расчет момента сопротивления, приведенного к валу электродвигателя, а также требуемой по условию реализации цикла движения частоты тока статора согласно следующим выражениям:

$$M_c = \frac{f \cdot m_a \cdot g \cdot \cos\alpha + m_a \cdot g \cdot \sin\alpha + \frac{\rho}{2} c_x \cdot S_a \cdot V^2}{i} r_k, \quad (1)$$

$$f_1 = \frac{30 \cdot V \cdot i}{3.6 \cdot \pi \cdot r_k} \frac{p}{60}, \quad (2)$$

где m_a – масса электромобиля, кг; f – коэффицент трения качения; α – угол наклона дороги; ρ – плотность воздуха; c_x – коэффициент аэродинамического сопротивления; S_a – площадь фронтальной проекии; r_k – динамический радиус колеса; i – передаточное число главной передачи; p – число пар полюсов электродвигателя.

Расчетные значения Mc и f_1 служат входными данными соответственно для модели электрической машины и системы управления инвертором. Автономный инвертор (АИ) осуществляет преобразование постоянного напряжения тяговой аккумуляторной батареи в трехфазное переменное напряжение, регулируемое по частоте и амплитуде для управления частотой вращения и крутящим моментом электродвигателя. АИ выполнен по мостовой схеме, включающей шесть транзисторно-диодных модулей (VT1-VT6). Входная силовая цепь инвертора содержит батарею фильтрующих конденсаторов. Вариант реализации силовой части АИ в среде компьютерного моделирования представлен на рисунке 2 [12].

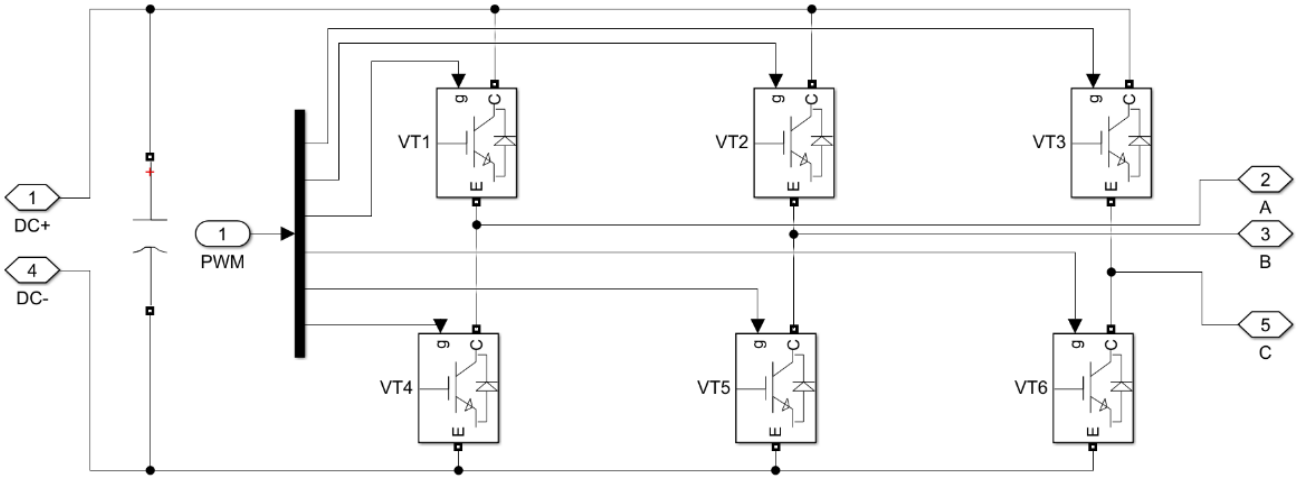


Рис. 2. Реализация силовой части автономного инвертора в среде компьютерного моделирования

С целью формирования в обмотках фаз двигателя переменного тока синусоидальной формы транзисторы АИ коммутируются по определенному алгоритму. В представленной модели система управления АИ формирует управляющие импульсы для транзисторных ключей согласно алгоритму синусоидальной широтно-импульсной модуляции (ШИМ). Для реализации данного метода в модели формируется трехфазный сигнал синусоидальной формы, частота которого соответствует расчетному значению f_1 и необходимой скорости движения электромобиля. Указанный сигнал сравнивается с опорным пилообразным напряжением фиксированной частоты с помощью компаратора. В результате сравнения после ряда преобразований формируются управляющие импульсы. При работе АИ должна исключаться возможность одновременного нахождения нижнего и верхнего транзисторов каждого плеча в открытом состоянии. Поэтому их управляющие сигналы должны находиться в противофазе, что реализуется в схеме управления с помощью логического инвертора [13].

Другой составной частью системы управления АИ в рассматриваемой модели является блок, реализующий закон управления асинхронной машиной. В настоящей работе реализован пропорциональный закон изменения выходного напряжения АИ с изменением частоты f_1. Для повышения устойчивости работы электрического привода закон управления корректируется регулятором, ограничивающим скольжение асинхронной машины на заданном уровне. Структурная схема системы управления АИ представлена на рисунке 3.

