ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.324 DOI: 10.34708/GSTOU. 2022.97.61.006

ОСОБЕННОСТИ ПЕРЕХВАТА ПАКЕТОВ И ИХ ПЕРВОНАЧАЛЬНОГО АНАЛИЗА В СЕТЕВОМ АНАЛИЗАТОРЕ ДАННЫХ ЦИФРОВОЙ ПОДСТАНЦИИ

© П. А. Кокшев[1], Н. А. Галанина[1], Д.Н. Суворов[2], В.И. Марсов[2]
[1]ЧГУ им. И. Н. Ульянова, Чебоксары, Россия
[2]МАДИ, Москва, Россия

Рассматривается необходимость разработки специализированного анализатора данных для высокоавтоматизированных подстанций. Представлены особенности просмотра и первоначального анализа данных, передающихся по сети. Приведен детальный разбор сообщений, передающихся по протоколам GOOSE, MMS и SV согласно IEC 61850. Разработана программа для анализа данных цифровых подстанций с поддержкой идентификации несанкционированных устройств и контроля работы оборудования.

Ключевые слова: IEC61850, высокоавтоматизированные подстанции, IED, GOOSE, MMS, SV, сетевой анализатор.

Введение. Современный мир постепенно движется к полной цифровизации во всех сферах деятельности человека. Это открывает возможности для появления новых технологий, программных продуктов и аппаратно-технических комплексов. В частности, цифровизация в значительной мере влияет на энергетику и активно проявляет себя в самых отдаленных краях земли, вплоть до Арктики [7].

Когда речь заходит о цифровизации в энергетике, не обходится без упоминания относительно новой коммуникационной технологии IEC 61850. Еще недавно темы касательно стандарта IEC 61850 «Сети и системы связи на подстанциях» вызывали оживленные дискуссии. Кто-то видел будущее в этих технологиях, а кто-то считал их бесполезными. Сейчас же все больше специалистов видят перспективы цифровых решений, что приводит к увеличенному спросу на высокоавтоматизированные подстанции.

Появление новых технологий влечет за собой изменение ряда сопутствующих систем, в частности появление новых протоколов передачи данных, для которых начали формироваться новые требования к надежности и производительности системы. Таким образом, появилась необходимость в регистрации информационных потоков на цифровых подстанциях с целью мониторинга состояния оборудования, а также внедрения интеллектуальных сетей [6].

Сетевой анализатор данных. Как известно, за регистрацию информационных потоков в сети отвечает сетевой анализатор, работающий на уровне сетевого адаптера и позволяющий просматривать весь трафик сети. Анализ данных представляет собой процесс обработки всех данных, проходящих через определенный сетевой интерфейс. Применение сетевого анализатора открывает возможности мониторинга сети и анализа всех необходимых данных путем перехвата пакетов, проходящих через эту сеть [1].

В данном случае речь идет о данных, передающихся по сети высокоавтоматизированных (цифровых) подстанций согласно IEC 61850. К таким данным относятся сообщения, передающиеся по протоколам:

- GOOSE (Generic Object Oriented Substation Event – IEC 61850-8-1) – протокол передачи данных о событиях на подстанции; данный протокол используется при передаче дискретных сигналов между устройствами, фактически позволяет заменить медные кабельные связи;
- MMS (Manufacturing Message Specification – IEC 61850-8-1) – протокол передачи данных реального времени и команд диспетчерского управления между сетевыми устройствами и/или программными приложениями, то есть благодаря данному протоколу происходит взаимодействие между SCADA-системой и устройствами РЗА;
- SV (Sampled Values – IEC 61850-9-2) – протокол передачи оцифрованных мгновенных значений от измерительных трансформаторов тока и напряжения. Данный протокол позволяет заменить цепи переменного тока, соединяющие устройства РЗА с трансформаторами тока и трансформаторами напряжения.

В рамках цифровых подстанций сеть разделяется на две шины:

- шина станции (по данной шине передаются сообщения по протоколу MMS и, опционально, по протоколу GOOSE);
- шина процесса (по данной шине передаются сообщения по протоколу SV и, опционально, по протоколу GOOSE).

По какой шине передавать GOOSE-сообщения, решается на этапе проектирования, в частности, это зависит от типа архитектуры, применение которой планируется в рамках реализации подстанции.

