DOI 10.37882/2223-2966.2023.6-2.36

АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ПОЛЕЗНОЙ НАГРУЗКИ И КЛЮЧЕВОЙ ИНФОРМАЦИИ НА ОСНОВЕ ШИФРА ВЕРНАМА И КОМПОЗИЦИОННОГО ШИФРА

ALGORITHM OF CRYPTOGRAPHIC TRANSFORMATION OF PAYLOAD AND KEY INFORMATION BASED ON VERNAM CIPHER AND COMPOSITE CIPHER

S. Tarasenko

Summary: This paper presents an algorithm for cryptographic transformation of the payload and key information based on the Vernam cipher and a composite cipher. The proposed algorithm implements the division of the key distributed between the parties into two components. The first component has the resistance to cryptanalysis inherent in data encrypted using the Vernam cipher, and the second one has the resistance characteristic of the fundamental principles of ensuring durability — random scattering and random mixing. The cryptographic strength of the first component is much greater than the strength of the second. Thus, the durability of the data encrypted using the proposed algorithm will be no less than the durability of the data encrypted using random scattering and mixing.

Keywords: Vernam cipher, composite cipher, cryptographic strength, cryptanalysis, encryption.

Тарасенко Сергей Сергеевич
сотрудник,
Академия ФСО России, г. Орёл
dor7la96@mail.ru

Аннотация. В данной работе представлен алгоритм криптографического преобразования полезной нагрузки и ключевой информации на основе шифра Вернама и композиционного шифра. В предлагаемом алгоритме реализовано деление распределяемого между сторонами ключа на две составляющие. Первая составляющая имеет стойкость к криптоанализу, присущую данным, зашифрованным с использованием шифра Вернама, а вторая — стойкость, характерную для фундаментальных принципов обеспечения стойкости — случайных рассеиваний и случайных перемешиваний. Криптостойкость первой составляющей много больше стойкости второй. Таким образом, стойкость данных, зашифрованных с использованием предлагаемого алгоритма, будет не менее, чем стойкость данных, зашифрованных с использованием *случайных* ***рассеиваний и перемешиваний***.

Ключевые слова: шифр Вернама, композиционный шифр, криптографическая стойкость, криптоанализ, шифрование.

Введение

Шифр Вернама имеет абсолютную криптографическую стойкость [1]. Однако его использование ограничено в связи с необходимостью генерации ключей большого размера и со сложностью распределения ключевой информации между корреспондентами. В связи с этим широкое распространение получили криптосистемы, базирующиеся на блочных [2] и/или поточных шифрах [3]. Но для большого количества ранее созданных алгоритмов были найдены способы снижения стойкости к криптоанализу в результате выявления слабых мест в алгоритме или в результате появления новых эффективных методов криптоанализа.

Вероятность снижения криптографической стойкости с течением времени подтверждает актуальность задачи проектирования алгоритма криптографических преобразований, стойкость которого базируется не на определенной реализации блочного или поточного шифра, а на сложности фундаментальных математических задач и длине используемого ключа.

Предлагаемый в данной работе алгоритм позволяет обеспечить *заданную* стойкость, устраняя риски *вероятного снижения* стойкости при использовании *блочных шифров*.

Для пояснения предлагаемого алгоритма необходимо ввести ряд обозначений.

Key_info — ключевая информация, необходимая для осуществления коммуникации между сторонами. *Key_info* состоит из:

1) одноразового ключа *OTK*, являющегося случайной последовательностью бит длиной W, сгенерированной генератором случайных чисел (ГСЧ) [4];
2) ключа *mac_generation_key* и *IV_mac* для выработки имитовставки [5];
3) ключа *permutations_generation_key* и *IV_permut* для осуществления перестановок местоположения имитовставки в очередном сообщении зашифрованного на шифре Вернама текста;
4) параметров *parameters*:
   — *L_mac* — длина имитовставки, генерируемой с использованием mac_generation_key;
   — *mac_key_generation_rule* — правило выработки ключей mac_key для формирования имитовставки очередного сообщения (например, блочный шифр в режиме простой замены (англ. *Electronic*