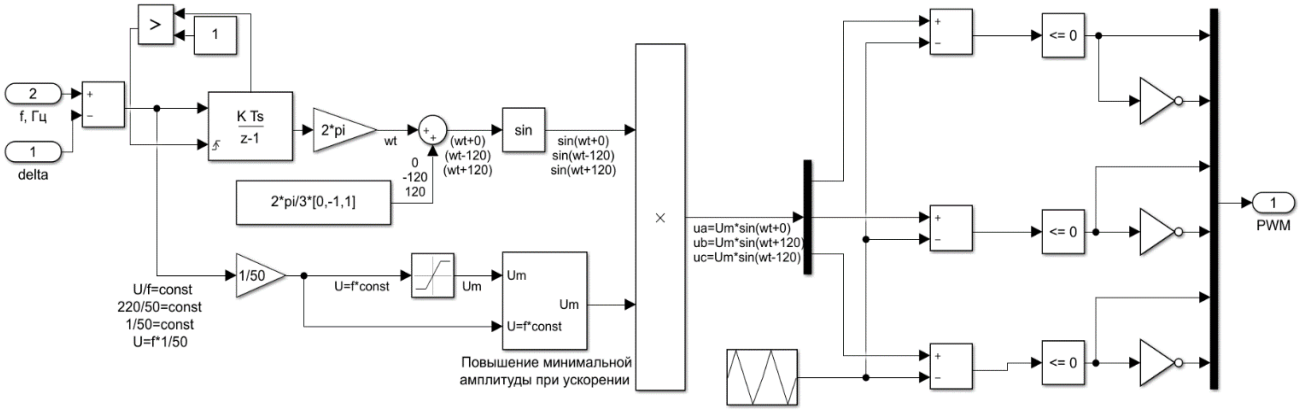


Рис. 3. Принципиальная схема системы управления двигателем

Некоторые результаты математического (компьютерного) моделирования электропривода электромобиля при движении последнего на участке типового цикла (WLTP) представлены на рисунке 4, где отражены зависимости частоты вращения ротора, электромагнитного момента и входного тока АИ от времени.

Для оценки энергетических показателей работы силовой установки в модели предусмотрен расчет удельного расхода энергии тяговой батареи согласно следующему выражению:

$$g = \frac{W_б}{L} = \frac{\int_0^T U_{АБ} \cdot I_{АБ} dt}{\int_0^T V dt}, \quad (3)$$

где $U_{АБ}$, $I_{АБ}$ – напряжение и ток тяговой аккумуляторной батареи, $W_б$ – расход энергии в цикле, L – пройденное расстояние, T – продолжительность цикла, V – скорость движения электромобиля.

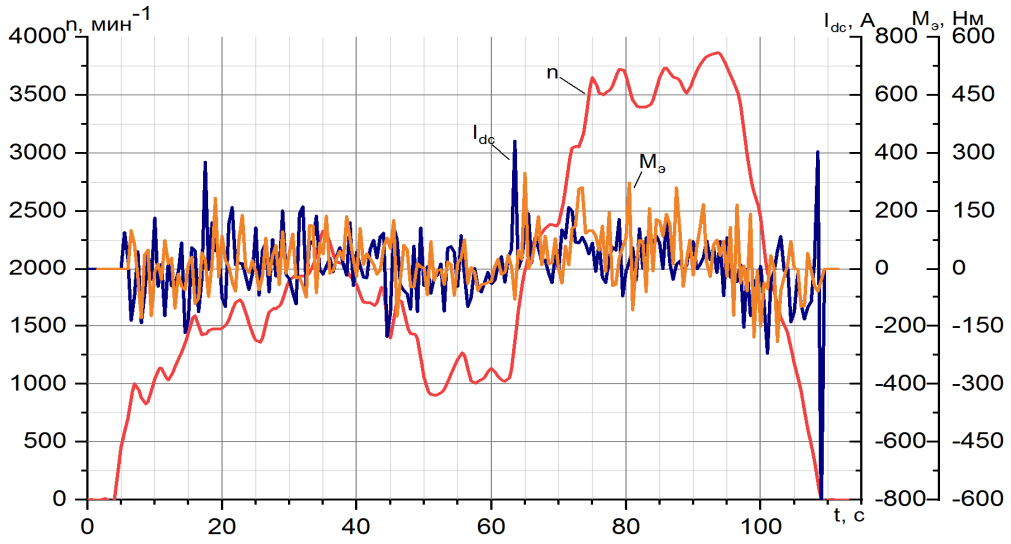


Рис. 4. Зависимости частоты вращения, электромагнитного момента и тока на входе инвертора от времени (движение электромобиля на участке цикла WLTP)

Заключение

В рамках настоящей работы в среде специализированного компьютерного моделирования сформирована комплексная модель тягового электрического привода электромобиля. Модель является универсальной и позволяет для заданных характеристик транспортного средства и параметров тягового электрооборудования получить ключевые показатели работы системы в различных условиях движения. В дальнейшем планируется совершенствование модели и реализация для целей выпускной квалификационной работы бакалавра векторного управления электрической машиной, как более эффективного для задач тягового электропривода.

Литература

1. *Гулямов К.Х., Гуломзода А.Х.* Разработка и исследование повышающего преобразователя постоянного напряжения // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2017. № 4 (51). С. 55-61.

2. *Карелина М.Ю., Арифуллин И.В., Терентьев А.В.* Аналитическое определение весовых коэффициентов при многокритериальной оценке эффективности автотранспортных средств // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2018. № 1 (52). С. 3-9.

3. *Пузаков А.В., Осаулко Я.Ю.* Исследование влияния эксплуатационных факторов на тепловое состояние автомобильного генератора // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2018. № 1 (52). С. 16-23.

4. *Надараиа Ц.Г., Селиванов А.И., Шестаков И.Я., Фадеев А.А., Бабкина Л.А.* Химико-кинетический накопитель энергии и мотор-редуктор для электромобиля // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2017. № 1 (48). С. 12-17.

5. *Мельникова Т.Е., Мельников С.Е., Завязкина В.В.* Электромобили: перспективы и пути развития // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2019. № 3 (58). С. 22-26.

6. *Блудян Н.О.* Перспективы развития электрических автобусов // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2020. № 3 (62). С. 19-24.