Анализ данных. Можно выделить несколько очевидных преимуществ, которые являются результатом анализа данных [2]:

- проверка правильности настройки конфигурации оборудования на подстанции, что дает возможность сразу после интеграции нового оборудования в систему и его запуска проверить соответствие публикуемых им сообщений с файлом конфигурации подстанции, в котором содержится информация обо всех устройствах, их сетевые настройки, а также данные об информационных потоках между этими устройствами;
- выявление некорректной работы сети и оборудования;
- обеспечение безопасности всей системы целиком и сети в частности.

Реализация процесса перехвата и анализа данных. Для перехвата пакетов исполь-

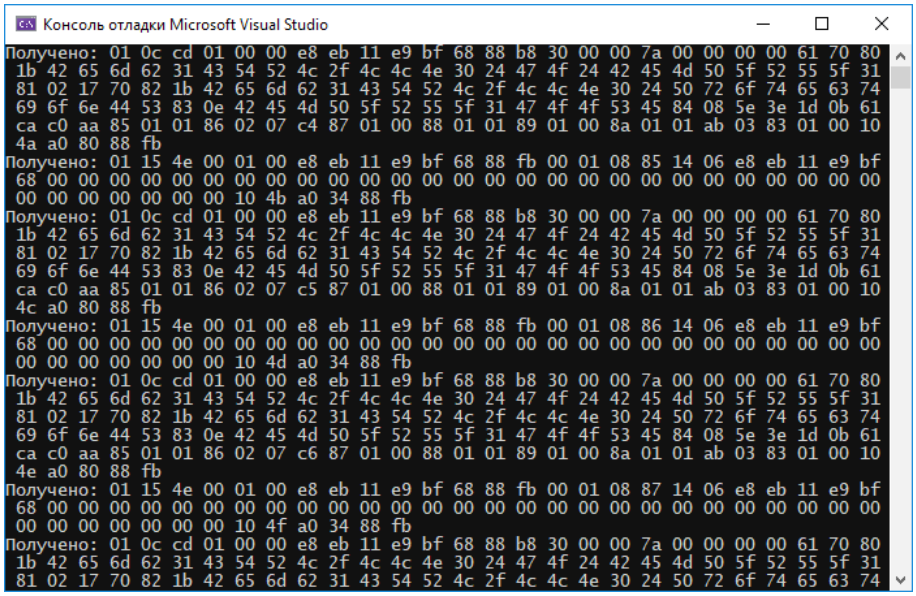

Рис. 1. Данные, полученные сетевой картой без предварительной обработки

зовалась библиотека для.NET, которая называется SharpPcap. Это обертка над библиотекой Pcap, которая позволяет создавать программы для анализа сетевых данных, поступающих на сетевую карту компьютера. Данная библиотека имеет открытый исходный код, ее преимуществом является то, что она является кроссплатформенной, а также имеет высокую производительность.

На рис. 1 представлены данные, полученные путем перехвата данных. Стоит отметить, что это просто поток информации, без какой либо обработки.

При разборе пакетов важно учесть тот факт, что MMS накладывается на уровень TCP, а GOOSE и SV – сразу на канальный уровень. На рис. 2 показано, как данные протоколы накладываются на сетевую модель OSI.

Следовательно, для GOOSE и SV мы должны разбирать все пакеты целиком, а для MMS, к которым относится ReportControl, только ту часть, которая начинается с ip-уровня.

Рассмотрим пример разбора пакета. Согласно рис. 1, GOOSE-сообщение состоит из следующих байт:

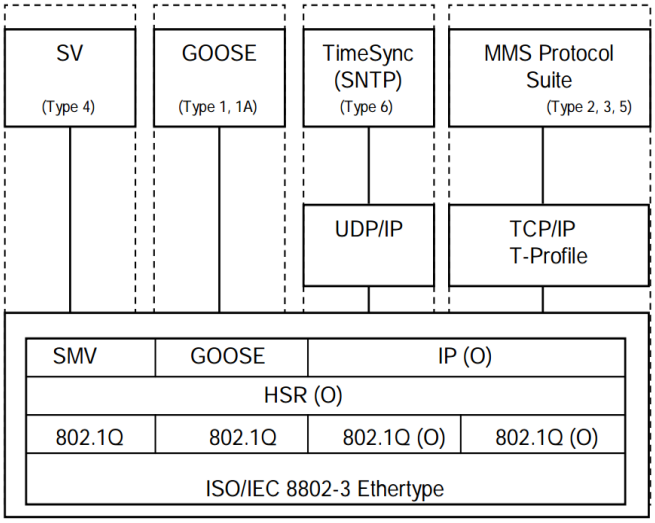

Рис. 2. Наложение протоколов на сетевую модель OSI

010c cd 010000 e8 eb 11 e9 bf 6888 b83000007a 000000006170801b 4265 6d 62314354524c 2f 4c 4c 4e 3024474f 244245 4d 505f 52555f 3181021770821b 4265 6d 62314354524c 2f 4c 4c 4e 302450726f 74656374696f 6e 4453830e 4245 4d 505f 52555f 31474f 4f 534584085e 3e 1d 0b 61 ca c0 aa 850101860207 c4870100880101890100 8a 0101 ab 03830100104a a08088 fb.

В табл. 1 приведен пример разбора GOOSE-сообщения согласно полученным данным.

Таблица 1

Разбор GOOSE-сообщения

Наименование атрибута	Количество байт	Данные
MAC dst	6	010c cd 010000
MAC source	6	e8 eb 11 e9 bf 68
Type (IEC 61850/goose)	2	88 b8
APPID	2	3000
Length	2	007a
Reserved 1	2	0000
Reserved 2	2	0000
goosePdu		
Start	1	61
Length goosePdu	1	70
gocbRef		
Type	1	80
Length gocbref	1	1b
Body	Length gocbref	4265 6d 62314354524c 2f 4c 4c 4e 3024474f 244245 4d 505f 52555f 31

Timeallowedtolive		
Type	1	81
Length	1	02
Body	length	1770
DataSet		
Type	1	82
Length Dataset	1	1b
Body	Length Dataset	4265 6d 6231 4354 524c 2f 4c 4c 4e 3024 5072 6f 7465 6374 696f 6e 4453
GoId		
Type	1	83
Length GoId	1	0e
Body	Length GoID	4245 4d 505f 5255 5f 3147 4f 4f 5345
Time		
Type	1	84
Length Time	1	08
Body	Length Time	5e 3e 1d 0b 61 ca c0 aa
StNum		
Type	1	85
Length StNum	1	01
Body	Length StNum	01
SqNum		
Type	1	86
Length SqNum	1	02
Body	Length SqNum	07 c4
Test		
Type	1	87
Length Test	1	01
Body	Length Test	00
ConfRev		
Type	1	88
Length ConfRev	1	01
Body	Length ConfRev	01
NdsCom		
Type	1	89
Length NdsCom	1	01
Body	Length NdsCom	00
NumDatSetEntries		
Type	1	8a
Length NumDatSetEntries	1	01
Body	Length NumDatSetEntries	01
AllData		
Start	1	ab
Length AllData	1	03
Data		

Type	1	83
Length Data	1	01
Body	Length Data	00
PRP метка	6	104a a08088 fb

Можно заметить, что большая часть сообщения строится по шаблону, приведенному на рис. 3.

В пакетах содержится информация, позволяющая их однозначно идентифицировать. Например, касательно GOOSE-пакетов, к таковым относятся: gocbRef (ссылка на пакет), datSet (имя набора данных), goID (идентификатор пакета) и MAC-адреса источника и приемника сообщения и т. д.

Похожим образом разбираются остальные пакеты в сети, передающиеся по стандарту IEC 61850.

Каждый пакет в сети имеет свой тип – идентификатор и занимает два байта. Благодаря этому можно однозначно определить, сообщение какого типа нам предстоит обрабатывать. В табл. 2 представлены идентификаторы пакетов, которые передаются согласно интересующим нас протоколам.

Без сомнения, в сети подстанции могут быть и будут другие типы пакетов, но детально анализировать каждый из них нет необходимости. Однако в рамках информационной безопасности подстанции данные пакеты нам тоже интересны. Эта тема будет затронута в следующей статье, а пока рассмотрим файл конфигурации подстанции.

Необходимость файла конфигурации подстанции. Файл конфигурации подстанции (SCL) содержит практически всю информацию о высокоавтоматизированной подстанции [4]. Следовательно, в нем также содержится информация обо всех информационных потоках, откуда мы можем получить необходимые нам сведения, а именно:

- сетевые параметры интеллектуального устройства (IED);
- параметры GSEControl;
- параметры SampledValueControl;
- параметры ReportControl;
- наборы данных и атрибуты, из которых они состоят.