Codebook, ECB), описанный в ГОСТ Р 34.13-2015 [6]), в качестве первоначального открытого текста которому подается последовательность *IV_mac*, а в последующем — сформированный для предыдущего зашифрованного на шифре Вернама текста ключ выработки имитовставки *mac_key*, а в качестве ключа для выработки ключей *mac_key* используется ключ *mac_generation_key*);
- *mac_rule* — правило выработки имитовставки (например, блочный шифр в режиме выработки имитовставки (англ. *Message Authentication Code algorithm*)), описанный в ГОСТ Р 34.13-2015 [6];
- *L_key_permutations* — длина ключа перестановок, генерируемого с использованием *permutations _genaration_key*;
- *permutations_key_generation_rule* — правило выработки ключей *P_key* для перестановок местоположения имитовставок для очередных сообщений (например, блочный шифр в режиме простой замены, описанный в ГОСТ Р 34.13-2015, в качестве первоначального открытого текста которому подается последовательность *IV_permut*, а в последующем — сформированный для предыдущего зашифрованного текста и имитовставки ключ перестановки *P_key*, а в качестве ключа для выработки ключей *P_key* используется ключ *permutations_genaration_key*);
- *CRC* — вариант алгоритма нахождения контрольной суммы [7];
- *L_block_cipher* — длина ключа для блочного шифра;
- *R* и *G* — целые положительные числа, выбираются в зависимости от необходимой *заданной* стойкости криптосистемы. На основе их рассчитывается *L_for_transfer_new_OTK* — оставшаяся неиспользованной длина одноразового ключа ОТК, при достижении которой стороны должны использовать ее для обмена новой ключевой информацией.

spent_key_len — израсходованная на текущий момент длина ключа *OTK*.

MAC — имитовставка для зашифрованного сообщения *Encrypt_message*.

Transmit message — передаваемое сообщение, включающее в себя перемешанные с использованием операции перестановки *permutation* и ключа перестановки *P_key* биты зашифрованного сообщения *Encrypt_message* и биты имитовставки *MAC*.

checksum_OTK — контрольная сумма от *OTK* с использованием *CRC*.

block_cipher_key — ключ шифрования для блочного шифра, на котором осуществляется шифрование *OTK*.

IV_block_cipher — вектор инициализации [8] для блочного шифра.

Encrypt_OTK — зашифрованный на блочном шифре *OTK*.

key_M — содержит в себе информацию о местоположении *M* частей *M_pieces*, которые будут извлечены из исходных *N* частей *N_pieces*.

P_k_nm — блок перестановки (*P*-блок) [9].

P_k_nm_compress — блок перестановки, сформированный на основе *P_k_nm* (*P*-блок сжатия);

K_pieces — *K* ложных частей *K_pieces*, представляющих собой случайные последовательности бит.

M_Pieces — извлеченные *M* случайных частей *M_pieces* из *N* частей *N_pieces* с использованием ключа *key_M*;

NM_pieces — (*N*–*M*) оставшихся частей из *N* частей *N_pieces* после извлечения *M* частей;

NMK_pieces — результат конкатенации *NM_pieces* и *K_pieces*;

R_permut — результат применения операции перестановки *permutation* к *NMK_pieces* в соответствии с блоком перестановки *P_k_nm* (*R* = (*N*–*M*)+*K* перемешанных частей);

info_repair — набор данных, позволяющий восстановить *Encrypt_OTK* из *R_permut*, который включает в себя: *M_pieces*, *key_M*, *P_k_nm_compress*.

file_ref — набор данных, содержащий: *info_repair*, *block_cipher_key*, *IV_block_cipher*, *checksum_OTK*, *mac_ generation_key*, *IV_mac*, *permutations_generation_key*, *IV_ permut*, *parameters*.

На рисунке 1 проиллюстрирована блок-схема алгоритма криптографического преобразования полезной нагрузки и ключевой информации на основе шифра Вернама и композиционного шифра.