7. *Ухов И.В., Климов А.В., Долгий И.О., Рябцев Ф.А.* Анализ и моделирование алгоритма i2t лимитирования тока для литий-ионных батарей // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2021. № 1 (64). С. 3-10.

8. *Климов А.В., Анисимов В.Р.* О некоторых аспектах повышения энергонасыщенности тяговых электрических двигателей // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2021. № 2 (65). С. 26-31.

9. *Черных И.В*. Моделирование электротехнических устройств в MATLAB, SimPowerSystems и Simulink. М.: ДМК Пресс; СПб.: Питер, 2008. 288 с.

10. *Shephard C.M*. Design of primary and secondary cells: An equation describing battery discharge // J. Electrochem. Soc. 1965. Vol. 112, Iss. 3. P. 252-257.

11. *Гельман М.В., Дудкин М.М., Преображенский К.А*. Преобразовательная техника: учебное пособие. Челябинск.: Издательский центр ЮУрГУ, 2009. 425 с.

12. *Лурье М.С., Лурье О.М*. Имитационное моделирование схем преобразовательной техники Красноярск: СибГТУ, 2007. 138 с.

13. *Томашевский Д.Н*. Автономные инверторы: учебное пособие. Екатеринбург: Изд-во Урал. ун-та, 2019. 120 с.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ СИНХРОННЫМ ЭЛЕКТРОДВИГАТЕЛЕМ С ВОЗБУЖДЕНИЕМ ОТ ПОСТОЯННЫХ МАГНИТОВ

Куприянов Егор Сергеевич
студент, МАДИ, Москва, Россия

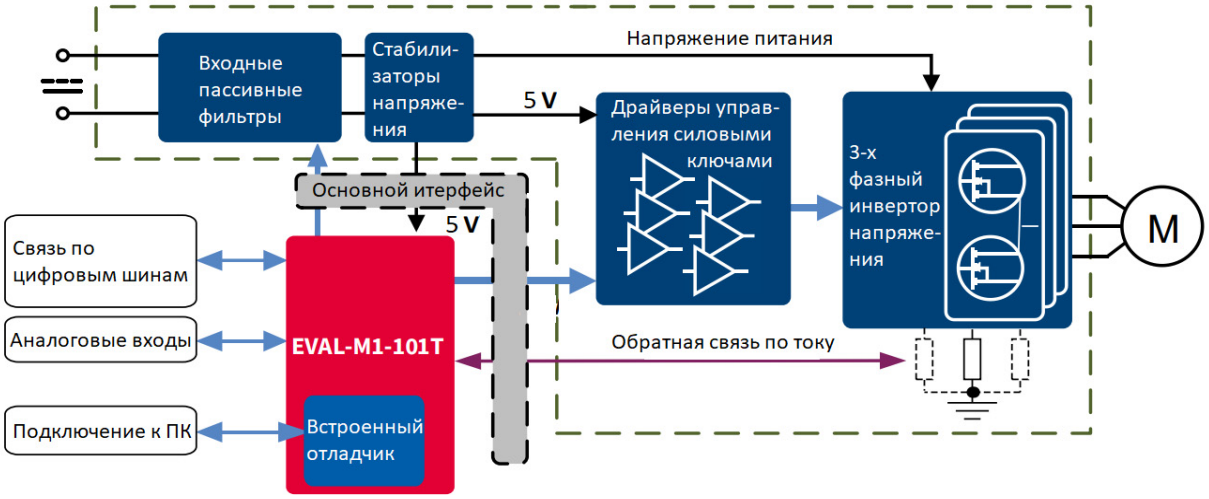
Сидоров Кирилл Михайлович
к.т.н., доцент., МАДИ, Москва, Россия, electro@madi.ru

Аннотация
Синхронные электродвигатели переменного тока с возбуждением от постоянных магнитов сегодня находят широкое применение в различных отраслях промышленности. Данный факт во многом касается и автомобилестроения. В настоящей статье рассмотрен вариант практической реализации системы управления подобной электрической машиной для системы вспомогательного электропривода транспортного назначения.

Ключевые слова: *автономный инвертор напряжения, синхронный электродвигатель, система управления, микроконтроллер.*

На транспортных средствах синхронные электродвигатели переменного тока с возбуждением от постоянных магнитов (СДПМ), помимо тягового применения [1-8], используются для привода вспомогательных агрегатов, таких как компрессоры кондиционеров, жидкостные насосы, специализированное технологическое оборудование. Управление такими электроприводами на борту осуществляется с использованием автономных инверторов напряжения (АИН) с системами векторного регулирования. В состав АИН входят силовая и управляющие части. Силовая цепь включает в себя фильтрующие и защитные элементы, а также силовые ключи, коммутирующие фазы электрической машины (ЭМ) в соответствии с заданным алгоритмом. Управляющая часть включает в себя модуль управления (МУ) на основе микропроцессорного контроллера (МК) и/или цифрового сигнального процессора, датчики обратных связей, драйверы силовых ключей, устройства питания и защиты. МУ, анализируя данные от устройств управления и датчиков АИН и ЭМ, согласно заложенному алгоритму, формирует сигналы управления силовыми ключами инвертора.

Существует несколько алгоритмических подходов к управлению СДПМ. При этом целесообразность реализации того или иного алгоритма диктуется назначением электропривода, его характеристиками, качеством регулирования и технико-экономическими показателями. Для задач вспомогательного привода транспортного назначения, для которого зачастую известен характер нагрузки во всем диапазоне допустимой работы, может быть применен алгоритм адаптивного векторного бездатчикового управления. Отличительная особенность данного способа – не физическое измерение угла положения ротора, а его косвенная оценка без использования датчика угла. На реализацию указанного алгоритма ориентирован МК IMC101T-F048 (Infineon) [9-13]. Этот МК позволяет обеспечить точное и эффективное управление СДПМ сравнительно небольшой мощности. Реализуемая в рамках настоящей работы функциональная схема системы управления приведена на рисунке [9].