В некоторых случаях SCL файлы также содержат в себе параметры клиентов, что дает возможность четко регламентировать количество всех возможных устройств в рамках подстанции.

Объектная модель SCL имеет три основные части:

Рис. 3. Структура данных APDU

Таблица 2

Идентификаторы протоколов

Тип идентификатора	Протокол
0x88b8	GOOSE
0x88ba	Sampled Values
0x0800	IPv4 (MMS)

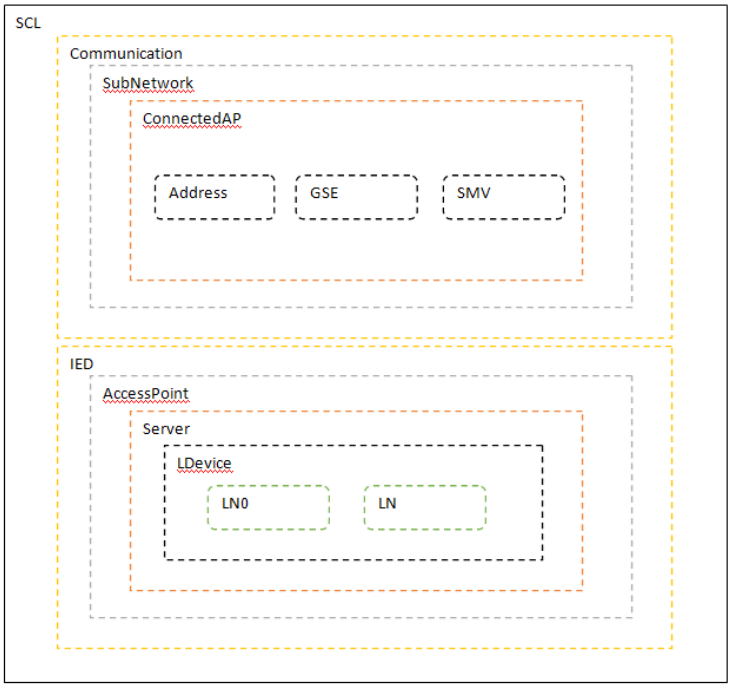

Рис. 4. Структура данных APDU

- Substation;
- IED;
- Communication.

На рис. 4 представлена структура SCL файла.

Блок Communication содержит типы объектов, относящиеся к связи, то есть подсеть (SubNetwork) и точки доступа к среде передачи (ConnectedAP), а также данные о коммуникационных соединениях между различными интеллектуальными электронными устройствами (IED), описание которых содержится в файле конфигурации подстанции.

SubNetwork – определяет принадлежность устройства к определенной шине данных на подстанции.

ConnectedAP – узел, содержащий в себе сетевые параметры интеллектуального устройства, такие как: IP-адрес, маска подсети и шлюз. В этом же узле содержатся сетевые параметры GSE с SMV. В то же время все остальные параметры GSEControl, SampledValueControl и ReportControl описываются в блоке IED.

IED – устройство автоматизации подстанции, является описанием реального устройства подстанции. С другими IED-устройствами в составе системы автоматизации оно обычно связывается через систему связи Communication.

Access point – коммуникационная точка доступа логического устройства (устройств) IED к подсети. Представляет собой ссылку на ConnectedAP, объявленную в узле Communication.

Server – связующий объект в IED-устройстве согласно серии стандартов МЭК 61850-7. Через систему связи и ее единственную точку доступа он обеспечивает доступ к данным LD и LN, содержащимся в устройстве.

LDevice – логическое устройство. Как видно на рис. 4, оно содержит в себе обязательный узел с именем LN0 и другой узел LN, имя которого может быть любым. Узлов LN в одном логическом устройстве может быть несколько.

LNO – обязательный узел, который есть в каждом логическом устройстве. Из интересующих нас данных он содержит ReportControl, GSEControl, SampledValueControl и DataSet.

Рассмотрим для примера GSEControl, который представляет собой блок GOOSE-сообщения, которое передается от одного устройства РЗА к другому и содержит следующие атрибуты:

- Name – имя goose-сообщения;

- Имя LD – имя логического устройства;
- Имя LN – имя логического узла;
- Имя DataSets – имя набора данных;
- ConfRev – версия конфигурации;
- appID – период сохранности, время отправки отчета;
- VLANID – идентификатор отчета;
- MAC-address;
- APPID;
- MaxTime / MinTime;
- данные.

