

**ИНФОРМАТИКА**

doi: 10.51639/2713-0576\_2021\_1\_2\_50

УДК 004.056.55

ГРНТИ 20.53.23

ВАК 05.13.19

**Программно-информационный комплекс защищенной передачи данных**<sup>1</sup> Бистерфельд Н. С., <sup>2\*</sup> Бистерфельд О. А.<sup>1</sup> МИРЭА – Российский технологический университет, 119454, ЦФО, г. Москва, пр. Вернадского, д. 78<sup>2</sup> СОШ № 66 г. Пензы им. В. А. Стукалова, 440013, г. Пенза, ул. Светлая, д. 1бemail: [bist18@yandex.ru](mailto:bist18@yandex.ru) , \* [bist19@yandex.ru](mailto:bist19@yandex.ru)

С целью повышения уровня защиты сетевой передачи данных в виде файлов предлагается использовать программно-информационный комплекс защищенной передачи данных. Комплекс включает: программно-информационный компонент «Генератор перестановок», программы «Преобразование файла» и «Дешифрование файла». С помощью программно-информационного компонента «Генератор перестановок» формируются последовательности перестановок, в соответствии с которыми проводится преобразование передаваемого файла (на передающей стороне) и дешифрование файла (на приемной стороне). В пределах размера группы меняются позиции передаваемых в канал связи бит. Предлагается ввести многократную и автоматическую смену правил преобразования файла. Чередование перестановок в последовательности зависит от алгоритма генерации. Реализованы несколько алгоритмов. Внедрение программно-информационного комплекса защищенной сетевой передачи данных между устройствами позволит существенно сократить затраты системных администраторов защиты данных и повысить уровень защищенности передаваемых данных.

*Ключевые слова:* информационная безопасность, передача данных, шифрование, метод перестановки.

**Введение**

Одним из отрицательных явлений развивающейся в настоящий период цифровизации экономики являются разнообразные киберпреступления. Борьба с киберпреступностью объявляется государственной политикой, предпринимаются активные действия, выделяются громадные финансовые ресурсы по недопущению несанкционированного доступа к данным на уровне значимых предприятий и организаций различных форм собственности. Проводятся попытки организации согласованной политики по борьбе с киберпреступностью на международном уровне. Несанкционированный доступ к разнообразным данным возможен и при передаче данных. Такой вид преступлений является одним из самых распространенных. Как правило, для передачи данных создаются организационно-технические системы разной сложности, в которых важной составной частью является персонал. Перед персоналом ставятся сложные задачи по защите от несанкционированного доступа, и снижение затраты персонала на осуществление защищенных передач данных также актуально. С целью повышения уровня защиты сетевой передачи данных в виде файлов предлагается использовать программно-информационный комплекс защищенной

передачи данных. Предлагаемый комплекс включает: программно-информационный компонент «Генератор перестановок» (КГП), программы «Преобразование файла» и «Дешифрование файла». С помощью КГП формируются последовательности перестановок, в соответствии с которыми проводится преобразование передаваемого файла (на передающей стороне) и восстановление файла (на приемной стороне).