Функциональная схема автономного инвертора напряжения

Силовые и управляющие цепи АИН в настоящей работе реализованы посредством нескольких печатных плат, коммутируемых между собой. На плате силовой части размещены: силовые транзисторно-диодные модули, образующие трехфазный мостовой АИН; фильтрующие конденсаторы; цепи датчиков обратных связей (ОС); силовые и сигнальные разъемы. Плата управления АИН включает модуль EVAL-M1-101T [9] на базе указанного выше МК, цепи аналоговой обработки сигналов датчиков обратных связей, блок питания, разъемы для подключения внешних устройств.

К используемым датчикам относится токовый шунт, необходимый для получения актуального значения тока АИН в силовой цепи. Программная часть МК реализована с возможностью использования нескольких схем измерения тока – с тремя шунтами в каждой стойке АИН или одним. Контроль входного постоянного напряжения осуществляется с использованием делителя напряжения, обеспечивающего измерение уровня напряжения в силовой цепи. Эта информация нужна для защитного отключения АИН в случае выхода контролируемой величины из заданного программой МК диапазона. Отличительной особенностью ОС по току и напряжению в реализуемой системе управления является гальваническая развязка с силовой частью, обеспечиваемая изолирующими оптопарами.

Датчик температуры в рассматриваемой схеме представляет собой терморезистор и служит для контроля температурного режима работы ключей с целью предотвращения перегрева силовой части инвертора. В случае превышения температуры двигатель останавливается, а силовая часть инвертора отключается. Помимо варианта бездатчикового регулирования модуль управления предусматривает контроль скорости с использованием датчиков положения ротора на эффекте Холла. В настоящей работе СДПМ применяется в составе привода дополнительного оборудования, при функционировании которого нет необходимости в высокой точности позиционирования ротора. Поэтому задействованы только основные датчики: токовый шунт в отрицательной шине постоянного тока, датчик температуры, делитель входного напряжения.

Необходимым условием работы МК является чистое от шумов и стабильное питающее напряжение. Эта задача реализуется предусмотренными на плате управления конверторами постоянного напряжения, в том числе с биполярным выходом. В системе управления при этом используются несколько уровней напряжения, в том числе 5 В и ±15 В, при входном напряжении цепей управления АИН в диапазоне 9…36 В.

Плата управления выполнена с возможностью разъемного подключения двухканальных драйверов затворов транзисторных ключей, которые формируют согласно управляющим импульсам от МК напряжения открытия +15 В и закрытия -4 В. Защита от некорректной работы транзисторных ключей, в том числе при токовых перегрузках, реализуется драйверами аппаратно, путем измерения напряжения открытого перехода и программно – с учетом заданных предельных значений токов АИН. Сопряжение драйверов с платой управления выполнено с учетом критерия минимизации длины цепей затворов управляемых транзисторов.

Заключение

Настоящая работа преследует цели экспериментальной апробации возможностей управления СДПМ за счет фактической интеграции модуля МК в виде законченного устройства в систему управления АИН. Существует несколько способов такой интеграции и в каждом из них необходима разработка платы управления с необходимыми согласующими звеньями, периферийными компонентами, реализующими должное функционирование МК и полноценное управление СДПМ. Результаты настоящей работы в виде макетного образца платы управления в последствии могут служить необходимой отправной точкой для проектирования законченного устройства – встраиваемого модуля управления СДПМ для АИН различного типоразмерного ряда.

Литература

1. *Гулямов К.Х., Гуломзода А.Х.* Разработка и исследование повышающего преобразователя постоянного напряжения // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2017. № 4 (51). С. 55-61.

2. *Карелина М.Ю., Арифуллин И.В., Терентьев А.В.* Аналитическое определение весовых коэффициентов при многокритериальной оценке эффективности автотранспортных средств // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2018. № 1 (52). С. 3-9.

3. *Пузаков А.В., Осаулко Я.Ю.* Исследование влияния эксплуатационных факторов на тепловое состояние автомобильного генератора // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2018. № 1 (52). С. 16-23.

4. *Надараиа Ц.Г., Селиванов А.И., Шестаков И.Я., Фадеев А.А., Бабкина Л.А.* Химико-кинетический накопитель энергии и мотор-редуктор для электромобиля // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2017. № 1 (48). С. 12-17.

5. *Мельникова Т.Е., Мельников С.Е., Завязкина В.В.* Электромобили: перспективы и пути развития // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2019. № 3 (58). С. 22-26.

6. *Блудян Н.О.* Перспективы развития электрических автобусов // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2020. № 3 (62). С. 19-24.

7. *Ухов И.В., Климов А.В., Долгий И.О., Рябцев Ф.А.* Анализ и моделирование алгоритма i2t лимитирования тока для литий-ионных батарей // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2021. № 1 (64). С. 3-10.

8. *Климов А.В., Анисимов В.Р.* О некоторых аспектах повышения энергонасыщенности тяговых электрических двигателей // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2021. № 2 (65). С. 26-31.

9. AN2018-01 EVAL-M1-101T User Manual // URL: https://www.infineon.com/dgdl/Infineon-An2018-01_EVAL-M1-101T_User_ Manual-UM-v01_06-EN.pdf (дата обращения: 14.04.2022).

10. Электронный каталог компонентов силовой электроники: Методика выбора драйвера IGBT или MOSFET транзистора // URL: www.efo-power.ru/pub/power/Drivers/AN1001_rus.pdf (дата обращения: 14.04.2022).

11. *Гельман М.В., Дудкин М.М., Преображенский К.А*. Преобразовательная техника: уч. пособие. Челябинск: Издательский центр ЮУрГУ, 2009. 409 с.