SampledValueControl практически идентичен GSEControl, за исключением нескольких параметров. В свою очередь, ReportControl по структуре совершенно другой и содержит куда больше параметров, которые в том числе могут быть динамически настроены клиентом (например SCADA-системой).

Далее путем сравнивания параметров полученных пакетов с данными из SCL-файла, можно проверять корректность настройки IED (соответствует ли его конфигурация конфигурации подстанции) и отлавливать неправильные пакеты, а также пакеты с некорректными значениями.

Результаты. Была успешно разработана программа, позволяющая значительно ускорить настройку и интеграцию новых цифровых устройств в высокоавтоматизированных подстанциях, а также просматривать состояние подключенного оборудования. С помощью разработанной программы можно идентифицировать неправильную работу устройств и возможные несанкционированные срабатывания. Программа была проверена путем проведения испытаний в лаборатории цифровой подстанции компании АО «ЧЭАЗ» и в ходе проведения пусконаладочных работ реальных подстанций.

Следующим шагом является интеграция в данную программу нейросетевых алгоритмов, с помощью которых в будущем появится возможность не только идентификации неправильных срабатываний, но и противодействия им, поддержания стабильности сети и эмуляции различных режимов работы [3,5].

ЛИТЕРАТУРА

1. *Кокшев П. А.* Анализ готовых решений для сетевого анализатора данных высокоавтоматизированной подстанции / П. А. Кокшев, Н. А. Галанина // Информационные технологии в электротехнике и электроэнергетике: материалы XIII-й Всерос. науч.-техн. конф. Чебоксары: Изд-во Чуваш. ун-та, 2022. С. 296-297.
2. *Кокшев П. А.* Особенности применения сетевого анализатора данных в цифровой подстанции и его возможности / П. А. Кокшев, Н. А. Галанина // Проблемы и перспективы развития энергетики, электротехники и энергоэффективности: материалы V Междунар. науч.-техн. конф. Чебоксары: Изд-во Чуваш. ун-та, 2021. С. 93-96.
3. *Кокшев П. А.* Применение нейросетевых алгоритмов обнаружения вторжений для сетевого анализатора данных цифровой подстанции / П. А. Кокшев // Современные тенденции развития цифровых систем релейной защиты и автоматики: материалы науч.-техн. конф. молодых специалистов форума «РЕЛАВЭКСПО-2021». Чебоксары: Изд-во Чуваш. ун-та, 2021. С. 199-203.
4. *Кокшев П. А.* Применение стандарта МЭК 61850 для систем автоматизированного проектирования цифровых подстанций / П. А. Кокшев, Д. А. Удиков, Д. Г. Мухин // Сборник докладов научно-технической конференции. Чебоксары: Изд-во Чуваш. ун-та, 2019. С. 178-183.
5. *Кокшев П. А.* Преимущества применения нейронной сети с архитектурой многослойного персептрона для сетевого анализатора данных цифровой подстанции / П. А. Кокшев, Н. А. Галанина // Динамика нелинейных дискретных электротехнических и электронных систем: Материалы XIV Всерос. науч.-техн. конф. Чебоксары: Изд-во Чуваш. ун-та, 2021. С. 127-129.
6. *Амхаев Т. Ш.* Повышение качества электроэнергии внедрением интеллектуальных сетей / Т. Ш. Амхаев, М. В. Дебиев, У. И. Абдулхакимов, У. Р. Асхабов // Вестник ГГНТУ. Технические науки. Том XVIII. № 1 (27). 2022. С. 5-10.

7. *Азиева Р. Х.* Новые горизонты: цифровые технологии в Арктике / Азиева Р. Х., Абуев А. И., Якубов Т. В. // Приоритетные направления инновационной деятельности в промышленности. Сборник научных статей X Международной научной конференции. Казань: Изд-во: ООО «Конверт», 2021. С. 92-98.

FEATURES OF PACKET CAPTURE AND THEIR INITIAL ANALYSIS IN THE NETWORK DATA ANALYZER OF THE DIGITAL SUBSTATION

© P. A. Kokshev[1], N. A. Galanina[1], D. N. Suvorov[2], V. I. Marsov[2]
[1]ChSU named after I. N. Ulyanov, Cheboksary, Russia
[2]MRI, Moscow, Russia

The necessity of developing a specialized data analyzer for highly automated substations is considered. The features of viewing and initial analysis of data transmitted over the network are presented. A detailed analysis of messages transmitted via the GOOSE, MMS and SV protocols according to IEC 61850 is given. A program has been developed for analyzing data from digital substations with support for identifying unauthorized devices and monitoring equipment operation.