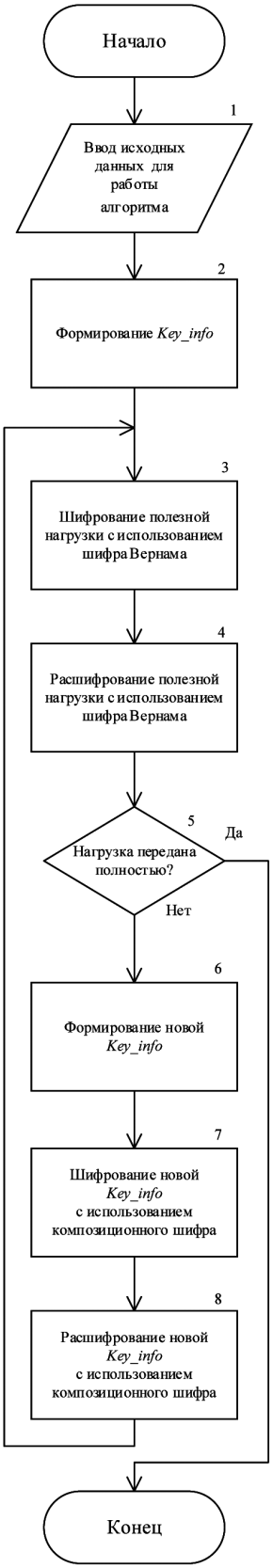

Рис. 1. Блок-схема алгоритма криптографического преобразования полезной нагрузки и ключевой информации на основе шифра Вернама и композиционного шифра

На рисунке 2 представлен в развернутом виде шаг 1 «Ввод исходных данных для работы алгоритма».

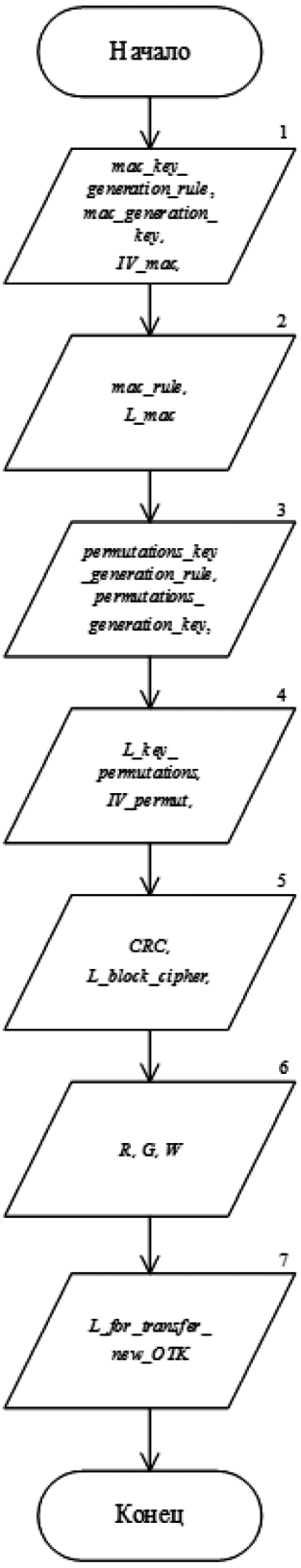

Рис. 2. Блок-схема алгоритма ввода исходных данных для работы общего алгоритма

Шаг 2 «Формирование ключевой информации *Key_info*» заключается в упаковке входных данных алгоритма в единую логическую структуру и в пояснении не нуждается.

На рисунке 3 представлен в развернутом виде шаг 3 «Шифрование полезной нагрузки с использованием шифра Вернама» предлагаемого алгоритма.