12. *Усольцев А.А*. Электрический привод: уч. пособие. Спб.: НИУ ИТМО, 2012. 238 с.

13. *Калачев Ю.Н*. Векторное регулирование (заметки практика). М.: компания «ЭФО», 2013. 63 с.

АНАЛИЗ ТЕХНИЧЕСКОГО УРОВНЯ И ТЕНДЕНЦИЯ РАЗВИТИЯ СПОСОБОВ И УСТРОЙСТВ В ОБЛАСТИ УПРАВЛЕНИЯ ТЯГОВОЙ СИСТЕМОЙ ТРАНСПОРТНЫХ СРЕДСТВ С ЭЛЕКТРОТЯГОЙ

Глазов Владимир Андреевич
студент группы 5ТК2 кафедры «Транспортные установки», Московский автомобильно-дорожный государственный технический университет (МАДИ), Москва, Россия
komoric@yandex.ru

Илюшенко Валентина Константиновна
студент группы 5ТК2 кафедры «Транспортные установки», Московский автомобильно-дорожный государственный технический университет (МАДИ), Москва, Россия,
ilusenkovaliya@gmail.com

Ерусланкин Сергей Алексеевич
старший преподаватель кафедры «Транспортные установки», Московский автомобильно-дорожный государственный технический университет (МАДИ), Москва, Россия,
riffcss@mail.ru

Аннотация
В статье рассмотрены основные виды типов управления электрическим приводом в транспортных средствах с электротягой, их отличительные особенности, достоинства и недостатки. Проведен анализ технического уровня разработок в области создания систем управления. По результатам проведенных исследований определена тенденция развития в данной области техники.

Ключевые слова: *электрический привод, электрическое регулирование скорости электропривода, управляющее устройство.*

Современный электрический привод в транспортных средствах с электротягой представляет собой сложную систему, включающую в себя силовой электрический преобразователь, тяговый электродвигатель постоянного или переменного тока, передаточное и управляющее устройства, а также большое количество различных датчиков, необходимых для контроля и управления этой системой [1-8].

Силовой электрический преобразователь предназначен для управления потоком электрической энергии, поступающей от источника энергии (аккумуляторных батарей, генератора) в целях регулирования работы электродвигателя.

Передаточное устройство предназначено для передачи вырабатываемой электродвигателем механической энергии исполнительному устройству через соединительные муфты и механические передачи [9].

Управляющее устройство представляет собой информационную слаботочную часть системы управления, предназначенную для получения и обработки информации о задающих воздействиях и состоянии системы и выработки на её основе сигналов управления преобразовательным и электродвигательным устройствам.

Быстрое развитие силовой электроники и микропроцессорной техники способствовали совершенствованию информационной части электропривода, что привело к появлению новых способов управления тяговой системой транспортных средств с электротягой.

Управление тяговой системой обеспечивается либо механическим путём, либо путём электрического регулирования скорости электропривода.

Механические способы регулирования реализуются с помощью ступенчатого или бесступенчатого изменения передаточного числа системы. Они требуют введения в кинематическую цепь приво-

да коробок передач, механических вариаторов и других устройств, усложняющих механическую часть электропривода, снижая его эффективность и надёжность. В настоящее время механическое регулирование находит ограниченное применение.

Электрическое регулирование скорости электропривода лишено вышеуказанных недостатков. Рассмотрим некоторые способы электрического регулирования, их достоинства и недостатки.

Реостатное регулирование скорости. Такой способ предусматривает введение добавочных сопротивлений разного номинала в силовую цепь двигателей как средство регулирования момента и тока. Достоинствами такого способа являются простота регулирования и невысокие затраты на реализацию. Недостатками являются невысокая плавность и, как следствие, необходимость увеличивать количество ступеней добавочных сопротивлений, а также снижение точности регулирования вследствие температурных изменений сопротивлений обмоток [10].

Частотное регулирование асинхронных электроприводов. При таком способе используются преобразователи, которые изменяют по требуемому соотношению или независимо друг от друга частоту и амплитуду напряжения. Достоинствами являются плавность регулирования и высокая жёсткость механических характеристик. Недостатками – сложность системы и высокая стоимость, а также сложность реализации в схемах режима рекуперативного торможения.

Каскадные схемы регулирования скорости асинхронного электропривода. Регулирование скорости вращения электродвигателя происходит за счёт введения в роторную цепь добавочной ЭДС, которая может иметь переменную величину и фазу. При этом энергия скольжения в зависимости от вида каскада, электрического или электромеханического, из роторной цепи передаётся либо обратно в питающую сеть, либо на вал двигателя. Достоинствами каскадного способа регулирования являются плавность и точность регулирования. Недостатком – снижение КПД из-за роста потерь в обмотке ротора пропорционально частоте скольжения.

Широтно-импульсное регулирование электроприводов постоянного тока. Данный способ регулирования осуществляется изменением напряжения за счёт использования мостовой схемы включения силовых транзисторных ключей. Достоинством широтно-импульсного регулирования является то, что на выходе преобразователя устанавливается неуправляемый выпрямитель, вследствие чего его $\cos\varphi_1$ (по первой гармонике) близок к единице, а коэффициент мощности будет не ниже 0,95. Недостатком – наличие пульсаций выходного напряжения создаёт необходимость устанавливать фильтры, что вызывает инерционность преобразователя.

Для анализа технического уровня разработок в области создания устройств управления тяговой системой транспортных средств с электротягой изучена патентно-лицензионная ситуация в исследуемой области техники.