### **Программно-информационный компонент «Генератор перестановок»**

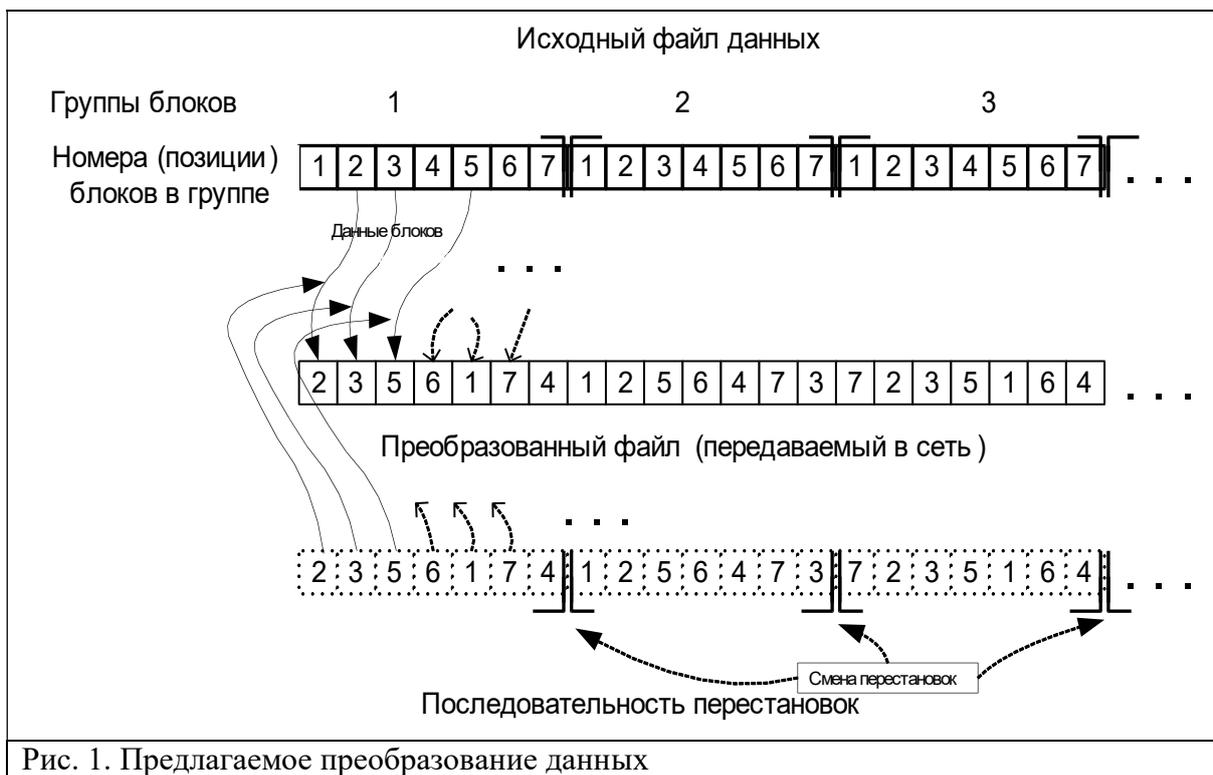
Генерация перестановок широко известная процедура (например, [2]). Однако, в предлагаемом подходе необходимы частые и автоматические процедуры использования целого ряда различных последовательностей перестановок. В связи с этим предлагается реализовать генератор перестановок в виде небольшой базы данных, позволяющей как генерировать последовательности в соответствии с идентификаторами на используемые алгоритмы, так и сохранять и предоставлять сгенерированные последовательности перестановок.

Генератор перестановок предлагается использовать в средствах защищенной передачи данных по вычислительным сетям. Как вариант скрытия передаваемых данных могут быть использованы перестановки блоков передаваемых данных (групп символов). При выборе размера блока данных не кратного размеру данных, представляющих символы, преобразовываются и символы передаваемых данных, что повышает уровень защищенности при передаче в сети. В таких средствах необходим генератор перестановок как на передающей стороне (для перестановок символов или групп символов в передаваемых по сети данных), так и на приемной стороне (для восстановления принимаемых данных). Генераторы на передающей и на приемной стороне должны формировать одинаковую последовательность перестановок.

Для усложнения несанкционированного доступа к данным периодически необходимо менять используемую последовательность перестановок (одна из задач персонала).

В разработанном действующем прототипе генератора перестановок максимально возможный размер группы равен 10. При необходимости размер группы может быть увеличен.