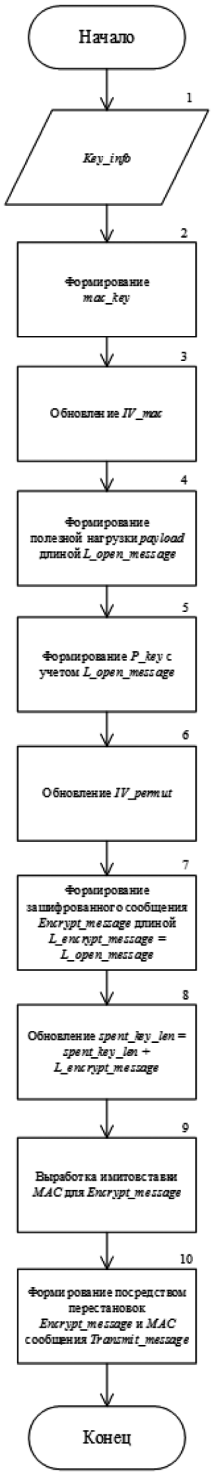

Рис. 3. Блок-схема алгоритма шифрования полезной нагрузки с использованием шифра Вернама

На рисунке 4 представлен в развернутом виде шаг 4 «Расшифрование полезной нагрузки с использованием шифра Вернама» предлагаемого алгоритма.

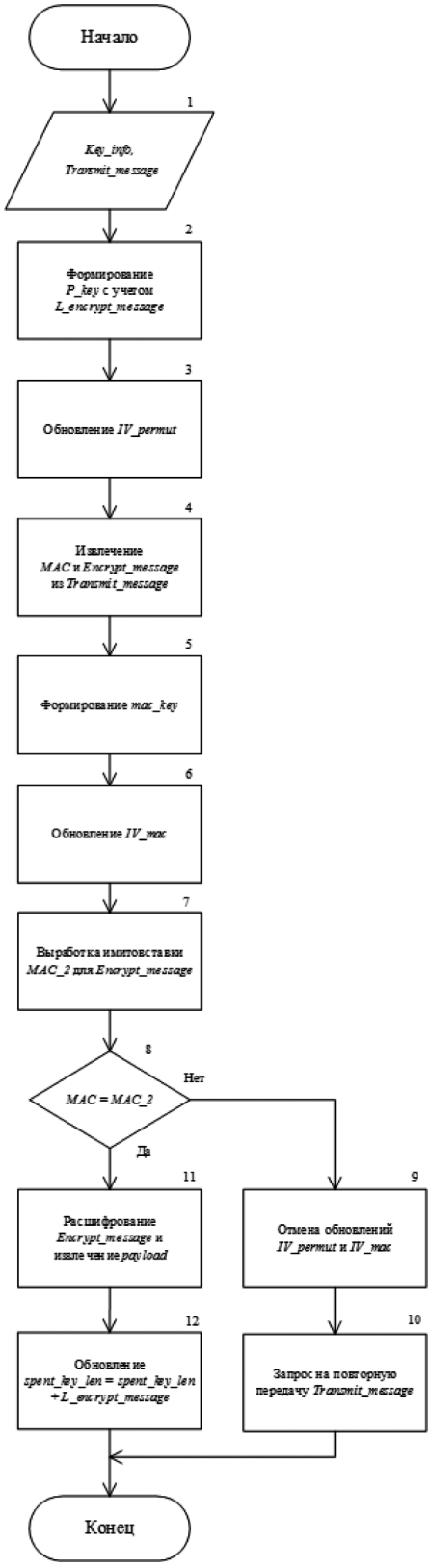

Рис. 4. Блок-схема алгоритма расшифрования полезной нагрузки с использованием шифра Вернама

На шаге 5 осуществляется проверка того, полный ли объем полезной нагрузки передан. Если да, то алгоритм завершает выполнение. Если нет, то происходит обновление ключевой информации, содержащейся у сторон, и продолжается передача полезной нагрузки.

Шаг 6 аналогичен шагу 2.

На рисунке 5 представлен в развернутом виде шаг 7 «Шифрование новой ключевой информации *Key_info* с использованием композиционного шифра» предлагаемого алгоритма.