Изобретательская активность, показателем которой является количество полученных патентов, является следствием вложения финансовых средств в разработку и может свидетельствовать либо об устранении конкретных технических проблем, либо о появлении новых принципиальных решений [13-17]. Для построения динамических кривых результаты патентных исследований по РФ были проанализированы все патенты за выбранный период времени. Ретроспективность исследования выбрана с 2012 по 2022 год. Такой подход позволяет облегчить сопоставительный анализ по исследуемым объектам, а также оценить перспективы развития каждого из направлений и посмотреть закономерность развития исследуемого объекта по станам. За исследуемый период по объектам было выбрано 10 патентов, которые наиболее соответствовали теме патентных исследований.

Через поисковую базу данных «PATENTSCOPE» (позволяет ознакомиться с полным текстом международных заявок, поданных в соответствии с Договором о патентной кооперации (PCT), с первого дня их публикации, а также с патентными документами национальных и региональных патентных ведомств государств-участников), проведен анализ самого встречающегося индекса международной патентной классификации (МПК) – № B60L15/00 – «Способы, электрические цепи и устройства для управления скоростью вращения тяговых электродвигателей транспортных средств». Найдено 22323 охранных документов, относящихся к данному МПК. На рисунке 1 показано распределение патентных документов по странам, из которого видно, что лидирующие позиции в 2022 году занимает Китай (8849 патентов). Большой объём полученных патентов указывает на то, что направление в улучшении систем управления тяговой системой актуально. Российская Федерация входит в ТОП-10 стран по публикациям изобретений по объекту исследований.

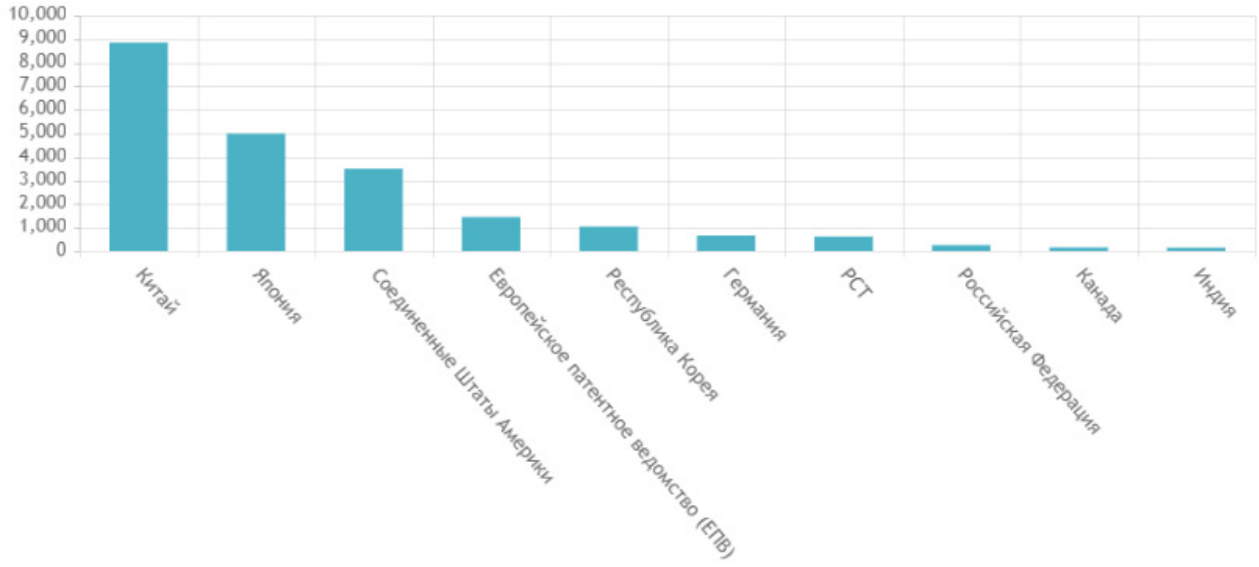


Рис. 1. Количество патентных документов по странам

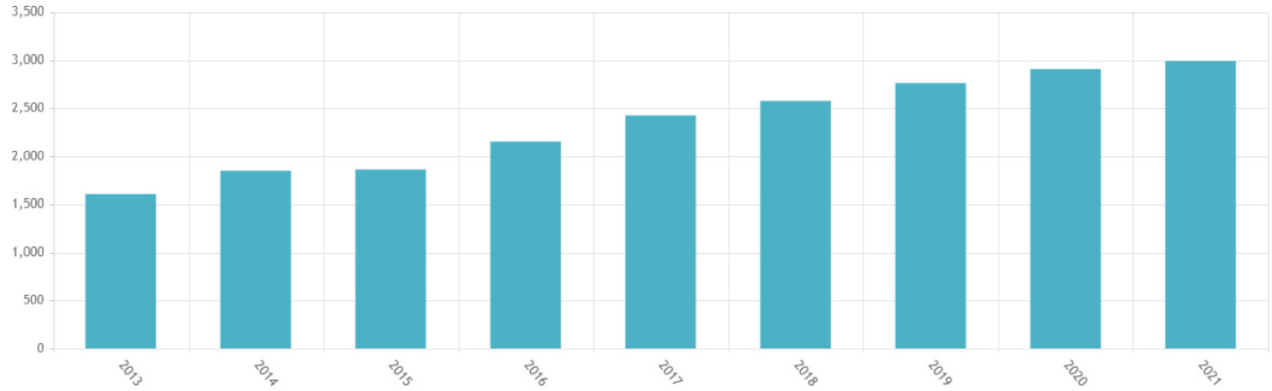


Рис. 2. График количества патентных документов по годам (изобретательская активность)

Можно отметить, что в течение всего рассматриваемого периода происходит рост объёма полученных патентов, что говорит об интересе в разработке данных устройств и актуальности темы применения электрической тяги в транспортных средствах.