Keywords: IEC61850, highly automated substations, IED, GOOSE, MMS, SV, network analyzer.

REFERENCES

1. Kokshev, P. A. and Galanina' N. A. (2022) Analiz gotovykh reshenii dlya setevogo analizatora dannykh vysokoavtomatizirovannoi podstantsii. Informatsionnye tekhnologii v elektrotekhnike i elektroenergetike: materialy XIII-i Vseros. nauch.-tekhn. konf. [Analysis of ready-made solutions for a network data analyzer of a highly automated substation'. *Information technologies in electrical engineering and electric power industry: materials of the XIII All-Russian Scientific and Technical conf.*]. [CHGU Bulletin] pp. 296-297.
2. Kokshev, P. A. and Galanina, N. A. (2021) Osobennosti primeneniya setevogo analizatora dannykh v tsifrovoi podstantsii i ego vozmozhnosti. Problemy i perspektivy razvitiya energetiki, elektrotekhniki i energoeffektivnosti: materialy V Mezhdunar. nauch.-tekhn. konf. [Features of using a network data analyzer in a digital substation and its capabilities'. *Problems and prospects for the development of energy, electrical engineering and energy efficiency: materials of the V International Scientific and Technical. conf.*]. [CHGU Bulletin. Technical Sciences] pp. 93-96.
3. Kokshev, P. A. (2021) Primenenie neirosetevykh algoritmov obnaruzheniya vtorzhenii dlya setevogo analizatora dannykh tsifrovoi podstantsii. Sovremennye tendentsii razvitiya tsifrovykh sistem releinoi zashchity i avtomatiki: materialy nauch.-tekhn. konf. molodykh spetsialistov foruma «RELAVEKSPO-2021». [Application of neural network intrusion detection algorithms for a network data analyzer of a digital substation'. *Modern trends in the development of digital relay protection and automation systems: materials of scientific and technical conf. of young specialists of the forum "RELAVEXPO-2021"*]. [CHGU Bulletin. Technical Sciences] pp. 199-203.
4. Kokshev, P. A., Udikov, D. A. and Mukhin, D. G. (2019) Primenenie standarta MEK 61850 dlya sistem avtomatizirovannogo proektirovaniya tsifrovykh podstantsii. Sbornik dokladov nauchno-

tekhnicheskoi konferentsii. [Application of the IEC 61850 standard for computer-aided design systems of digital substations'. *Collection of reports of the scientific and technical conference*]. [CHGU Bulletin] pp. 178-183.

5. Kokshev, P. A. and Galanina, N. A. (2021) Preimushchestva primeneniya neironnoi seti s arkhitekturoi mnogosloinogo perseptrona dlya setevogo analizatora dannykh tsifrovoi podstantsii. Dinamika nelineinykh diskretnykh elektrotekhnicheskikh i elektronnykh sistem: materialy XIV Vseros. nauch.-tekhn. konf. [Advantages of using a neural network with a multilayer perceptron architecture for a network data analyzer of a digital substation'. *Dynamics of nonlinear discrete electrical and electronic systems: materials of the XIV All-Russian Scientific and Technical conf.*]. [CHGU Bulletin] pp. 127-129.
6. Amkhaev, T. S., Debiev, M. V., Abdulkhakimov, U. I. and Askhabov, U. R. (2022) Povyshenie kachestva elektroenergii vnedreniem intellektual'nykh setei. [Improving the quality of electricity by the introduction of intelligent networks]. *Vestnik GGNTU. Technical Sciences*. [Vestnik GGNTU. Technical Sciences. Volume XVIII]. № 1 (27), pp. 5-10.
7. Azieva, R. H., Abuev, A. I. and Yakubov, T. V. (2021) Novye gorizonty: tsifrovye tekhnologii v Arktike. Prioritetnye napravleniya innovatsionnoi deyatel'nosti v promyshlennosti. Sbornik nauchnykh statei X mezhdunarodnoi nauchnoi konferentsii. [New horizons: digital technologies in the Arctic'. *Priority directions of innovation activity in industry. Collection of scientific articles of the X International Scientific Conference*.]. [Publishing House: LLC "Konvert"], pp. 92-98.