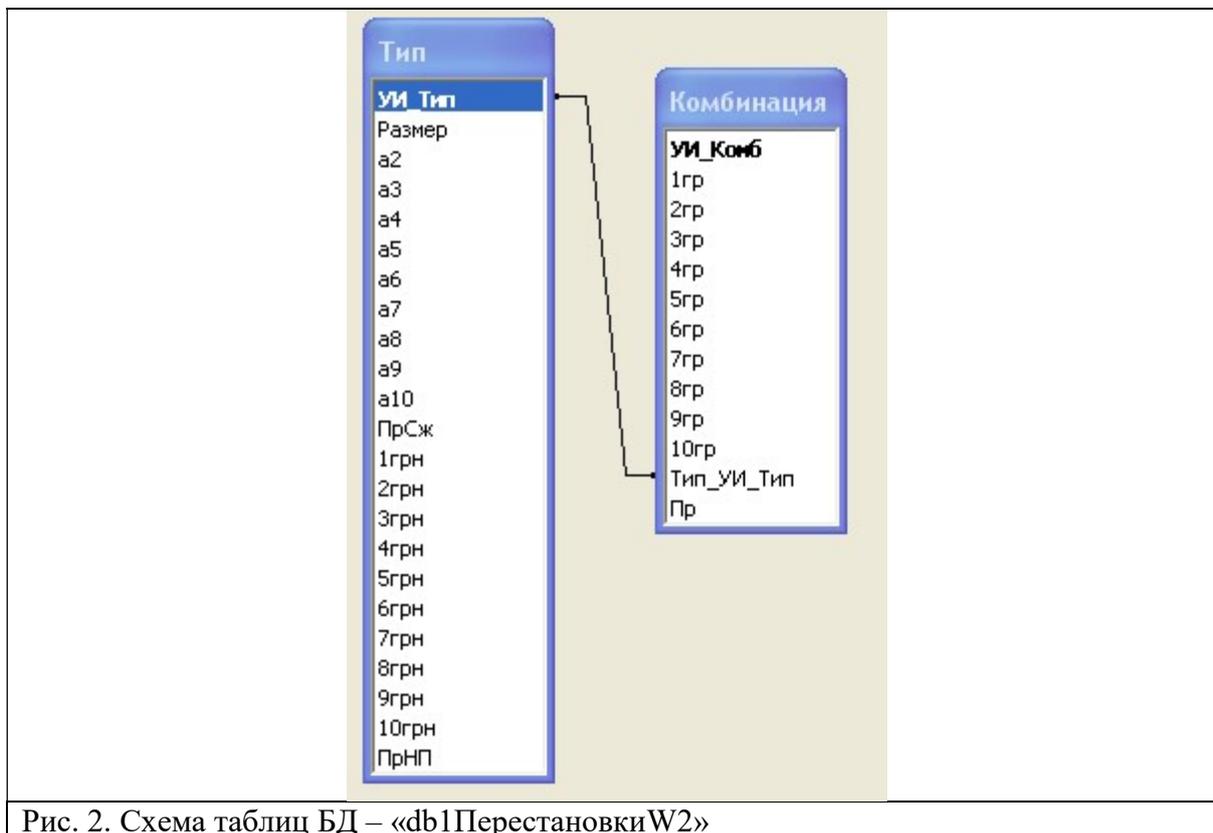
В пределах размера группы меняются позиции передаваемых в канал связи символов (групп, части символов), схема перестановок показана на рисунке 1. На практике, конечно, представляют интерес существенные размеры групп (7, 8, 9 и 10 в действующем прототипе). Для каждой следующей группы символов используется очередная перестановка из применяемой последовательности. После исчерпания всех перестановок последовательности, для следующих групп передаваемых в канал символов, использование последовательности перестановок повторяется.



Чередование перестановок в последовательности зависит от алгоритма генерации. В предлагаемом КГП реализованы несколько алгоритмов.

### Информационная схема генератора перестановок

Генератор перестановок выполнен в виде базы данных (наименование БД – db1ПерестановкиW2). Схема таблиц БД представлена на рисунке 2.