В таблице 1 представлены заявители охранных документов имеющих наибольшее количество патентов. Toyota Motor Co является лидером по полученным охранным документам.

Таблица 1

Заявители охранных документов

Наименование организации	Количество документов
TOYOTA MOTOR CO	1128
HONDA MOTOR CO LTD	595
TOYOTA JIDOSHA KABUSHIKI KAISHA	502
NISSAN MOTOR CO LTD	452
HYUNDAI MOTOR COMPANY	416
FORD GLOBAL TECH LLC	373
NTN CO	330
MITSUBISHI ELECTRIC CO	303
DENSO CO	289
KIA MOTORS CO	289

Для определения тенденции развития устройств управления тяговой системой транспортных средств с электротягой рассмотрим несколько патентов на изобретение.

В таблице 2 показано количество полученных патентов по смежным отраслям промышленности, где косвенно могут быть использованы способы, электрические цепи и устройства для управления скоростью вращения тяговых электродвигателей транспортных средств.

Таблица 2

Смежные области патентования

Индекс МПК	**Наименование индекса МПК**	**Количество патентов**
B60L	Способы, электрические цепи и устройства для управления скоростью вращения тяговых электродвигателей транспортных средств	22 328
B60K	Расположение или монтаж силовых установок и трансмиссий транспортных средств; расположение или монтаж нескольких различных первичных двигателей; вспомогательные приводы; контрольно-измерительные приборы и панели управления; устройства и приспособления силовых установок, связанные с охлаждением, забором воздуха, выхлопом газов или подачей топлива в транспортных средствах	5 550
B60W	Комбинированное управление узлами транспортного средства разного типа или функции; системы управления, специально предназначенные для гибридных транспортных средств (с комбинированной силовой установкой); системы управления дорожными транспортными средствами с иными целями, чем управление отдельным узлом	5 083
H02P	Управление или регулирование электрических двигателей, генераторов, электромашинных преобразователей; управление трансформаторами, реакторами или дроссельными катушками	2 386
F16H	Передачи	1 259
B60T	Системы управления тормозами транспортных средств или их элементы; системы управления тормозами или их элементы вообще; размещение тормозных элементов на транспортных средствах вообще; переносные устройства для предотвращения нежелательного движения транспортных средств; модификация транспортных средств для облегчения охлаждения тормозов	1 211
B62D	Сцепные устройства для транспортных средств	1 023
H02J	Схемы или системы питания электросетей и распределения электрической энергии; системы накопления электрической энергии	994
B60R	Транспортные средства, оборудование или конструктивные элементы транспортных средств, не отнесенные к другим подклассам	947
H02K	Электрические машины	879

Рассмотрим патент РФ на изобретение № 2707429. Система управления полноприводным электромобилем.

Система управления полноприводным электромобилем содержит тормозную систему, асинхронные электродвигатели, блоки разделения крутящего момента и блоки управления тягой и стабилизацией [11-12].

Техническим результатом является обеспечение безопасности, устойчивости и проходимости с повышенными возможностями преодоления пути в условиях бездорожья.

Эта цель достигается тем, что в известной системе управления полноприводным электромобилем, содержащей тормозную систему, асинхронные электродвигатели; блоки разделения крутящего момента и блоки управления тягой и стабилизацией, в соответствии с изобретением по крайней мере два асинхронных тяговых электродвигателя интегрированы в колеса транспортного средства по принципу мотор-колеса, блоки разделения крутящего момента, блок управления тягой и стабилизацией интегрированы в контроллеры асинхронных электродвигателей и количество таких контроллеров соответствует количеству применяемых электродвигателей, причем один из контроллеров выполнен мастер-контроллером, обрабатывающим данные с положения рулевой колонки, педалей скорости и тормоза, со всех контроллеров электродвигателей и выдающим сигналы управления на кон-

троллеры электродвигателей, причем мастер-контроллер выполнен с возможностью перевода в ручном переключении на режим бездорожья принудительно вводя электродвигатели в режим синхронизации по крутящему моменту на колесах.

Абсолютный контроль позволяет управлять каждым колесом, как угодно. В частности, реализовывать различные алгоритмы управления, такие как,

1) ABS (Anti-lock Braking System – антиблокировочная система: система, предотвращающая блокировку колёс транспортного средства при торможении).

2) ESP (Electronic Stability Program – Электронный контроль или динамическая система стабилизации автомобиля: активная система безопасности автомобиля, позволяющая предотвратить занос посредством управления компьютером момента силы колеса (одновременно одного или нескольких)).

3) Terrain Control – система адаптации к дорожным условиям (песок, грязь, лед и т.д.).

4) Танковый режим разворота на месте – колеса по разным сторонам (левой и правой) транспортного средства вращаются в разные направления, обеспечивая разворот на месте.

5) И конечно, сама система движения по внедорожью, когда происходит синхронизация по крутящему моменту, обеспечивая таким образом программно одинаковое усилие на всех колесах.

Такой абсолютный контроль позволяет улучшать безопасность (абсолютный контроль при торможении, мгновенное перераспределения усилий на колесах при поворотах) и устойчивость (мгновенная стабилизация при проскальзывании одного из колес или нескольких в миллисекунды).

Рассмотрим ещё один патент РФ на изобретение № 2709639. Способ управления приводом электромобиля и устройство для его осуществления.

Устройство привода электромобиля содержит тяговую аккумуляторную батарею, блок старт-стопа, электродвигатель постоянного тока и реверсор возбуждения, переключатель режима движения, вариатор, главную передачу и блок управления.

Технический результат заключается в упрощении управления приводом электромобиля [4].