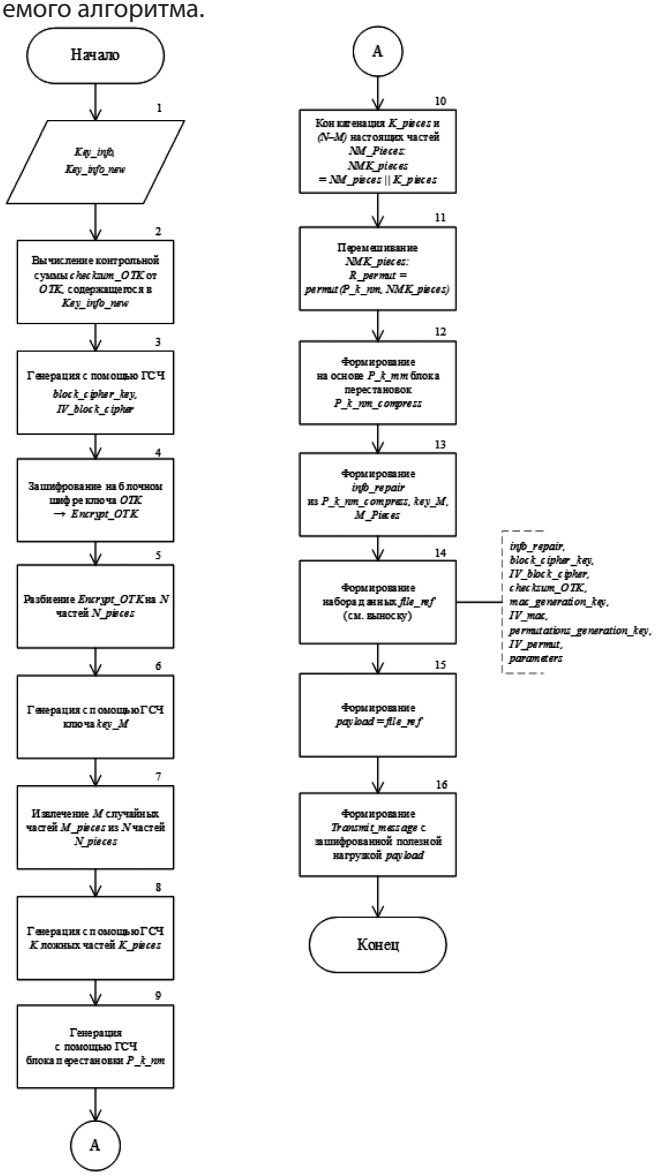

Рис. 5. Блок-схема алгоритма шифрования новой ключевой информации *Key_info* с использованием композиционного шифра

На рисунке 6 представлен в развернутом виде шаг 8 «Расшифрование новой ключевой информации *Key_info* с использованием композиционного шифра» предлагаемого алгоритма.