В таблице «Тип» сохраняют данные по размеру группы (колонка «Размер»), идентифицирующему кортежу используемых алгоритмов (колонки «a2», «a3», «a4», «a5», «a6», «a7», «a8», «a9», «a10»), признаку сжатия последовательности (колонка «ПрСж»), идентифицирующему заданной начальной перестановки (колонки «1грн», «2грн», «3грн», «4грн», «5грн», «6грн», «7грн», «8грн», «9грн», «10грн»), признаку использования опции начальной перестановки (колонка «ПрНП»).

В таблице «Комбинация» сохраняют данные по сформированным последовательностям перестановок.

### Форма, отчет и запрос генератора перестановок

Вид формы для генерации последовательностей перестановок представлен на рисунке 3.

Генерация перестановок

Просмотр отчета

УИ\_Тип: 1    Размер группы: 4

Набор перестановок:  Полный     Сжатый

Алгоритм: А2: 1    А3: 1    А4: 1    А5: 0    А6: 0    А7: 0    А8: 0    А9: 0    А10: 0    Сж: 1

В наборе должна быть первой перестановка: 4    1    3    2    0    0    0    0    0    0

УИ_Комб	1гр	2гр	3гр	4гр	5гр	6гр	7гр	8гр	9гр	10гр	УИ_Тип
265	1	2	3	4	0	0	0	0	0	0	1
266	2	1	3	4	0	0	0	0	0	0	1
267	1	3	2	4	0	0	0	0	0	0	1
268	2	3	1	4	0	0	0	0	0	0	1
269	3	1	2	4	0	0	0	0	0	0	1
270	3	2	1	4	0	0	0	0	0	0	1
271	1	2	4	3	0	0	0	0	0	0	1
272	2	1	4	3	0	0	0	0	0	0	1
273	1	3	4	2	0	0	0	0	0	0	1
274	2	3	4	1	0	0	0	0	0	0	1
275	3	1	4	2	0	0	0	0	0	0	1
276	3	2	4	1	0	0	0	0	0	0	1
277	1	4	2	3	0	0	0	0	0	0	1
278	2	4	1	3	0	0	0	0	0	0	1

Номер выбранной записи: 1

Запись: 1 из 24

Запись: 1 из 5

Рис. 3. Вид формы для генерации последовательностей перестановок

Идентифицирующие данные (размер группы, признак последовательности /полный или сжатый набор, кортеж используемых алгоритмов, признак начальной перестановки, сама начальная перестановка) формируемой последовательности перестановок задаются в верхней части формы (с зеленым фоном). Генерация последовательности запускается кнопкой «Генерация перестановок». Сгенерированная последовательность заносится в

подчиненную форму «Перестановки» (в нижней части формы, см. рис. 3). По кнопке «Просмотр отчета» открывается отчет со сгенерированными последовательностями (рисунок 4).