Эта цель достигается в следующем. Во всех режимах движения передаточное отношение вариатора в пределах диапазона D его плавного изменения поддерживают обратно пропорциональным сигналу задатчика интенсивности скорости движения. При трогании с места якорь и обмотку возбуждения двигателя подключают к батарее сразу, а в случае движения назад одновременно понижают до требуемого максимальный уровень сигнала задания скорости. При автоматической остановке скорость электромобиля плавно снижают и в момент спада сигнала задания скорости до уровня 1/D двигатель переключают в режим электродинамического торможения, а при спаде сигнала задатчика ниже 0,1/D от аккумуляторной батареи отключают и обмотку возбуждения. При ускоренном торможении дополнительно наращивают темп спада сигнала задания скорости пропорционально положению педали тормоза.

В результате анализа технического достигнутого технического уровня в области создания устройств управления тяговой системой транспортных средств с электротягой, можно сделать вывод о признаках разработок, определяющих их современный научно-технический облик.

Основным направлением разработки, определяющий современный научно-технический облик, можно признать рассмотренные выше патенты на изобретения № 2707429 «Система управления полноприводным электромобилем» и № 2709639 «Способ управления приводом электромобиля и устройство для его осуществления». Данные изобретения позволяют повысить не только безопасность, устойчивость и проходимость с повышенными возможностями преодоления пути в условиях бездорожья, но и упростить управление приводом электромобиля.

По результатам проведённых исследований наблюдается большой объём полученных патентов на разработку устройств управления тяговой системой транспортных средств с электротягой, что указывает на перспективное направление разработки. Принимая во внимание очевидный интерес к этому направления исследований, можно сделать вывод о его актуальности и перспективности дальнейших исследований. Направление исследований следует продолжить в направлении анализа целей (задач, технических результатов) охранных документов для формирования требований к созданию данной продукции по объекту исследований.

Литература

1. *Гулямов К.Х., Гуломзода А.Х.* Разработка и исследование повышающего преобразователя постоянного напряжения // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2017. № 4 (51). С. 55-61.

2. *Карелина М.Ю., Арифуллин И.В., Терентьев А.В.* Аналитическое определение весовых коэффициентов при многокритериальной оценке эффективности автотранспортных средств // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2018. № 1 (52). С. 3-9.

3. *Пузаков А.В., Осаулко Я.Ю.* Исследование влияния эксплуатационных факторов на тепловое состояние автомобильного генератора // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2018. № 1 (52). С. 16-23.

4. *Надараиа Ц.Г., Селиванов А.И., Шестаков И.Я., Фадеев А.А., Бабкина Л.А.* Химико-кинетический накопитель энергии и мотор-редуктор для электромобиля // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2017. № 1 (48). С. 12-17.

5. *Мельникова Т.Е., Мельников С.Е., Завязкина В.В.* Электромобили: перспективы и пути развития // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2019. № 3 (58). С. 22-26.

6. *Блудян Н.О.* Перспективы развития электрических автобусов // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2020. № 3 (62). С. 19-24.

7. *Ухов И.В., Климов А.В., Долгий И.О., Рябцев Ф.А.* Анализ и моделирование алгоритма i2t лимитирования тока для литий-ионных батарей // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2021. № 1 (64). С. 3-10.

8. *Климов А.В., Анисимов В.Р.* О некоторых аспектах повышения энергонасыщенности тяговых электрических двигателей // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). 2021. № 2 (65). С. 26-31.

9. *Ключев В.И.* Теория электропривода: Учеб. для вузов. 2-е изд. перераб. и доп. М.: Энергоатомиздат, 2001. 704 с.

10. *Фираго Б.И., Павлячик Л.Б.* Регулируемые электроприводы переменного тока. Мн.: Техноперспектива, 2006. 363 с.

11. Пат. № 2707429 Российская Федерация, МПК B60L15/20, B60L50/60, B60K7/00. Система управления полноприводным электромобилем / Вагнер Вальдемар Олегович (RU), Щуровский Денис Васильевич (RU); заявитель и патентообладатель Вагнер Вальдемар Олегович (RU), Щуровский Денис Васильевич (RU); заявл. 13.02.2019. опубл. 26.11.2019, Бюл № 33. 15 с.

12. Пат. № 2709639 Российская Федерация, МПК B60L50/60, B60L15/20, B60W10/101, F16H9/02. Способ управления приводом электромобиля и устройство для его осуществления / Аджиманбетов Султанхан Багатович (RU), Хатагов Александр Черменович (RU), Хатагов Заурбек Александрович (RU), Дрияев Тамерлан Вячеславович (RU); заявитель и патентообладатель Федеральное государственное бюджетное образовательное учреждение высшего образования "Горский государственный аграрный университет" (RU); заявл. 30.10.2018. опубл. 19.12.2019, Бюл № 35. 10 с.

13. *Скорняков Э.П., Горбунова М.Э.* Теория и практика патентных исследований. М.: ИНИЦ «ПАТЕНТ», 2014. 208 с.

14. *Дымкова С.С.* Повышение эффективности функционирования информационных систем и процессов в высшей школе // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2017. Т. 6. № 2. С. 45-48.

15. *Дымкова С.С.* Новые принципы организации функционирования систем по продвижению результатов научных исследований // Системы синхронизации, формирования и обработки сигналов. 2017. Т. 8. № 1. С. 34-37.

16. *Дымкова С.С.* Разработка информационной системы для продвижения результатов научных исследований // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 7. С. 38-41.

17. *Артюшенко В.М., Аббасова Т.С., Стреналюк Ю.В., Васильев Н.А., Белюченко И.М., Самаров К.Л., Зиновьев В.Н., Посеренин С.П., Вокин Г.Г., Мороз А.П., Шайдуров В.С., Шаврин С.С.* Системный анализ в области управления и обработки информации. Королев, 2015.