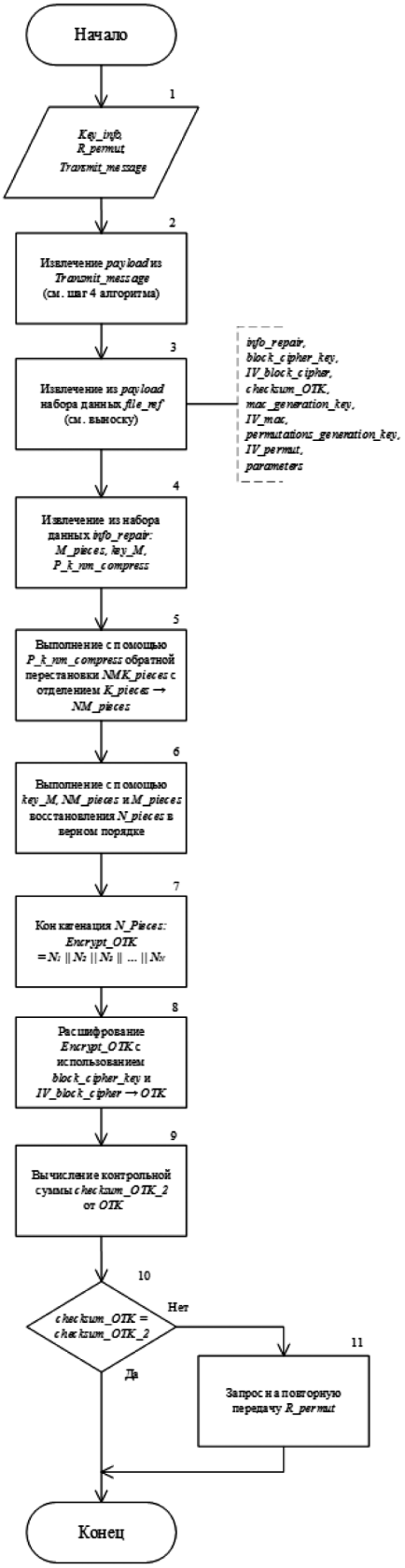

Рис. 6. Блок-схема алгоритма расшифрования новой ключевой информации Key_info с использованием композиционного шифра

Предлагаемый алгоритм соответствует следующим требованиям, предъявляемым к алгоритмам:

— понятность (каждое из действий и алгоритм в целом реализуем исполнителем (ЭВМ));
— дискретность (состоит из упорядоченного выполнения простых шагов);
— конечность (каждое из действий и весь алгоритм в целом обязательно завершаются);
— детерминированность (однозначное получение результата при заданных исходных данных);
— результативность (алгоритм прекращается за конечное число шагов с определенным результатом);
— массовость (возможность использования различных исходных данных).

Заключение

Использование алгоритма криптографического преобразования полезной нагрузки и ключевой информации на основе шифра Вернама и композиционного шифра, представленного в данной работе, в долгосрочной перспективе обеспечивает заданную стойкость зашифрованных данных к криптоанализу [10] при выполнении требований по управлению ключами для шифра Вернама [11]. Постоянство стойкости основывается на доказанной абсолютной стойкости шифра Вернама и операциях случайных рассеиваний (англ. *Diffusion*) и *случайных* перемешиваний (англ. *Confusion*) [12], в отличие от аналогичных операций, используемых в *блочных шифрах*, где они имеют *псевдослучайный* [13] характер.

ЛИТЕРАТУРА

1. Shannon, C.E. (1948) A Mathematical Theory of Communication. Bell System Technical Journal, 27, 379–423.
2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии — 3-е изд. — М.: Диалог-МИФИ, 2011. — 176 с. — ISBN 978-5-9912-0182-7.
3. Габидулин Э.М., Кшевецкий А.С., Колыбельников А.И. Защита информации: учебное пособие — М.: МФТИ, 2011. — 225 с. — ISBN 978-5-7417-0377-9.
4. Lemire, Daniel (23 February 2019). «Fast Random Integer Generation in an Interval». ACM Transactions on Modeling and Computer Simulation. 29 (1): 1–12. arXiv:1805.10941. doi:10.1145/3230636. S2CID 44061046.
5. ISO/IEC 9797-1 Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.
6. ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».
7. T.V. Ramabadran, S. S. Gaitonde. A tutorial on CRC computations // IEEE Micro. — 1988. — Т. 8, № 4. — С. 62–75.
8. Menezes, van Oorschot, Vanstone. Chapter 7: Block Ciphers // Handbook of Applied Cryptography — CRC Press, 1996. — ISBN 0-8493-8523-7.
9. Брюс Шнайер. «Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си». — М.: Триумф, 2002. — ISBN 5-89392-055-4.
10. Junod, Pascal; Canteaut, Anne (2011). Advanced Linear Cryptanalysis of Block and Stream Ciphers. IOS Press. ISBN 978-1-60750-844-1.
11. The Venona Translations. The Venona Story. Fort Meade, Maryland: National Security Agency. 2004-01-15. p. 17th.
12. Shannon, C.E. (October 1949). «Communication Theory of Secrecy Systems*». Bell System Technical Journal. 28 (4): 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x.
13. R.S. Wikramaratna. ACORN — A new method for generating sequences of uniformly distributed Pseudo-random Numbers // Journal of Computational Physics. — 1989-07. — Т. 83, вып. 1. — С. 16–31. — ISSN 0021-9991. — doi:10.1016/0021-9991(89)90221-0.

Журнал «Современная наука: актуальные проблемы теории и практики»