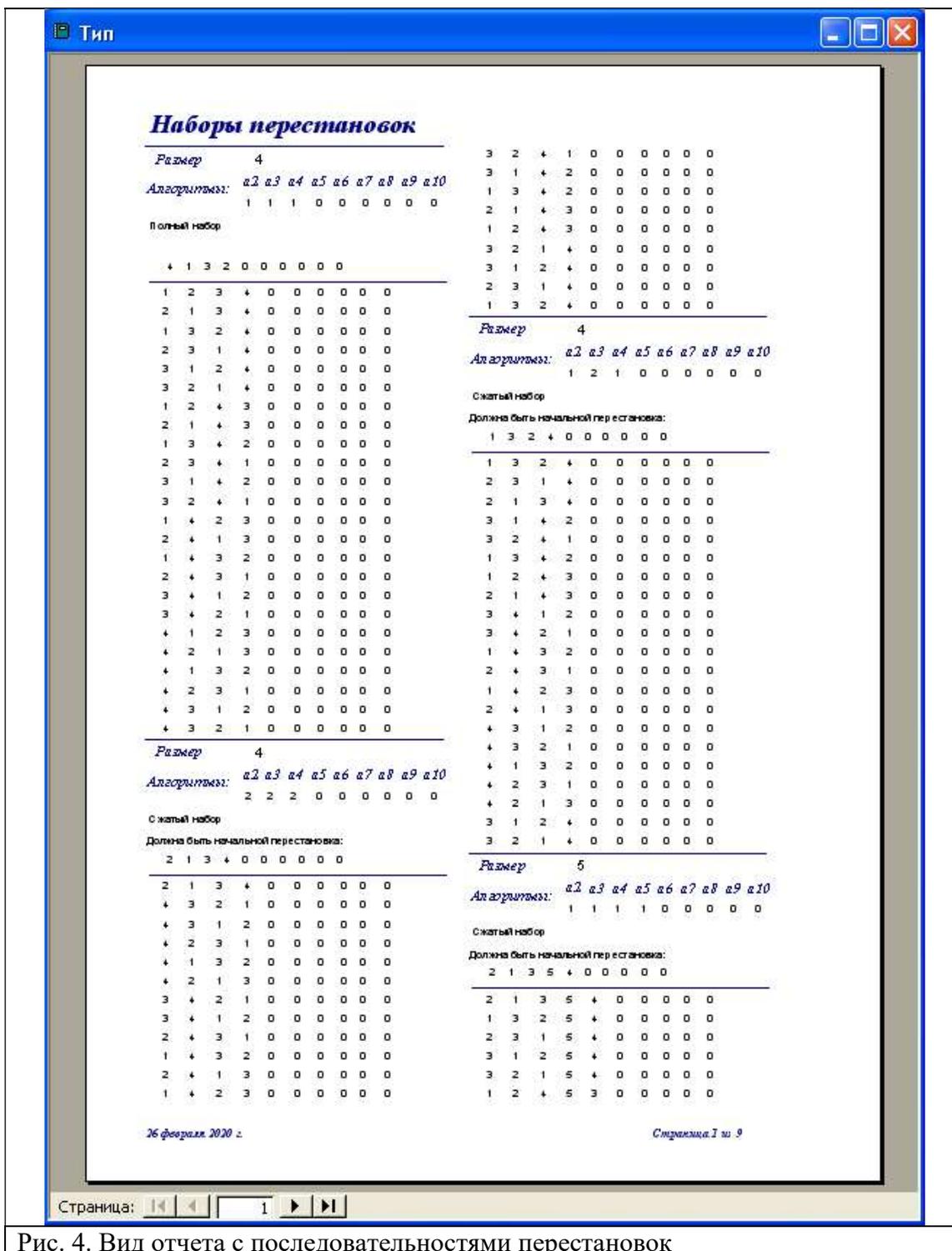


Рис. 4. Вид отчета с последовательностями перестановок

## Программы «Преобразование файла» и «Дешифрование файла»

В простейших схемах защиты передачи файла данных в компьютерных сетях:

- при передаче данных используют телекоммуникационные протоколы с подтверждением;

- перед передачей файла намеренно искажают содержимое файла, чем обеспечивают скрытие его содержимого; например, разбивают файл на группы (группы кодов символов или последовательности блоков двоичных бит файла); в пределах группы в соответствии с некоторой перестановкой (заранее известной и на передающей, и на приемной стороне; периодически такие перестановки меняют синхронно и на передающей и на приемной стороне) меняют порядок следования символов или блоков бит в файле; или криптографически преобразуют [1];
- передают преобразованный файл по сети от передающей к приемной стороне;
- на приемной стороне проводят обратное преобразование.

Такие способы недостаточно скрывают содержимое передаваемых данных. Существуют и другие способы намеренного искажения содержимого файла, но все они предусматривают определенный и неизменный в процессе передачи порядок начальной переработки и конечного восстановления файла; порядок преобразования известен заранее на приемной и на передающей стороне; предусматривают систематическое изменение, например, смену используемой перестановки на приемной и передающей стороне, но частая смена правила преобразования требуют от пользователей приемной и передающей стороны организационных затрат, вызывающих некоторое раздражение при использовании подобных средств защиты.

Предлагается ввести многократную и автоматическую смену правил преобразования файла по ходу первоначального формирования (а, следовательно, и соответствующие смены правил по ходу передачи файла в сети). Использование программы автоматической генерации перестановок (применяемой и на приемной и на передающей стороне) позволяет сократить организационные расходы администраторов системы безопасности. В большинстве случаев достаточно изменить только идентификатор алгоритма формирования перестановок и этого будет достаточно для смены правил преобразований файлов при их передаче по компьютерной сети.

Предлагаются следующие положения, реализуемые в разрабатываемых программах «Преобразование файла» и «Дешифрование файла» для защищенной передачи файлов по сети:

- использование последовательностей перестановок при передаче файла;
- при генерации последовательностей перестановок исключение перестановки с последовательным возрастанием нескольких позиций (например, три и более позиции, что позволяет исключить практически все случаи последовательной передачи групп символов исходного файла);
- использование одной и той же программы генерации последовательности перестановок на приемной и передающей стороне и идентификаторов алгоритмов генерации, что позволяет при организационных решениях исключить необходимость передачи содержательных данных по защищенной трансляции файлов;
- в качестве дополнительной возможности исключение из оборота использование существующих общепринятых средств передачи файлов (программ трансляции файлов, транспортных протоколов с подтверждением) и переход к нестандартным средствам передачи файлов – пользовательским средствам, заменяющим стандартные; это затрудняет доступ к передаваемому и намеренно преобразованному файлу, а, кроме того позволяет в ряде случаев существенно ускорить передачу файлов.

## **Заключение**

Внедрение программно-информационного комплекса защищенной сетевой передачи данных между устройствами существенно сократить затраты системных администраторов защиты данных, повысить уровень защищенности передаваемых данных, а в случае применения альтернативного транспортного протокола, сократить затраты и на собственно передачу данных.

## Список литературы

1. Пат. №2734829, Российская Федерация, МПК: H04L 9/00 (2006.01). Способ криптографического преобразования данных / А. П. Мартынов, И. А. Мартынова, Д. Б. Николаев, А. А. Рыжов, Д. В. Сплюхин, В. Н. Фомченко. Патентообладатели: Российская Федерация, от имени которой выступает Государственная корпорация по атомной энергии "Росатом" (Госкорпорация "Росатом"), Федеральное государственное унитарное предприятие "Российский федеральный ядерный центр - Всероссийский научно-исследовательский институт экспериментальной физики" (ФГУП "РФЯЦ-ВНИИЭФ"). – № 2020109438; заявл. 03.03.2020 опубл. 23.10.2020.
2. Генератор перестановок. Перестановки без повторов и с повторениями // Программирование [Электронный ресурс] URL: <https://prog-cpp.ru/permutation> (28.02.2021).

## Software and information complex for secure data transmission

<sup>1</sup> Bisterfeld N. S., <sup>2</sup> Bisterfeld O. A.

<sup>1</sup> MIREA – Russian Technological University, 119454, Russia, Moscow, Vernadsky Avenue, 78

<sup>2</sup> School 66 of Penza named after Victor Stukalov, 440013, Russia, Penza, Svetlaya St., 1b

To improve the protection of network data transmission, it is proposed to use a software and information complex of secure data transmission. The complex includes: software and information component "Permutation Generator", programs "File Conversion" and "File Decryption". Using the component "Permutation Generator", permutation sequences are generated, according to which the transferred file is converted (on the transmitting side) and the file is decrypted (on the receiving side). Within the group size, the positions of the bits transmitted to the communication channel are changed. We propose to introduce multiple and automatic change of file conversion rules. The alternation of permutations in the sequence depends on the generation algorithm. Several algorithms are implemented. The introduction of a secure network communication software and information complex between devices will significantly reduce the costs of system data protection administrators and improve data transfer security.

*Keyword:* information security, data transfer, encryption, permutation method.